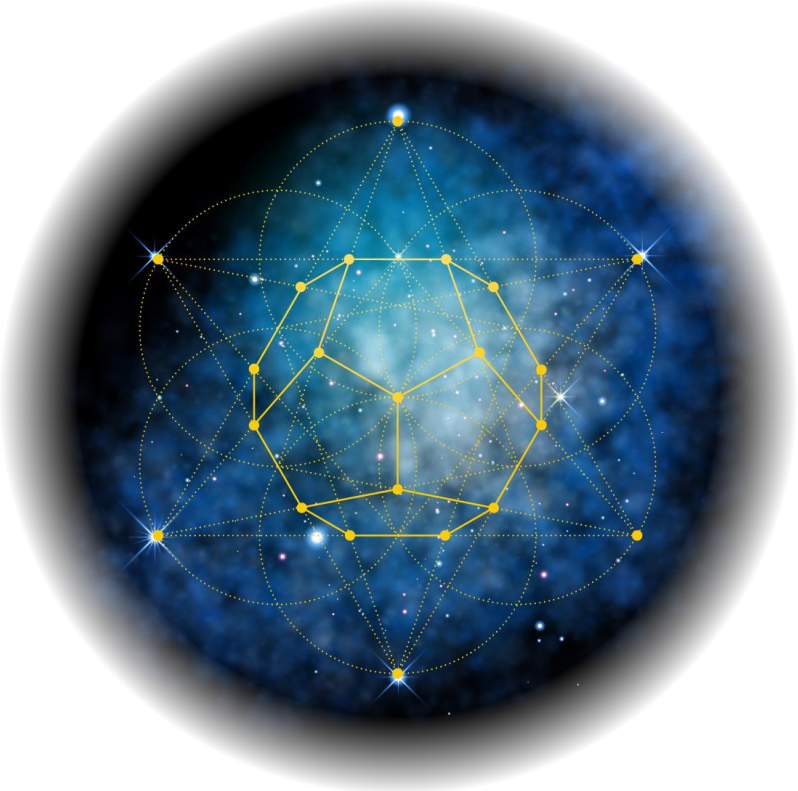
European Commission

Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability



FINAL REPORT

A study prepared for the European Commission

DG Communications Networks, Content & Technology by:

Deloitte.

Digital Single Market

This study is carried out for the European Commission by

Authors

Martina Barbero (Deloitte)

Diana Cocoru (Openforum Europe)

Hans Graux (Deloitte)

Annette Hillebrand (WIK Consult)

Florian Linz (Deloitte)

David Osimo (Open Evidence)

Anna Siede (Deloitte)

Patrick Wauters (Deloitte)

Internal identification

SMART number 2016/0030

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-79-76987-0

doi 10.2759/781960

Catalogue number KK-07-17-132-EN-N

Table of Contents

Table of figures

Table of tables

Abstract (EN)

Analysing and understanding the European Data Economy has recently become a key concern for policy makers willing to enable data based services and products in Europe and willing to exploit all opportunities deriving from new (Big) Data technologies. Although the European Data economy is still "emerging", it is of utmost importance to identify and remove, at this stage, the barriers for its further development in order to achieve a well-functioning and competitive Digital Single Market. This study is a first attempt to characterise the legal, technical and other types of barriers which currently prevent the full deployment of the European Data Economy and which limit Business to Business (B2B) data sharing and re-use in Europe. Based on this analysis, a number of policy options for the future are put forward and considered from a coherence, effectiveness and efficiency perspective. This assessment shows that, at this stage of market development, policy makers should adopt horizontal non-legislative measures in order to build a better ground for a flourishing European Data Economy.

Executive summary (EN)

There is a growing interest in the EU in the data economy, in IoT, robots and autonomous systems and in the emerging challenges they pose for EU policy makers. The purpose of this study was to identify the most important barriers to the development of the data economy and the use of IoT, robots and autonomous systems. It looked in particular at the extent to which issues in the areas of liability, (re-)usability of and access to (third party) data, and interoperability are impediments to the development of these markets.

These are markets that are still in their infancy, i.e. what is known as an 'emergence phase'. To be entirely active in these markets, EU companies need to be intensive data users, but that is the case of only 6.3% according to a study for the European Commission[1]. The fact that most companies have not yet engaged with these markets has been borne out by the qualitative assessment of the business models of more than 100 European firms as part of this study. Most companies have not yet completely integrated these new realities into their business models and approaches. But for the small number of companies which are currently proactively engaged in the data economy, there are genuine uncertainties and barriers to them moving forward, and which may well be acting as deterrents to companies want to enter the market.

Quantifying the barriers is much more difficult, precisely because the market and the barriers are both still emerging. This report should therefore be seen as a first attempt to provide indicative evidence of what barriers exist, their current and likely future impacts on businesses and citizens, and the implications for policy makers. A number of policy options were developed and tested to obtain an indicative ranking of relevant solutions for the short and medium term.

Limitations relating to the findings of this study

The data economy is in the "emergence phase" of a new market. The vast majority of European businesses are still considering how they will integrate these technologies into their business models. Consequently, the results of the study inevitably come from a relatively small group of proactive users of third parties data, IoT, robots and autonomous systems.

The findings on the genuine uncertainties and barriers for the proactive group nevertheless come from a wide range of sources though desk research, surveys, interviews and workshops, but are largely qualitative. The small number of cases and the difficulty for the companies themselves of knowing the true scale or cost of barriers that are still emerging put limits on meaningful quantification.

[1] Source: IDC and Open Evidence study, see p. 30, Second Interim Report, European Data Market Study, June 2016, http://www.datalandscape.eu/study-reports

This report should therefore be considered a first attempt at examining this topic, gathering the existing data and providing pointers for policy makers on where the data economy, as well as the IoT, robots and autonomous systems technologies are heading. The conclusions are based on independent judgement and are specific to this study.

Emerging barriers to the data economy

The barriers identified by this study fall into three broad categories:

- **Technical**: these are primarily in the area of IT and its infrastructure (interoperability and portability);
- **Legal:** these fall into two broad groups – contractual (e.g. 'data ownership' and access to and (re-)use of data) and non-contractual (e.g. extra-contractual liability);
- **Other:** these cover a range of business dimensions (e.g. skills, competition, pricing).

Not all these barriers are equally important individually or to a given company. The extent to which a business operating in the EU will be affected depends on its **position in the value chain, its size and the sector in it operates** (and whether there is already regulation in place to impose some degree of data sharing, as in the case in the automotive value chain, where motor manufacturers must share date with repairers, or in the financial services sectors as the result of the Payments Services Directive 2). The combination of these elements can be a guide to the barriers that a particular firm is likely to face when wanting to share, access or (re-)use third party data.

Looking at the barriers from the perspective of how serious they are, it is possible to distinguish **primary and secondary barriers.**

PRIMARY BARRIERS

- **Access and to (re-)use of data**: Companies cannot access the data they need or would like, and they face strict (contractual) limitations when wanting to (re-)use data;
- **Data liability**: Existing liability laws are based on the concept of tangible products. Companies cannot be sure whether they can have recourse to this legislation for data-based products, so prefer to fall back on contractual liability on a case-by-case basis;
- **Data interoperability:** Different standards and specifications are used for the same data and for different datasets;
- **Unequal bargaining power**: Smaller companies (SMEs) and companies in a weaker position in the value chain do not have the bargaining power to obtain access to certain data, whether for free or at a cost;
- **Skills**: There are not enough people now with the right skills, and the problem is likely to get worse in future.

The barriers in the areas of liability, interoperability and skills are essentially cross-cutting, though large businesses may be better placed to incur the costs of overcoming them. The issues of equitable access to data and unequal bargaining power tend to affect SMEs more.

SECONDARY BARRIERS

Other barriers which are relevant, but not seen as so serious at the current stage of market development are, both in terms of their importance and the number of firms affected:

- **'Data ownership'**: The concept of 'data ownership' is far less controversial for companies than thought when the study was launched; access to and (re-)use of data are much more important;
- **Data portability:** This is not a bar to companies sharing, accessing and re-using data, except in very particular cases;
- **Intellectual property rights (IPR):** There is not felt to be a need to have recourse to the exclusive protection conferred by IPR when sharing, accessing and re-using data as this tool seems inadequate in most cases;
- **Valuing data:** The cost of data is an obstacle for data (re-)users, but if a company is interested in sharing data, it will find a means of valuing it;
- **Procurement:** Procurement barriers are more sporadic than recurrent.

THE CONSEQUENCES

The result, when these barriers (and especially the primary barriers) are taken together, is that:

- They are an impediment to data sharing;
- Businesses and consumers are incurring undue costs;
- Consumer safety is at risk;
- Clear and easy compensation for damage cannot be assured.

This has negative implications for the **Digital Single Market (DSM) and the society overall**. First, these barriers to the data economy are also barriers to **digital competitiveness and innovation.** Second, they constrain **freedom of choice for consumers** and **digital inclusion**.

Issues related to liability of IoT, robots and autonomous systems

A second area looked at in detail in this study is the extent to which **deficiencies in liability legislation are hampering the development and uptake in the EU of data-driven technologies, notably the IoT, robotics, and autonomous systems**. This is largely because of the non-deterministic autonomy of these systems, i.e. their behaviour may change based on what they have learned from their environment, and because of complexity.

This poses problems along the value chain through to the end-user, although these will vary depending on how developed the market is, the development stage a given company has reached in that market and the company's position in the value chain.

Nevertheless it is possible to identify five main axes which determine the types of liability issues and risks:

- **Axis 1 – Autonomy:** the degree of freedom that a device has to actuate in its environment, and specifically the degree of human involvement in either steering the device directly, or in controlling the flow of information that allows the device to determine its actions;
- **Axis 2 – Determinism:** the degree to which the actions of the device are fully pre-programmed or determined algorithmically;
- **Axis 3 – Dependence:** the degree to which the actions of the device depend fully on data derived from its own sensors or on external data;
- **Axis 4 – Operating environment:** the degree to which the devices operate in a clearly demarcated or unbounded space;
- **Axis 5 – Risk context:** the degree of risk that device errors may pose for their owners, businesses, the environment, or society.

The unique characteristics of the IoT, robots and autonomous systems on all of these axes are resulting in the emergence of new and specific liability challenges. These need to be considered in addition from the perspective of different stakeholder groups.

- **Producers** who manufacture an IoT device, robot or autonomous system, either by manufacturing it from scratch or assembling it from pre-existing components. This includes manufacturers of physical components and the providers of the operational logic (i.e. software providers);
- **Product or service providers** who offer a product or service in the market consisting of or using the robot or IoT device. This group includes direct vendors and importers, and service providers. Service providers offer a service that holds, integrates or uses the robot or IoT device. The customer does not necessarily become the owner of a device or robot, but enters into a service agreement;
- **End-users** who buy a robot or device (without the intent of building their own product or service around it), or who use a robot or device without necessarily owning it;
- **Injured parties** who suffer harm in relation to the use of a robot or device. These are not necessarily owners or users; they may simply be bystanders who were in the wrong place at the wrong time.

The combination of the Axes and the range of stakeholders makes this a more complex landscape than for conventional products, so that existing product liability concepts based on tangible products whose characteristics do not change over time may cease to be adequate. At the same time, this is an emerging market, where quantitative data is lacking and there is no experience of testing how liability law might apply. Moreover, it is evolving rapidly and in unpredictable ways. It is likely that the business models of today are not the business models of tomorrow.

On the one hand, there is a risk therefore in rushing to legislate and in singling out the IoT or robots specifically. On the other, the uncertainty about the liability regime in combination with the issues around autonomy and complexity could limit the take-up of IoT, robotics, and autonomous devices, by producers, service providers and end users because of:

- **Uncertainty about the extent to which existing liability regimes might apply;**

- **Divergences in national liability regimes; and**
- **The inability of Injured parties to count on the effective availability of redress.**

Both B2B and B2C transactions are suffering undue cost as a result. If costs to business came down, including the cost of legal advice and drawing up contracts case-by-case, the savings would be passed on to consumers, assuming competitive markets.

Assessment of the possible policy options

The study identifies a number of 'hard' and 'soft' options for the Commission if it wants to address the negative externalities related to the emerging barriers to the data economy and the liability issues affecting the IoT, robots and autonomous systems. They are:

- **Option 0 – No intervention:** no policy measure is taken to address these emerging barriers. This is the baseline scenario against which all other options are assessed.
- **Option 1A – Horizontal non-legislative measures:** awareness-raising, sharing of best practices, funding for research etc. across sectors and domains;
- **Option 1B – Sector-specific non-legislative measures:** a mirror of 1A but by sector.
- **Option 2A – Horizontal legislative measures:** a limited number of cross-cutting regulatory measures by barrier: liability, access to and (re-)use of data or interoperability, in the form of Regulations or Directives.
- **Option 2B – Sector-specific legislative measures:** mirrors option 2A but Regulations or Directive would be sector-specific (akin to the existing. Regulation that gives independent car repair companies access to manufacturers' data).

Options 1A first and then option 1B emerged from multi-criteria analysis as those to be preferred based on three main criteria (effectiveness, efficiency and coherence). They were followed by the baseline scenario and finally by policy options 2A and 2B.

Thus, **non-legislative measures (and especially cross-sectoral non-legislative measures) are to be preferred at this stage of the development of the markets**. However, continuous monitoring of barriers, liability issues and cases, and business models is called for to be ready to regulate when and if it is necessary.

Résumé extrait (FR)

Analyser et comprendre l'économie européenne des données est devenue une préoccupation majeure pour les décideurs politiques souhaitant favoriser le développement de services et produits basés sur les données en Europe et exploiter toutes les opportunités dérivant des nouvelles technologies issues du « Big data ». Même si l'économie européenne des données est toujours à ses prémices, il est primordial dès ce stade d'identifier et d'éliminer les barrières à son évolution future, nécessaire au bon fonctionnement et à la compétitivité d'un marché unique du numérique. Cette étude est une première tentative d'identification des barrières légales, techniques ou de tout autre type, qui empêchent le déploiement intégral de l'économie européenne des données en limitant leurs partages entre entreprises (« Business to Business ») et leurs réutilisations en Europe. Sur la base de cette analyse, un certain nombre d'options politiques pour l'avenir sont proposées et évaluées en fonction de leur cohérence, de leur efficacité et de leur efficience. Cette évaluation montre qu'au stade actuel du développement de ce marché, les décideurs politiques devraient adopter des mesures horizontales, non-législatives, permettant la création d'un terrain plus propice à l'épanouissement d'une économie européenne des données.

Résumé (FR)

Ces dernières années ont vu l'émergence d'un intérêt croissant en Europe pour l'économie des données, pour l'Internet des Objets (IdO), la robotique ou pour les systèmes autonomes notamment par rapport aux nouveaux défis que ces derniers posent aux décideurs politiques européens. L'objet de cette étude est d'identifier les barrières les plus importantes relatives au développement de l'économie des données et à l'utilisation de l'IdO, des robots et des systèmes autonomes. Cette dernière cherche plus particulièrement à évaluer dans quelle mesure des problèmes concernant la responsabilité juridique, les possibilités de réutilisation ou d'accès aux données (notamment de tiers) ou d'interopérabilité, constituent des entraves aux développements de ces marchés.

Ces marchés n'en sont encore qu'à leurs débuts, c'est à dire dans une « phase d'émergence ». Pour être classifié comme « actif » sur ces marchés, les entreprises européennes doivent utiliser des données de manière intensive, ce qui est le cas pour seulement 6,3% d'entre elles selon une étude commanditée par la Commission européenne.[2] Le fait que la vaste majorité des entreprises ne se soient pas encore pleinement engagées sur ces marchés est corroboré dans cette étude par une analyse qualitative des modèles économiques de plus de 100 entreprises européennes. La plupart des entreprises n'ont pas encore complètement intégré ces nouvelles réalités que ce soit au sein de leurs modèles économiques ou de leurs stratégies. Mais un petit nombre d'entreprises, actuellement engagé de façon proactive dans l'économie des données, font face pour aller plus en avant à un nombre d'incertitudes et à des obstacles qui pourraient bien avoir un effet dissuasif pour des compagnies souhaitant également entrer sur ce marché.

Mesurer l'impact de ces barrières est beaucoup plus difficile, précisément car ce marché et ces dites barrières sont en voie d'émergence. Cette étude doit de ce fait être perçue comme une première tentative d'apporter des éléments de preuve quant à l'existence de ces barrières, à leur impact actuel ainsi qu'à leurs incidences futures sur le commerce et les citoyens, et dans un second temps d'en tirer les conclusions qui s'imposent pour les décideurs politiques. Un certain nombre d'options politiques ont ainsi été développées et testées afin d'obtenir un classement indicatif des solutions pertinentes à court et moyen terme.

Limites concernant les conclusions de la présente étude

L'économie des données n'en est qu'à la phase d'émergence d'un nouveau marché. La grande majorité des entreprises sont encore en train d'évaluer comment elles vont intégrer

[2] Source: IDC and Open Evidence study, see p. 30, Second Interim Report, European Data Market Study, June 2016, http://www.datalandscape.eu/study-reports

ces technologies à leurs modèles commerciaux. Par conséquent, les résultats de cette étude proviennent nécessairement d'un groupe proactif relativement réduit d'utilisateurs ayant recours aux données de parties tierces, et aux technologies basées sur l'IdO, la robotique ou sur les systèmes autonomes.

Les conclusions concernant les incertitudes et les barrières auxquelles sont confrontées les entreprises qui composent ce groupe proactif proviennent cependant d'un large éventail de sources issues de recherches documentaires, d'études, d'interviews et de workshops, essentiellement qualitatives. Le petit nombre de cas et les difficultés pour les entreprises elles-mêmes de connaître l'étendue des coûts engendrés par des barrières en cours de création sont autant de limites à une quantification probante.
Ce rapport doit donc être considéré comme une première tentative d'analyse de ce sujet, collectant les données existantes et proposant des pistes de réflexions pour les décideurs politiques quant aux directions actuellement prises par l'économie des données, ainsi qu'en matière d'IdO, de robotique et de systèmes autonomes. Les conclusions reposent sur un examen indépendant et sont spécifiques à cette étude.

Les barrières émergeantes dans l'économie des données

Les barrières identifiées par cette étude tendent à se répartir en trois grandes catégories :

- **Techniques :** se trouvant principalement dans le domaine de l'informatique et de ses infrastructures (interopérabilité et portabilité) ;
- **Légales :** pouvant être divisées en deux grands groupes – contractuel (ex : « propriété des données », accès et ré(utilisation) de données) et non-contractuel (ex : responsabilité extracontractuelle);
- **Autres :** couvrant un large éventail de dimensions commerciales (ex : compétences, concurrence, prix).

Toutes ces barrières ne sont pas d'une importance égale, et doivent être examinées individuellement que dans le cadre d'une entreprise donnée. Le degré d'affectation d'une entreprise opérant dans l'UE **dépendra de sa position au sein de la chaine de valorisation, de sa taille et du secteur dans lequel elle opère** (et de l'existence ou non d'une réglementation imposant un certain degré de partage des données, comme c'est le cas au sein de la chaine de valorisation de l'automobile, où les fabricants de moteurs doivent partager des données avec les réparateurs, et dans le secteur des services financiers du fait de la directive sur les services de paiement DSP2). La combinaison de ces éléments peut constituer un guide des barrières qu'une entreprise est susceptible de rencontrer lorsqu'elle souhaite partager, accéder ou (ré)utiliser des données de parties tierces.

Si l'on considère ces barrières en fonction de leur impact, il est possible de distinguer des **barrières primaires et secondaires**.

BARRIÈRES PRIMAIRES

- **Accès et (ré)utilisation des données** : certaines entreprises ne peuvent accéder aux données auxquelles elles souhaiteraient avoir accès ou dont elles ont besoin, et elles

font face à des limitations (contractuelles) strictes lorsqu'elles souhaitent (ré)utiliser ces données ;

- **Responsabilité en raison des données :** les réglementations en matière de responsabilités reposent sur le concept de produits tangibles. Les entreprises ne peuvent être certaines de pouvoir avoir recours à ces législations pour des produits reposant sur des données, et préfèrent au cas par cas se tourner vers la responsabilité contractuelle ;
- **Interopérabilité des données :** différents standards et spécifications sont utilisés pour les mêmes données et pour différents jeux de donnés.
- **Inégalité du pouvoir de négociation** : les petites entreprises (PME) et les entreprises de moindre importance au sein de la chaine de valorisation n'ont pas un pouvoir de négociation suffisant pour obtenir accès à certaines données, que ce soit gratuitement ou contre rémunération ;
- **Compétences :** il n'y a actuellement pas assez de personnes possédant les compétences nécessaires et ce problème tend à s'aggraver.

Les barrières dans les domaines de la responsabilité, de l'interopérabilité et des compétences sont partagées, même si de grandes entreprises peuvent s'avérer être dans une meilleure position pour supporter les coûts nécessaires à leurs dépassements. Les problématiques relatives à l'accès équitable aux données et concernant l'inégalité du pouvoir de négociation tendent à affecter d'avantage les PME.

BARRIÈRES SECONDAIRES

D'autres barrières sont importantes, mais ne sont pas considérées comme aussi déterminantes à l'étape actuelle du développement du marché, que ce soit au regard de leur importance et du nombre d'entreprises affectées :

- **« Propriété » des données :** la question de la « propriété » des données est beaucoup moins sujette à controverse pour les entreprises qu'envisagé lors du lancement de la présente étude : l'accès et la (ré)utilisation des données sont des préoccupations beaucoup plus importantes ;
- **Portabilité des données :** la portabilité n'est pas un obstacle pour les entreprises partageant, accédant et (ré)utilisant des données, à l'exception de quelques cas très particuliers ;
- **Droits de propriété intellectuelles (DPI) :** il ne semble pas y avoir de besoin d'un recours à la protection exclusive conférée par les DPI en ce qui concerne le partage, l'accès et la (ré)utilisation de données, car ces droits apparaissent comme des outils inadéquats dans la plupart des cas ;
- **Valorisation des données** : le coût des données est un obstacle pour les (ré)utilisateurs de données, cependant si une entreprise est intéressée par leurs partages, elle trouvera une possibilité de les valoriser ;
- **Processus d'acquisition:** les barrières relatives au processus d'acquisition sont plus sporadiques que récurrentes.

LES CONSÉQUENCES

Lorsque ces barrières (et particulièrement les barrières primaires) sont considérées dans leur ensemble, l'on peut conclure que :

- Il existe des entraves au partage des données ;
- Les entreprises et les consommateurs supportent des coûts indus ;
- La sécurité du consommateur est mise en jeu ;
- Une compensation claire et facile en cas de dommage ne peut être assurée.

Il en résulte un impact négatif sur le **Marché Unique Numérique (MUN) et pour la société dans son ensemble.** Premièrement, ces barrières à l'économie des données sont également des barrières à la **concurrence et à l'innovation digitale.** Deuxièmement, elles réduisent la **liberté de choix du consommateur** et **l'insertion numérique**.

Problèmes relatifs à la responsabilité en matière d'IdO, de robotique et de systèmes autonomes

Un second domaine abordé par cette étude est la question de savoir dans quelle mesure des **lacunes dans les législations relatives au droit de la responsabilité entravent le développement et l'adoption de technologies basées sur les données, notamment l'IdO, la robotique, et les systèmes autonomes dans l'UE.**

Ceci est largement attribuable à l'autonomie non-déterministe de ces systèmes (leur comportement pouvant changer en fonction de ce qu'ils ont appris et de leur environnement) ainsi qu'en raison de leur complexité.

Cela pose des problèmes tout au long de la chaine de valeur jusqu'à l'utilisateur final, même si ces derniers varieront en fonction du degré de développement du marché, du stade de développement atteint par une entreprise donnée au sein de ce marché et enfin de la position occupée par l'entreprise au sein de la chaine de valeur.

Cependant, il est possible d'identifier cinq axes majeurs qui déterminent les types de problèmes et les risques relatifs à la responsabilité :

- **Axe 1 – Autonomie :** le degré de liberté dont dispose un équipement pour agir dans son environnement, et spécifiquement le degré d'implication humaine qu'il soit direct par le pilotage de l'équipement ou qu'il consiste dans le contrôle du flux d'informations qui permet à l'équipement de déterminer ses actions ;
- **Axe 2 – Déterminisme :** le degré de complète pré-programmation ou détermination algorithmique des actions de l'équipement ;
- **Axe 3 – Dépendance :** le degré de dépendance pour la détermination des actions de l'équipement, de données dérivées de ses capteurs ou de sources externes ;
- **Axe 4 – Environnement opérationnel :** le degré de délimitation spatiale dans lequel l'équipement est utilisé ;
- **Axe 5 – Contexte de risque :** le degré de risque que les erreurs de l'équipement pourraient causer à ces détenteurs, aux entreprises, à l'environnement ou à la société.

Les caractéristiques uniques de l'IdO, des robots et des systèmes autonomes sur l'ensemble de ces axes expliquent l'émergence de nouveaux enjeux spécifiques à la responsabilité. Ces derniers doivent qui plus est être mis en perspective des différents groupes de parties intéressées :

- **Les producteurs** qui fabriquent un équipement basé sur l'IdO, un robot ou un système autonome, que ce soit en partant de zéro ou en l'assemblant à partir de composantes préexistantes. Ce groupe comprend les producteurs de composants physiques et les fournisseurs de la logique de fonctionnement (ex : fournisseur de logiciel);
- **Les fournisseurs de produits ou de services** qui offrent un produit ou un service sur un marché fournissant ou utilisant le robot ou un équipement basé sur l'IdO. Ce groupe inclut les vendeurs directs, les importateurs ainsi que les prestataires de services. Les prestataires de services offrent un service contenant, intégrant ou utilisant un robot ou un équipement basé sur l'IdO. Le client ne devient pas nécessairement le détenteur de l'équipement ou du robot, mais conclut une convention de service;
- **Les utilisateurs finaux** qui achètent le robot ou l'équipement (sans avoir la volonté d'élaborer leur propre produit ou service à partir de ce dernier), ou qui utilise le robot ou le service sans nécessairement le détenir;

- **Les victimes** qui souffrent d'un dommage causal à l'utilisation du robot ou de l'équipement. Ils ne sont pas nécessairement des détenteurs ou des utilisateurs : ils peuvent simplement être des passants qui se trouvaient au mauvais emplacement au mauvais moment.

La combinaison des axes d'analyse et la diversité des parties prenantes rend ce paysage plus complexe que pour des produits conventionnels, ce qui explique que des concepts de responsabilité, basés sur des produits tangibles dont les caractéristiques n'évoluent pas au fil du temps, se révèlent en la matière inadéquats. Cependant, il s'agit d'un marché en développement, pour lequel des données quantitatives manquent et pour lequel aucune d'application du droit de la responsabilité n'a encore eu lieu. Qui plus est, ce marché évolue rapidement et d'une façon imprévisible. Il est aussi probable que les modèles économiques d'aujourd'hui ne soient pas ceux de demain.

Il y a donc un risque de se hâter à légiférer et d'isoler l'IdO ou les robots spécifiquement. Cependant, l'incertitude concernant le régime de responsabilité en combinaison avec les problématiques relatives à l'autonomie et à la complexité de ces systèmes pourraient limiter l'adoption de l'IdO, de la robotique et des systèmes autonomes, que ce soit par les fabriquant, les fournisseurs de services et les utilisateurs finaux en raison de :

- **l'incertitude quant au degré d'application des régimes de responsabilité existant ;**
- **des divergences dans les régimes nationaux de responsabilité et ;**
- **dans l'incapacité pour les victime de pouvoir compter sur des moyens de recours efficaces.**

Aussi bien les transactions entre entreprises (B2B) que celles entre entreprises et consommateurs (BC2) souffrent de ce fait de coûts injustifiés. Si les coûts des entreprises diminuent, notamment ceux relatifs aux conseils légaux et à la rédaction de contacts au cas par cas, ces économies devraient se répercuter sur les consommateur (en supposant que les marchés soient compétitifs).

Evaluation des options possibles

Cette étude identifie un certain nombre d'options législatives et non-législatives pour la Commission, si cette dernière souhaite résoudre les externalités négatives liées aux barrières émergentes dans l'économie des données et aux problématiques relatives à la responsabilité affectant l'IdO, la robotique et les systèmes autonomes. Il s'agit :

- **Option 0 – l'absence d'intervention :** aucune mesure politique n'est prise pour remédier à ces barrières. Il s'agit du scénario de base à partir duquel toutes les autres options sont évaluées.
- **Option 1A – prise de mesures horizontales non-législatives :** travail de sensibilisation, partage des meilleures pratiques, financement pour la recherche, etc. de façon transversale aux secteurs et domaines ;
- **Option 1B – prise de mesures sectorielles non-législatives :** l'équivalent de l'option 1A mais par secteur.
- **Option 2A – prise de mesures législatives horizontales :** un nombre limité de mesures réglementaires transversales par barrière : relatif à l'accès et à la (ré)utilisation des données ou à leurs interopérabilités, prenant la forme de Règlements ou de Directives.
- **Option 2B – prise de mesures législatives sectorielles :** l'équivalent de l'option 2A, mais les Règlements ou Directives seraient sectoriels (similaires aux régulations donnant accès aux réparateurs indépendant de voitures aux données des fabricants).

Les option 1A suivie par l'option 1B ont émergé d'analyses basées sur des critères multiples comme celles devant être préférées sur la base des trois critères principaux (l'efficacité, l'effectivité et la cohérence). Elles sont suivies par le scénario de base et finalement par les options 2A et 2B.

Ainsi, **des mesures non-législatives (et particulièrement horizontales non-législatives) devraient être préférées au stade présent de développement de ce marché.** Cependant, un suivi continue des barrières, des problématiques de responsabilités et des affaires qui y sont liées, ainsi que des modèles économiques est souhaitable pour être prêt à légiférer lorsque, et si, cela venait à s'avérer nécessaire.

1 Introduction

This chapter illustrates the purpose of the document and briefly explains which data collection tools were used to gather the evidence underpinning the findings and conclusions of this assignment.

Purpose of the document

This document is the Final Report of the assignment: ***Study on emerging issues of data ownership, interoperability, (re-)usability and access to data and liability***. It contains the final problem assessments for the assignment, a description of the policy options available and assessment of their impact against the criteria defined as relevant[3].

The purpose of the document is to offer:

- An **analysis of the emerging barriers** (or problems) for firms wanting to share or access third party data. The analysis builds on all the data collected through different tools, such as interviews, case studies, surveys and workshops, which are presented in the next section. It triangulates these findings in order to provide a representative picture of the status quo in terms of barriers (Chapters 2 and 3).
- An **analysis of the issues** related to liability in relation to the Internet of Things (IoT), robots and autonomous systems. This analysis also builds on the evidence gathered through the assignment and especially on the legal analysis (Chapter 3).
- **Policy objectives and policy options** based on discussion held with the Commission and during stakeholders' workshops (Chapter 4).
- **Insights into the impact of the different options compared to the baseline scenario**. The assessment of the impact is based on the criteria defined and agreed with the European Commission. The chapter on the impact assessment also provides a clear order of preference of potential policy options for the European Commission in order to address the problems identified in the first part of the analysis (Chapter 5).
- **Final conclusions** on the main findings of this assignment and pointers for the European Commission's future activities (Chapter 6)

This document also contains Annexes setting out:

- the outcome of the **legal mapping** (Annex 1);
- the outcome of the **sectoral case studies** (Annex 2);
- the outcome of the **general and specific survey results** (Annex 3);
- the approach for the **impact assessment** (Annex 4);

[3] See Annex 4 - Approach to the impact assessment

- the supporting tables for the **Multi-Criteria Analysis - MCA** (Annex 5).

The next section briefly presents the methodological tools used for data collection.

Methodology for the assignment

The evidence supporting this analysis comes from a number of different sources:

- Business model mapping;
- Legal research, mapping and analysis;
- General survey;
- Specific survey;
- Interviews;
- Case studies; and
- Workshops;

The first step of the assignment consisted of **business model mapping** based on desk research and analysis of some 100 real life cases[4]. The team also carried out selected interviews with sector experts and data analytics companies in order to fine tune the understanding of the real-life cases. This contributed to the development of the qualitative and quantitative assessment of how companies share, access and (re-)use data in the current context.

In parallel to the business model mapping, the team carried out **legal research, mapping and analysis** focussing on two aspects. First, to the extent possible, the teams collected real contracts regulating the data sharing and access between firms. Particular attention was paid to questions related to 'ownership', re-use, intellectual property protection and liability. This also involved looking at the clauses underlying access to data from online business platforms and analysing relevant case law at the European and national level. Second, the team mapped the Member States' specific legal frameworks on data 'ownership', Machine 2 Machine (M2M) contracting and liability for IoT and autonomous systems. Additionally, the team also considered other sectoral (e.g. automotive) or horizontal legal frameworks (e.g. consumer protection rules) impacting the digital economy overall in order to gain a complete picture of the legal and regulatory environment.

The team also carried out two separate surveys for this assignment. The **general survey** was entrusted to an external survey company and targeted random companies in different sectors through phone interviews conducted in three languages (English, French and German). This general survey covered all sectors, albeit to a different extent, and with the exception of aerospace and finance for which sufficient data could be gathered through the other sources. It covered nine countries (Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Sweden and United Kingdom). The purpose of the general survey was to reach out to

[4] Typically, reports about the impact of big data on specific sectors mention examples of cases to illustrate the impacts. These cases have been gathered and systematically analysed. While not providing a statistically representative sample, this method is effective for a) gathering a high-level overview of the degree of data sharing and b) identifying a rich and diverse typology of solutions.

European companies to collect data on the barriers which are the object of this assignment and on the related costs and effects.

The outcome of the general survey should not be used for generalisations or be taken as representative given the number of respondents (N = 151). This is too limited to represent all European businesses in all sectors, but these data nonetheless provide a very good indication of the barriers and problems of European companies as the interviewees were selected based on randomisation.

The **specific survey** aimed to gather evidence on the barriers, benefits and costs related to the sharing of data from data analytics companies and start-ups which do already have a strong interest in this domain. This survey obtained 58 completed answers (and 150 uncompleted) coming from companies based in different European countries and operating in different sectors, although mostly from the automotive sector. The outcome of this survey was useful therefore in refining the analysis based on the experience of the data economy frontrunners.

Because the respondent pool of the general survey included companies who are already very active in the data economy and others which are not, while the respondents to the specific survey were all already active, this explains discrepancies between the general survey and specific survey data.

The input coming from the general and specific survey were always considered in the light of the findings emerging from the **case studies** and the interviews. The team carried out ten case studies in a number of sectors and domains:

- Aerospace;
- Agriculture;
- Chemicals;
- Energy;
- Financial services;
- Health;
- Machinery and industrial platforms
- Retail;
- Telecommunication;
- Transport and automotive.

The case studies were developed based on desk research and interviews with stakeholders from the sector value chain. Each case study built on the data coming from the business model mapping and provided insights into the main barriers for the specific sector.

Further to the interviews carried out for the case studies, the team also had a number of **semi-structured interviews** with other stakeholders in additional sectors (e.g. IT service providers). These interviews were mostly carried out in the inception phase of the assignment and helped fine-tune the team's understanding of the current situation as well as develop all the other data collection tools.

Finally, the team assisted the European Commission in the organisation of **three different workshops** aimed at consulting stakeholders on the emerging barriers, especially with respect to access and (re-)use of data, as well as liability. One workshop specifically targeted SMEs while the other two targeted the Member States and the stakeholders coming from smart industries respectively. The discussion held during these workshops also fed into this deliverable.

The data coming from all these different sources was triangulated for the purpose of validation and to ensure the soundness of the analysis presented below.

Before entering into the detail of the assessment, the next chapter presents the main data on the status quo of the B2B data market and its trends, in order to provide the background for building a number of hypotheses to test.

Limitations relating to the findings of this study

As part of this study, evidence was gathered from various sources, including desk research, surveys with businesses, interviews with businesses and other stakeholders as well as several workshops.

The data collection was hampered by the fact that the markets considered are still emerging: European businesses are currently examining and integrating new technologies such as data, IoT, robots and autonomous systems in their ways of working. However, this study found that the share of businesses that can be considered proactive users of these technologies is still small.

This situation poses challenges on the findings of this study. While we were able to find genuine uncertainties and barriers for the companies that are already active users of new technologies, it was more difficult to quantify such challenges, e.g. because case numbers are still small or the barriers are just emerging and stakeholders themselves do not yet know their scale and/or costs. In addition, the stakeholders consulted do not yet have a final and consolidated perception of how these new technologies will work for them and which particular challenges they will bring in future.

Given the "emergence" stage of the markets under scrutiny, this report should be considered as a first attempt at examining this topic and gathering the existing data on these subjects. This analysis is therefore based on the limited data available and provides a preliminary (mainly qualitative) overview of the main trends, barriers and risks which should be the object of the policy makers' attention for the future with respect to the data economy as well as the IoT, robots and autonomous systems technologies. The conclusions reached are based on independent judgement and specific to this study.

2 State of the data market and trends over time

This chapter illustrates the state of play of the data market and its current trends in order to provide the basis for the problem assessment.

State of play of the data market

Key messages:

- The data market in Europe is still emerging as only a limited number of companies (6.3%) take active part in B2B data sharing and (re-)use.
- Companies are still analysing what their role in the data economy might be and how they can benefit from it, very often adopting a 'wait-and-see' approach.
- All the available data nonetheless confirms that companies are increasingly interested in sharing and accessing data.
- This 'emergence stage' of the market does not mean that the problems assessed by this report are not relevant or impactful, but rather that, for the moment, they affect primarily the most innovative players in Europe.

For the understanding of the following sections and of the assessment of causes and problems described in the next chapter, it is crucial to acknowledge that the **EU data economy is still in an 'emergence stage'**. This was suggested by the vast majority of the interviewees across all sectors and also reiterated during the stakeholder workshops[5]. Moreover, according to a recent study on the European Data Market, ***6.3% of European companies only are currently intensive data users***[6].

In fact, although there are very good examples of how the exchange of data between businesses within the same ecosystem can work[7], the overwhelming majority of businesses across all industries are still trying to identify their role, their niche, the added value for them, and the tools they might need etc. As one interviewee put it, "we are on the verge of a data revolution and we want to be part of it. However, we need to make sure that we have the right understanding of the challenges and the right equipment before we jump off the cliff."[8] In short, although businesses recognise the great potential of generating, sharing and

[5] http://ec.europa.eu/information_society/newsroom/image/document/2016-48/17_october_high_level_conference_report_final_40080.pdf
[6] See *The European Data Market Study: Final Report, 2017*: http://www.datalandscape.eu/study-reports
[7] See Annex 2 – Sectoral Case Studies
[8] See case study on the Financial Services sector

re-using data, most of them are tending to 'wait and see' and follow a step-by-step, piece-meal-engineering type of approach instead of fully embracing digital (business) opportunities[9].

Many of the reasons for this caution are associated with uncertainty around technical and legal issues[10], as well as with actual technical and legal barriers, which are all causes that are assessed in the present assignment. Sometimes fear of reputational losses also enters into play[11]. Most importantly, however, this can be regarded as a natural market development: it takes time before technologies – especially those with such disruptive potential as the Internet of Things, Robotics, and M2M contracting – realises their full economic potential within the different sectoral markets. In many sectors, CEOs are still waiting for a demonstration of successful business cases before deciding to change traditional ways of doing things and share their data or invest in accessing others'.

The extent to which this 'wait-and-see' attitude can be attributed to either the market 'emergence stage' or to the technical, legal and other barriers cannot be assessed at this stage. Most probably, both are intertwined and are mutually dependent:

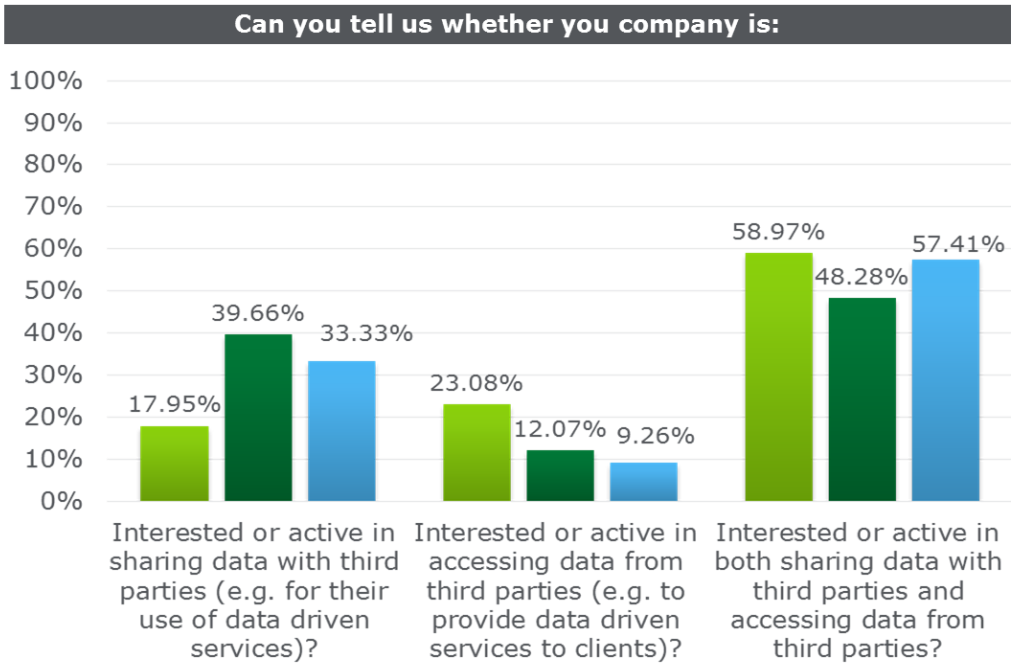
- The market is still emerging because there are technical, legal and other barriers; and
- At the same time, the technical, legal and other barriers have not yet been overcome by businesses themselves because businesses are not yet fully up to speed, 'ready', and 'savvy' about the current possibilities and future opportunities for data sharing (i.e. the market 'emergence phase').

This means that for some industries (or specific businesses, or Member States, or types of products and services), it is critical to address the technical and/or legal barriers to developing the market. However, for other industries (or specific businesses, or Member States, or types of products and services), adapting to the changing nature of business and preparing internally for future business opportunities in order to be 'ready' and 'savvy' can also be a priority in moving to the 'breakthrough stage' of the market.

Despite the market being still in the 'emergence stage'[12], the general survey carried out by the team suggests that there is an appetite for data: as shown in the figure below, companies of all sizes are interested or already active in reaping the benefits of the data economy and deploying data based business models. Most of them are interested and/or active in both sharing and accessing data with third parties (see figure below).

[9] See for instance the case study on the Chemicals sector or the case study on traditional banks within the Finance sector, Annex 2 – Sectoral case studies
[10] See Chapter 3 – Problem Assessment
[11] See for instance the Finance case study, Annex 2 – Sectoral case studies.
[12] See the following section on the theoretical market development

Figure 1: Interest in sharing and accessing data



Light green: companies with fewer than 250 employees
Dark green: between 250 and 1000
Light blue: more than 1000

Source: Deloitte, General Survey

Given the interest of businesses in both accessing and sharing data, one could argue that there is a trend towards more and more data ecosystems rather than bilateral data relations. This hypothesis is supported by some recent experiences in various domains (e.g. agriculture, retail) which aim at creating Data Lakes and industrial data platforms where different players can upload their data and have access to third party's data. From these experiences, it emerged that there is an interest in sharing and accessing data along the value chain.

This trend will be further amplified by increased take-up of IoT as there will be an increased availability of sensor- and machine-generated data to tap into. In this respect, a preference emerged from the general survey for human-generated data[13] (chosen by 76% of respondents[14]), while data analytics companies and start-ups answering the specific survey opted more for sensor-generated data (82% against 3% for human generated data and 15% for

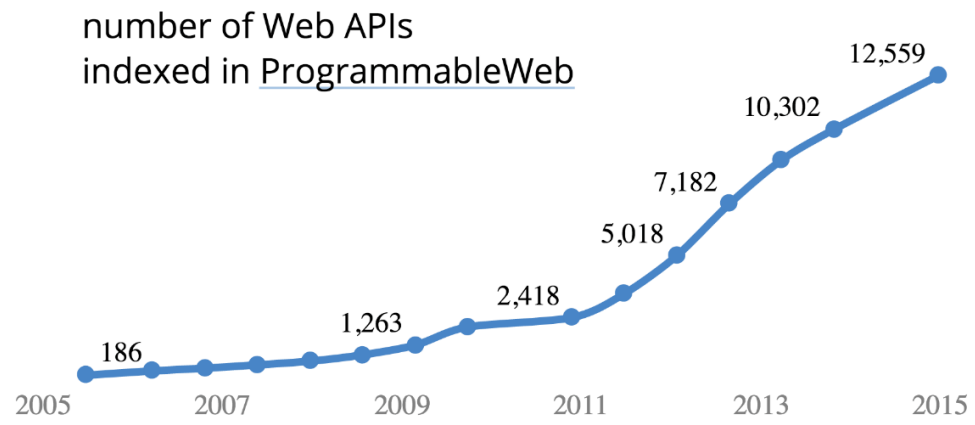
[13] Human generated data can be defined as the record of human experiences and they include for instance social media and internet searches, videos, messages and human-produces online contents.

[14] From the general survey: to the question "what kind of data does your company need"? 76% of respondents said they need human-generated data against 22% who said they do not, 51% said they need process-generated data against 49% who do not, 30% said they need sensor-generated data against 70% who do not.

other types of data)[15]. As the availability of sensor-generated data will increase in the near future, the possibilities for exploiting such data through analytics will also increase and this will drive further market development.

Another clear sign of rising interest in data sharing along the value chain and in the development of data ecosystems is the worldwide surge in availability of application programming interfaces (APIs), which provide controlled access to a company data[16]. Today there are more than 15,000 APIs published, and for instance "nearly two-thirds of telecom operators have launched or are developing APIs […] to grant large global brands access to non-sensitive customer data"[17].

Figure 2: Growth of APIs over time



Source: Ruben Verborgh, Ghent University – iMinds, See: http://rubenverborgh.github.io/WebFundamentals/web-apis/#web-api-growth

Although, according to our general survey, only 9% of data sharers are currently opening up their data with the objective of "fostering the creation of an ecosystem through open platforms," the trend towards an API economy is strengthening over time, as proven by the data collected through case studies and interviews[18]. In the financial sector for instance, allowing third parties to create new value-added services based on its data and foster an ecosystem culture have been strategic priorities for BBVA since 2013[19].

Despite this increasing interest in and awareness of the benefits of data flows across businesses, our general survey and the data coming from the recent European Data Market study[6] show that, **in general, companies that share and acquire data are still the exception rather than the rule**.

[15] From the specific survey, answers to the question "which kind of data does your company need amongst human-generated, sensor-generated, process-generated and other types of data?"
[16] http://nordicapis.com/tracking-the-growth-of-the-api-economy.
[17] http://www.forbes.com/sites/mckinsey/2014/01/07/ready-for-apis-three-steps-to-unlock-the-data-economys-most-promising-channel/#4ab71db89e5e.
[18] See for instance the Finance case study or the case study on industrial platform.
[19] Centro De Innovacion BBVA, Big Data - Now's the time to create business value with data: http://www.centrodeinnovacionbbva.com/sites/default/files/bigdata_english.pdf, 2013.

This is particularly true from the perspective of data sharers. Indeed, some of the barriers analysed through this assignment seem to particularly discourage businesses from sharing data. For instance, 17% of the respondents within the data sharer category said that contractual uncertainty is a blocking factor for them, preventing data sharing. In addition, for 41% this is a very important or considerable barrier[20]. Similarly, 50% of respondents consider uncertainty about data ownership and (re-)use of data as a considerable or very important barrier. Finally, from a data sharer perspective, the costs of sharing data are also not negligible and can influence the decision to open up the data: 66% of data sharers consider these costs to be a very important or considerable barrier[21].

Moreover, businesses might often prefer to protect their data and use them directly to provide value added services, rather than partnering or trading with third parties. One study recently found that most business respondents stated that they "prefer to have control over the development of new products and services. They frequently contract with third parties to help speed development, but full-fledged partnerships or alliances are still a relatively uncommon arrangement."[22] A further indication of this reluctance to trade data is that established companies often acquire start-ups in order to gain ownership of the data they hold. Even when considering big data start-ups, the vast majority of companies provide information or knowledge services, and only exceptionally provide raw data[23].

Examples from case studies

Within the financial sector, the adoption of the Payment services directive 2[24] (PSD2) forced banks to reflect on the question of data sharing. The PSD2 in fact mandates the opening of banks' APIs to third parties if the account holder provides consent (articles 66 and 67). Although extremely important for establishing a framework for exchange of data, it is worth mentioning here that the PSD2 applies to personal data (financial data of the account holder, hence categorised as personal) rather than the non-personal data covered by this assignment. There is a link between these two categories of data: some innovative banks[25] are already using the same API that they use to share and access the data of the account holders to share and access other datasets (e.g. aggregated data on number of money withdrawal for each ATM) in order to develop data ecosystems and to share aggregated data which do not enter in the realm of personal data anymore.

[20] The scale considered 5 possible responses: 1- Blocking factor, 2 – Important Barrier, 3 – Considerable Barrier, 4 – Small Barrier and 5 – Not a Barrier plus 0 – I do not know.
[21] Ibid.
[22] https://www.bcgperspectives.com/content/articles/information_technology_strategy_digital_economy_seven_ways_profit_big_data_business/
[23] Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2014). Big Data for Big Business? Cambridge Service Alliance Blog, 1–29. http://doi.org/10.1016/j.im.2014.08.008
[24] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=en
[25] See Annex 2 – Sectoral Case Studies

Confronted with the question raised by this new piece of regulation, which favours data openness and contributes to enhancing the financial data market, banks could decide to adopt different strategies:

- Comply with the regulation only: e.g. make the minimum effort to comply with the legislation and provide third parties with access to data through basic APIs;
- Facilitate and monetise access: e.g. allow more granular access to data (beyond what is prescribed by law) through more advanced APIs;
- Provide advice and new services: e.g. provide insights and analytics services through the API platform;
- Expand the ecosystem and aggregate value: e.g. create an ecosystem around the API involving other financial players and consumers, and customise their experience and the services provided to them[26].

Although the PSD2 serves as catalyst for the evolution of incumbents as it imposes an obligation it imposes on them, only a limited number of traditional financial institutions are embracing more than a 'pure compliance strategy' towards data sharing. This is the result of the 'wait-and-see' attitude mentioned above, coupled with the wish to protect data and have control over the development of product and services in-house.

Similarly, in the chemical sector, although companies have strongly embraced connected technologies inherent in the Internet of Things (IoT), including analytics, additive manufacturing, robotics, high-performance computing, artificial intelligence, cognitive technologies, advanced materials, and augmented reality, sharing of data is still limited. Indeed, chemical companies mostly rely on data analytics companies which can neither access nor (re-)use the data once they have finished the project covered by their mandate. This sector is therefore another example of a data-intensive value chain which has not yet opened up data.

The fact that the market is at an 'emergence stage' does not mean that the problems described in this report are not important or relevant. Quite the opposite, as argued during a webinar on "data access and data sharing: the real impact on SMEs' and start-ups' business models[27]" organised by the European Commission in May 2017, "Europe lost the race for the development of a competitive personal data economy and cannot afford to do the same with respect to the industrial data"[28]. Moreover, the market will eventually move to the 'breakthrough stage' anyway and this will cause more undesired effects if the barriers are not addressed.

[26] Accenture, *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive - PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*: https://www.accenture.com/t20160505T180127__w__/ca-fr/_acnmedia/PDF-15/PSD2-Seizing-Opportunities-EU-Payment-Services-Directive%20(1)%20(1).pdf

[27] See: Webinar on data access and data sharing: the real impact on SMEs' and start-ups' business models: https://ec.europa.eu/digital-single-market/en/news/webinar-data-access-and-data-sharing-real-impact-smes-and-start-ups-business-models

[28] See: Stakeholder Workshop on Sharing and Accessing data: issues for SMEs and start-ups - Summary of the discussion: https://ec.europa.eu/digital-single-market/en/news/stakeholder-dialogue-building-european-data-economy

Nonetheless, if one accepts that the European Data Market is still not yet fully mature, it is possible to apply market development theories to this domain to get some insights into the next phases of the data market and the possible remedies to the emerging issues.

Theoretical market development

The aim of the following sub-sections is to explain the development of markets from *infancy* to *maturity* in an abstract and rather theoretical way. This serves as a bracket and theoretical foundation for understanding the problems faced by companies and for the development of the policy objectives and policy options, which can accelerate the market development and the move from one phase to another.

Markets and industries often develop in the form of an S-curve. This is also valid for the digitisation of markets and industries.

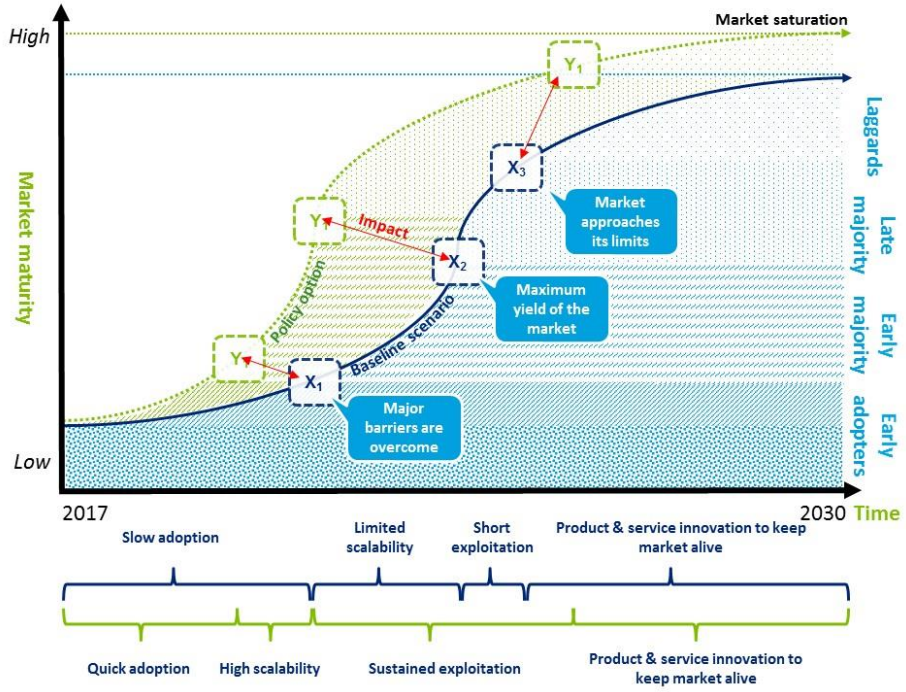
The S-curve concept

The concept of the S-curve first emerged as a sociological model in 1903 and was the work of Gabriel Tarde. According to Tarde, inventions spread through the process of imitation. With help of the S-curve, Tarde was able to map the spread of coffee in the late 19th century.

Multiple disciplines such as economics, physics and biology adopted the S-curve to explain different developments, for example to illustrate the spread of viruses or the growth of an embryo over time. In the context of this study, the model represents the lifecycle of a technology or innovation.

An illustrative, yet typical S-curve is shown in Figure 3.

Figure 3: Typical development of digitised market



Source: Deloitte

In the figure above, the x-axis (from left to right) and y-axis (from bottom to top) contain different types of information:

- The x-axis shows the **time**[29] (in this illustrative case from 2017 to 2030) which is a key variable in Impact Assessment studies; and
- The y-axis represents variables in relation to the maturity of the market.[30]

In addition, Figure 3 contains two different graphs:

- **Blue graph:** The potential market development in a (unspecified) industry under the baseline scenario[31]; and
- **Green graph:** The potential market development in a (unspecified) industry when policy option is in place[32].

Both graphs follow an illustrative S-shape and thus represent typical market development patterns. By comparison with the development of the market under the baseline scenario (as illustrated by the blue graph), the development of the market under the policy option (as illustrated by the green graph) is steeper and the market develops earlier.

These and other differences are explained in the following sub-sections on four distinct stages:

- Stage 1: Emergence;
- Stage 2: Breakthrough;
- Stage 3: Consensus; and
- Stage 4: Saturation.

Stage 1: Emergence

An S-curve typically starts from a situation where a technology is still at its very beginning.

Naturally, the emergence of a market is characterised by a **high degree of uncertainty** about a certain[33] technology's possibilities and challenges. This means that businesses and consumers alike are not yet fully aware of how the technology works, and how it could help and benefit *them* in their business and daily routine.

Thus, the adoption and usage of the technology is low and growing only at a slow pace which is represented in the blue graph by a low slope (i.e. low growth rates).

[29] The x-axis can, of course, also concern other (monetary) variables such as: amount of investments in specific technology; cumulative expenditures on research and development (R&D); extent to which technology is improved.
[30] This variable can e.g. be replaced by variables such as: degree of market digitisation; extent to which data is shared between businesses.
[31] The notion of a baseline scenario refers to future development without policy action from the European Commission apart from what is already planned.
[32] The concept of policy option refers to future development under the condition of (non-)legislative policy action from the European Commission.
[33] The concept of "certain" refers to an unspecified type of technology as S-curve developments can potentially be applied to any type of technology.

In this situation businesses that are not yet familiar with the technology can be expected to behave risk-aversely. This means that businesses will, if at all, only make small-scale investments as the challenges and barriers at this stage outweigh the benefits of the technology for them.

As market growth rates are low at this stage, individual businesses' investments are (in comparison to later development stages) relatively inefficient. The reasons for this are:

- Technical, legal, and/or other types of barriers may impede the development of sound and sustainable business models; and
- Technology has not (yet) been adopted by most other market actors.

Moreover, businesses can reasonably be expected to struggle with the prediction of the technology's future development – thus making it **uncertain whether investments at this stage would amortise over time**.

At this stage, (emerging) technology is typically used by *early adopters* – often start-ups spearheading the development of business models[34] – that can be characterised by their affinity with and open-mindedness about the technology (including its potential benefits, challenges, and drawbacks).

However, **most market participants remain cautious and uncertain**. Therefore, the market volume is still relatively small. This is due to a limited amount of imitation of the early adopters by most of the population.

At this stage, **EU action** could contribute to reducing this cautiousness and uncertainty on the part of market participants, e.g. by raising awareness of technology, as well as by mandating stakeholders to engage in discussions on how to overcome existing (technical) barriers. Moreover, EU funding initiatives (e.g. in the area of R&D) could contribute to overcoming existing barriers.

As illustrated by the green, policy option graph in Figure 3, this could contribute to generating higher market growth rates and accelerating the adoption of the technology (thus leading to a shorter and steeper S-curve).

This could, potentially, lead to higher market volumes in less time.[35]

Stage 2: Breakthrough

In an ideal situation, over time, the technology is expected to **overcome existing major technical, legal and other types of barriers** – either without or with EU intervention (see X_1 or Y_1 respectively in Figure 3 above). Technology is thus expected to break through into mainstream markets.

[34] Consumers can, of course, also be early adopters of technology. At this stage of the study, however, this is considered to be of less relevance.

[35] This is visualised by the green- and blue-hatched areas beneath X1 and Y1 respectively. The green-hatched area has a higher volume than the blue one.

In its further development process, the market in which the technology is used is expected to experience **steep growth** as more and more market participants *jump on the bandwagon* to implement technical solutions in order to reap the respective benefits for their own business (e.g. by becoming more efficient in their internal processes, and/or developing new goods and services).

Thus, businesses' inclination to invest capital in the technology is much higher than in stage 1 of the market development. This leads to an S-curve that is much steeper in stage 2 than in stage 1 of the development. In fact, each individual business's investment becomes increasingly efficient in stage 2 as the **return on investment increases due to the (technical) scalability of the market**.[36] This means that businesses are, ideally, able to realise large gains with limited investment, thus making it rational for them to invest as much as possible and reasonable in order to capture profits.

Consequently, an increasing number of market participants becomes less cautious and uncertain, leading to:

- Increasing innovation and development of new products and services;
- Higher adoption of technology;
- Faster and more wide-spread implementation of (sustainable) business models;
- Rapid expansion of outputs generated by the use of technology; and
- Increased consumption of the respective goods and services.

Moreover, technology-based companies are expected to experience steep growth, e.g. in terms of turnover, profits and staff. This leads to higher external company valuations.

Comparing the blue, baseline scenario and the green, policy option graph, an observation similar to stage 1 applies: **EU action could contribute to fostering economic growth** by setting legally binding (technical) market standards that form the base for future developments and innovation.

In stage 2, standardisation could contribute to maximising market volume and economic yield for market participants, while simultaneously accelerating the mainstreaming of technology (thus leading to steeper growth of and a higher volume under the green graph compared to baseline scenario and stage 1).

Stage 3: Consensus

At *some* point after the technology breaks through to mainstream markets, it becomes part of the **market *consensus***. This means that market participants agree on the usefulness and added value of the technology, e.g. for innovative products or services, or the development of their own business processes.

[36] This means that, e.g. as part of industry-lead standardisation processes, formerly innovative technical solutions slowly become part of the mainstream market.

During this stage, businesses achieve the **optimal combination of investment and return on investment**, i.e. the most efficient spot on the S-curve, characterised by the highest growth rate achievable in comparison with the least amount of investment necessary.

This point is marked as X_2 and Y_2 in Figure 3 and mathematically represents the turning point of the curve:

- From *today* (i.e. 2017) until the turning point, the S-curve is characterised by increasingly steep growth rates; and
- After the turning point, the S-curve is characterised by decreasingly steep growth rates.

This means that, after the turning point, **further investments become increasingly inefficient** for businesses, i.e. the marginal return on investment will decline over time. There can be several reasons for this.

For instance, the number of businesses providing technology-based goods and services is very high due to the efficient market development in stage 2. This can lead to intense competition among businesses for consumers and, potentially, to a race-to-the-bottom from a price perspective – thus decreasing businesses' revenue margins and their inclination/capability to invest in the same and/or different technologies or markets.

Another reason is that consumers are less willing to pay current prices for mainstream goods as they may have lost their innovative character to them. This decrease in consumers' willingness to pay, ultimately also results in a decreased inclination of businesses to invest.

However, as the **mainstreaming of technology** is still on-going, the market volume is still expanding. Thus, businesses face a trade-off decision between:

- Investing in new technologies and markets (e.g. by increasing their R&D expenditures or by acquiring other companies); and
- Exploiting the market as much as reasonable, simultaneously accepting decreasing revenue and profit margins.

Naturally, established market participants, such as large manufacturers or service providers, will follow both strategies with different types of products and services for different types of target groups.

Smaller firms and especially start-ups, however, can expect to face increasing pressure at this stage of market development as investors' inclination for providing equity finance decreases as well. In such a situation, ideally, smaller firms and start-ups sell their business model (and e.g. the underlying respective patents, data, services etc.) to larger entities that can cross-finance decreasing margins – or turn around their business model to more innovative technological opportunities that again offer increased growth potential.

In this stage of market development, **EU intervention** could e.g. take the form of R&D-related funding, or the revision of legislative requirements in terms of whether they are fit-for-purpose based on the experiences of stages 1 and 2 of the market development. In that

way, EU action could contribute to maximising the market volume for the remaining market participants while simultaneously safeguarding consumer protection standards.

Hence, most consumers by then accept the technology, so its innovative character and attractiveness to new customer groups are cooling off, with the result that the green, policy option curve covers a larger area underneath the curve, than its blue, baseline scenario counterpart.

Stage 4: Saturation

Ultimately, however, markets can – at some point — be expected to reach **saturation**. This means that marginal investments are inefficient (i.e. every additional euro of investment does not increase the return on investment) with no additional consumers purchasing the respective goods or services.

For businesses, it is key as part of this stage of market development – if they are still invested at all within the market – to **minimise investments in market- or technology-related innovation and to maximise replication or marginal improvements** to further exploit the market.

Although Figure 3 displays this period as relatively short, its actual length depends on the technology and its market circumstances. It is still possible to attract consumers who previously were extremely uncertain about paying for or unwilling to pay for the respective goods or services ('laggards') as the adoption by earlier consumers is seen as a guarantee of the reliability and credibility of technology-based products and services.

Within this stage, **EU action** could concern safeguarding consumer protection standards from bad business practices and market abuse (e.g. cartels), as well as attempts to illegally exploit the market by under-cutting agreed legislative standards (e.g. for product safety).

Depending on the market development in stages 1 to 3, the point at which market saturation is reached is expected to be higher under the green policy option curve than under the blue, baseline scenario curve. This can be explained by market participants, together with public authorities, actively shaping the market development in its early stages in order to be better able to exploit its potential later — while simultaneously safeguarding consumer protection rights.[37]

Different technologies, industries, and markets find themselves on different points of the S-curve. EU intervention can, potentially, accelerate the adoption of technology and contribute to maximising the market volume (revenue, profit, margins) for businesses while safeguarding potential detriments, e.g. environmental or consumer-related.

Most importantly, however, EU intervention is most effective when it is:

[37] Finally, technologies can also have negative slopes and minimal market volume after the market saturation. This becomes obvious, for example, in case a product becomes obsolete and replaced by another. Ideally, all respective businesses have divested before arriving at this point.

- Tailored towards the needs of the specific markets, industries, and their consumers (no one-size-fits-all approach); and
- In reasonable balance with progressive and cautious voices within these markets.

It is also important to recall here that most of the sectors and therefore most companies in Europe are to be found in the 'emergence' stage of the market. As mentioned in the previous section on the state of play, fewer than 10% of companies in Europe are already intensive data users. Some sectors and companies are nonetheless more advanced than others and have already moved to the 'breakthrough' stage. This is the case for instance of the automotive sector. This sector in fact already heavily relies data technologies (linked to the development of connected cars) and it has therefore already encountered a number of obstacles to be overcome[38].

Based also on this theoretical understanding, the next sections and chapters of this report examine the problems challenging further data sharing, access and (re-)use in Europe, in general, and per sector and market segment, and the specific or overall solutions which could lower these barriers.

[38] According to recent studies, the faster development of the automotive sector is linked to the need for car manufacturers to keep their competitive advantage in a very competitive market. See for instance: https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf

3 Problem assessment

This chapter contains the problem assessment of issues related to access and (re-)use of data, as well as liability, of IoT, robots and autonomous systems. This chapter also contains an analysis of how the problems, their causes and effects are expected to develop from now on (/'baseline scenario').

Introductory remarks and main findings

The purpose of this chapter is to elaborate on the problems, their causes, and effects businesses and citizens face today in relation to emerging issues relating to:

- Access and (re-)use of data; and
- Liability of IoT, robots, and autonomous systems.

For each of the above subjects, we have drafted a separate problem assessment in line with the Commission's *Better Regulation Guidelines.*

Although separated as part of the problem assessment, both areas are treated jointly as part of the chapters related to the development of policy options (chapter 4), as well as their assessment and comparison against the baseline scenario (chapter 5).

Each problem assessment contains a brief presentation of the problem tree, as well as the logical links between its elements. Moreover, we outline determinants for the types and magnitude of problems faced by businesses and citizens. This is followed by a detailed analysis of the problems for businesses and citizens, their causes, as well as effects.

Within its Better Regulation Guidelines, and especially within the Toolbox (see p. 83, #14: "How to analyse the problem"), the European Commission has provided a list of five issues (or rather questions) that "should be covered" in the problem assessment:

- What is the problem and why is it problematic (i.e. its negative consequences)?
- What is the magnitude and EU dimension of the problem?
- What are the causes ('drivers') and their relative importance for the problem?
- Who are the relevant stakeholders?
- How is the problem likely to evolve with no new EU intervention?

These questions are, however, not necessarily to be understood as a structure for the problem assessment but rather as guidelines for its content. The reason is that these questions are mutually interconnected and the specific answer to each question depends on the answer to another question.

For instance, as a problem and its magnitude, can e.g. be different for each type of stakeholder affected, a discussion of the problem and why it is problematic is inseparably linked to the question of who is affected by the problem and the causes of the problem.

Thus, from an analytical perspective, it is very useful to structure the analysis by means of a problem tree. While differentiating between the problem, its causes and effects, each box in the problem tree – as well as their connections – forms a separate entity for analysis (e.g. in the form of hypotheses that are tested). Within each of those smaller entities of analysis, the high-level questions identified by the *Better Regulation Guidelines* are subsequently answered to the extent possible. Nonetheless, Table 1 shows high-level answers to the questions identified in the *Better Regulation Guidelines*, together with the location of more detailed information in the report.

Table 1: High-level answers to questions in #14 of the Better Regulation Toolbox

<table>
<tr><th rowspan="2">Questions</th><th colspan="2">High-level answers</th><th rowspan="2">Detailed information</th></tr>
<tr><th>Access and (re-)use of data</th><th>Liability of IoT, robots and autonomous systems</th></tr>
<tr><td>What is the problem and why is it problematic (i.e. its negative consequences)?</td><td>Data sharing is impeded
This leads to undue costs for businesses
Businesses pass on their costs to consumers. Therefore, they pay unduly high prices</td><td>Uptake of IoT, robots and autonomous systems is impeded due to unexpected or unpredictable costs
Divergences in national liability regimes create market barriers for producers and service providers
Injured parties cannot count on availability of redress</td><td>See the sections on “the problem, its magnitude and the stakeholders affected”</td></tr>
<tr><td rowspan="2">What is the magnitude and EU dimension of the problem?</td><td colspan="2">The intensity and magnitude of the problem are different by industry sector and the relative position of a specific stakeholder in the value/production/use chain
At this stage, no quantitative assessment is possible due to limited availability of data and due to the emerging nature of the market
Costs of acquiring the right skills are transversal, applicable to companies with different maturity.</td><td rowspan="2">See the sections on “the problem, its magnitude, and the stakeholders affected”</td></tr>
<tr><td>Data monopolies and lack of competition linked to unwillingness of data holders to share data could also entail higher costs for businesses and consumers overall.
The evidence on the magnitude of the problem is contradictory:
General survey data seems to suggest that the problem is not very acute
However, the results of (some) interviews and workshops show that the problem is a major concern for specific types of company and business sector
The stage of data maturity of the company determines which type of costs are more relevant
Public administrations across the EU face costs, e.g.</td><td>Harmonisation of product liability law has occurred, but does not address the emerging issues of autonomy and complexity
The lack of harmonisation of other types of liability has caused market fragmentation; Member States adopt both differing extra contractual/tort rules and sector- specific rules. This increases the cost of introducing cross-border IoT/robotics products and services</td></tr>
</table>

Questions	High-level answers		Detailed information
	Access and (re-)use of data	Liability of IoT, robots and autonomous systems	
	linked to setting up specific platforms		
What are the causes ('drivers') and their relative importance for the problem?	• The problem is mainly caused by contractual and legal, but also by technical barriers. • Contractual and legal barriers are impeding the sharing, access and (re-)use of data in the EU but different barriers matter to different extent. Issues are more important for 'data users' than for 'data producers' • Barriers related to interoperability have a strong impact on data sharing, accessing and (re-)use, depending on businesses' position along the value chain and their size • Unequal bargaining power is very important for (smaller) stakeholders along the value chain • Issues related to the development and acquisition of skills, as well as devising appropriate economic value data, are widespread across companies and sectors	• There is uncertainty around the suitability of current liability legislation • Emerging challenges are not considered consistently: ○ Non-deterministic autonomy (i.e. self-learning and self-modifying characteristics) are not considered ○ Complexity of IoT and robotics products creates evidentiary barriers that threaten the effectiveness of compensation regimes	See the section on "causes of the problem"
Who are the relevant stakeholders?	• The problem affects both businesses, especially SMEs, and consumers • Consumers are a crucial type of stakeholder as they are directly affected by the problems businesses face		See the sections on "the problem, its magnitude, and the stakeholders affected"
	• With regard to businesses, their position in the data value chain, their size (SMEs vs. large enterprises), as well as the industrial sector in which they operate are crucial • More specifically, the following types of affected stakeholders can be distinguished:	• The following types of affected stakeholders can be distinguished: • The producers, i.e. the entities that manufacture an IoT device, robot or autonomous system • Service or product providers who will offer a product or service in the market consisting of or	

Questions	High-level answers		Detailed information
	Access and (re-)use of data	Liability of IoT, robots and autonomous systems	
	○ Players co-producing data: product/service providers and users ○ Players interested in accessing data: providers' competitors and same-sector downstream providers ○ Players interested in re-using data: data analytics companies and (re-)users of public interest data	using robot, autonomous or IoT devices • End-users who buy a robot or device as end-users (without the intent of building their own product or service around it), or those who use a robot or device without necessarily owning it. • Injured parties, i.e. those that suffer harm in relation to the use of a robot or device.	
How is the problem likely to evolve with no new EU intervention?	• It is expected that: ○ Contracts will continue to be the main vehicle for sharing and accessing data. ○ Contractual barriers will be solved on a case-by-case basis, thus leading to dispersed approaches towards similar legal concepts and to the persistence of unequal bargaining power between parties ○ Technical barriers will be addressed at the industry and sectoral level but at different speeds in the different sectors ○ Based on standard economic theory, this could result in consumers paying higher prices than needed	• It is expected that: ○ Businesses will continue to take a case-by-case approach to liability through their contractual arrangements within the boundaries of the 1985 Product Liability Directive ○ Injured parties (especially consumers) will face difficult access to compensation for liability	See section on the baseline scenario: The likely development of the problems

Source: Deloitte

Limitations relating to the findings of this study

As mentioned in chapter 1, the data collection was hampered by the fact that the markets considered are still at the "emergence" stage. This applied in particular to our ability to quantify the evidence relating to the barriers identified. Thus, the findings of this section should be considered as a first attempt at examining this topic and gathering the existing data on these subjects. This analysis is based on the limited data available and provides a preliminary (mainly qualitative) overview of the main problems, their causes and effects.

Access and (re-)use of data: The problem, its causes, and effects

This section contains the problem assessment of issues relating to the access and (re-)use of data.

After a brief presentation of the problem tree, as well as the logical links between its elements, we outline determinants for the types and magnitude of problems faced by businesses and citizens. This is followed by a detailed analysis of the problems for businesses and citizens, their causes, as well as effects.

Problem tree: The logical links between the problem, its causes and effects

Key messages:

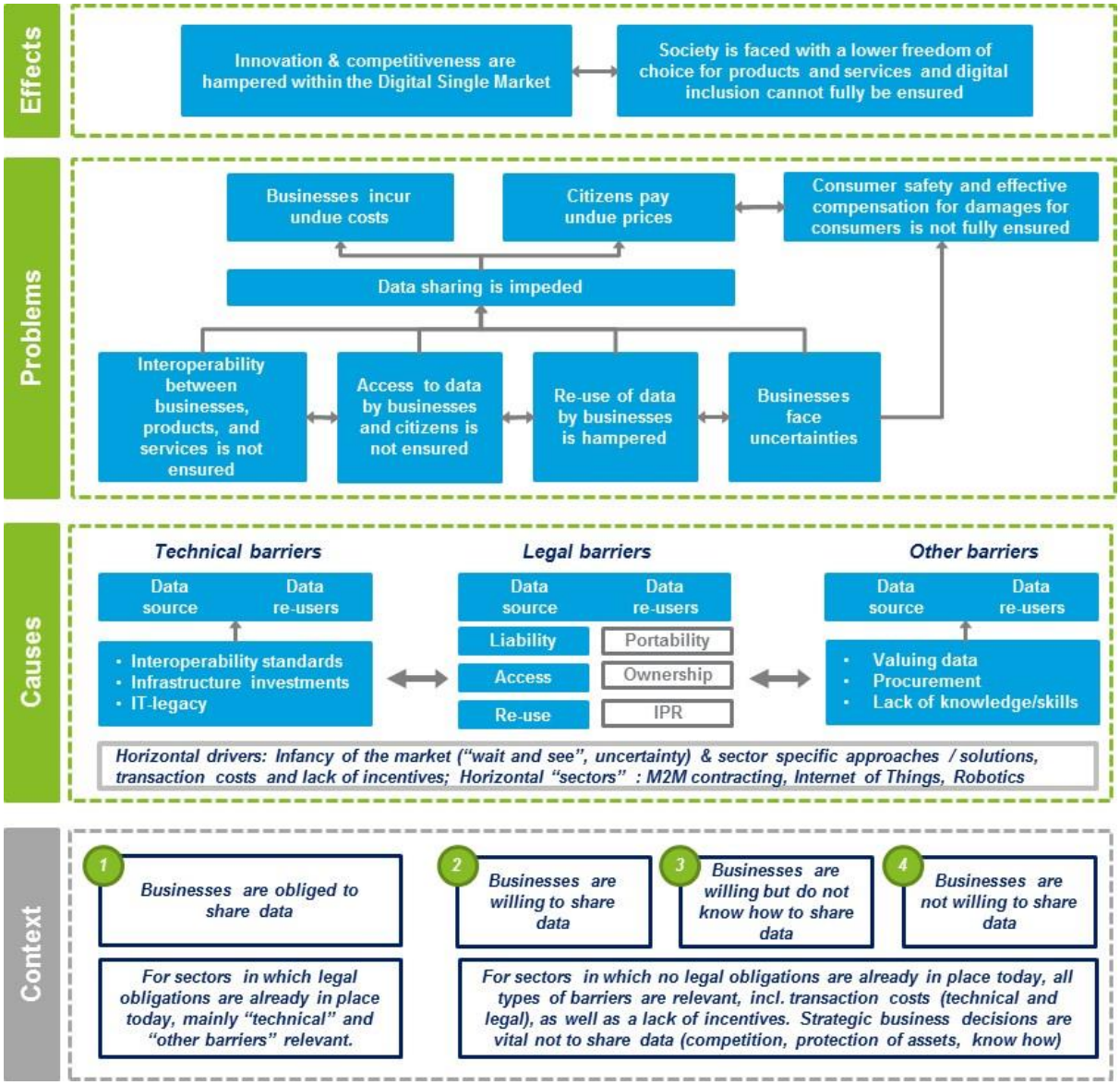
- The main hypothesis of this study is that there are a number of technical, legal and other barriers which are impediments to B2B data sharing, access and (re-)use in Europe.
- This leads to certain problems affecting business and consumers.
- Different companies will face different barriers in the data market and this is why the analysis of the context (e.g. the stage of market development of the company/business considered) and preconditions (e.g. the sector, position in the value chain and size of the company) are also important elements for a sound problem assessment.

The main hypotheses underlying this study are a number of legal, contractual and technical barriers relating to data ownership, interoperability, (re-)usability and access to data, and liability are impeding B2B data sharing and access in Europe. This means that these barriers are the causes of problems for businesses, and thus can have a negative impact on the Digital Single Market and EU society:

- Data ownership *matters*;
- Interoperability *matters*;
- (Re-)usability of data *matters*;
- Access to data *matters*; and
- Liability issues *matter*.

The data collection and analysis carried out as part of this study made it possible to carry out a 'reality check' of the initial understanding of the existing problems, their causes, and impacts. This understanding is depicted in the figure below.

Figure 4: Our understanding of the problems related to data access and sharing, their causes, and impacts (problem tree)



Source: Deloitte

The problem tree should be read from the bottom to the top.

At the bottom of the figure, contextual information is provided with respect to differences between sectors in which legal obligations to share certain types of data (personal or non-personal) are already in place (e.g. in banking and financial services, where the Payment Services 2 Directive requires incumbents to share their client data with authorised third par-

ties[39]) while in other sectors no such obligations exist (e.g. agriculture, machinery or chemical sector). The main reason for this distinction is that the significance of *the different barriers can change according to the cases considered*. For instance, if there is an obligation to provide the data in place, businesses interested in these will face fewer access problems but possibly more technical issues. They fall into the 'type 1' category, unless they wish to have access to more data than those that are opened up by law[40], in which case they fall into the next category. Businesses willing to access and (re-)use data within sectors that are not governed by such legal obligations can face a wider range of technical, legal, and other barriers, including barriers to accessing the data itself.

From the data sharer perspective, we then distinguish between businesses that are willing to share and do share data even in the absence of any obligation ('type 2'), businesses that are willing to share data but do not know how to do it ('type 3'), and businesses that are not willing to share data ('type 4').

For each of these four types of business, different types of barriers will also differ in importance depending on the sector they are in.

Specific sections are devoted to the problems, their causes, and effects below. In these we examine these more closely and provide illustrative evidence from the case studies carried out for this study. This illustrative evidence is in text boxes for greater clarity.

Naturally, the analysis focuses on problems for existing business models.[41]

Determinants of the type and magnitude of problems

Key messages:

- There are three, equally important, preconditions that can help determine the types of barrier a company is likely to face in the data market:
  - its position in the value chain;
  - its size (SMEs versus larger companies); and
  - the sector it is in.
- In terms of position in the value chain, companies can fall in the data production, data access or data (re-)use category. Each of these categories has its own characteristics in terms of needs and risks within the data market, thereby resulting in certain barriers being more or less significant.

It is argued here that the problems and the likely effects for businesses from the barriers to the emerging data economy are strongly dependent on the conditions below:

[39] The Payment Services 2 Directive concerns the sharing of personal data rather than non-personal data. Nonetheless, this legal framework has a wider effect on data flow as personal data are used in aggregated form in the financial sector thus also becoming non-personal datasets.

[40] See for instance the case of the after-market car repairers.

[41] It is also important to keep this in mind for the assessment of current opportunity costs and the impacts of the policy options, e.g. in relation to the access to data. As it cannot be anticipated what types of business models would evolve if access to data were easier, the assessment of opportunity costs and impacts at a later stage of the project will be limited.

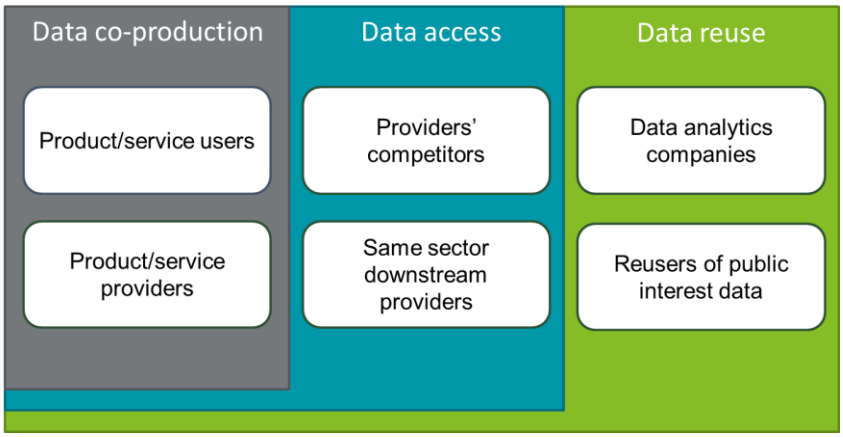
- The positioning of the firm in the data value chain;
- The size of the company; and
- The industrial sector in which it operates.

For each company willing to access or share data, the combination of these elements can determine the types of problems to be faced. Each of these important elements is detailed below.

Position of companies in the value chain

By using stakeholder mapping, it is possible to position company categories along the value chain and identify the effects for the different players.

Figure 5: Data economy stakeholder map



Source: Deloitte

As the figure shows, from the business perspective there are three main categories of stakeholder involved in the data economy:

- **Players co-producing data**: Product/service providers and product/service users;
- **Players interested in accessing data**: Providers' competitors and same sector downstream providers;
- **Players interested in re-using data:** mainly data analytics companies and (re-)users of public interest data although other categories of stakeholder (e.g. universities, statistical offices etc.) might be interested in re-using data etc.)

Firstly, there are the **players directly contributing to the production of data**. These are typically the service or product provider and the user of the service: a social network and its user, a tractor manufacturer and the farmer, cars and drivers, airlines and engine producers. **These parties are indispensable for the production of the data in the first place and have, de facto, a different degree of control over the data.**

In most cases, it is the product/service provider who retains the greatest degree of control over the data (as the provider 'owns' the data by means of full access to it), and the user has more limited control: for instance, the farmer over the data generated by the sensors, or the bank client over its transaction data. However, in some cases, the product user retains

greater control: for instance, in the aviation sector, manufacturers of aircraft components very often do not have access to their engines' data after they sell them[42].

The pure debate over 'data ownership' affects these two types of player and obviously, the market power of the different players matters in this contractual relationship, as it can help tip the scales in favour of one or another player. The players co-producing data are also the most relevant 'data sharers', whose reasons for sharing or keeping data have been analysed by this study.

The second category of economic actor is made up of **those players (most often in the same value chain) that need the data for their business**. Typically, they are competitors of the service producer needing access to the data in order to deliver their services, as in the case of banks-payment service providers as defined by the Payment Services Directive 2[43]. In addition, they can be players downstream or upstream in the same value chain: for instance, independent car repairers who need access to the data from the car in order to be able to provide the services. **These players do not participate in the production of data but need access in order to ensure a level playing field for competition, and allow for business model innovation**. Therefore, the question for these players does not revolve around 'ownership' itself but rather around the issue of access to data and the terms and conditions of access. This category of players suffers the most from lack of access to data as their business model is conditional on the availability of these.

The third category of economic actor **includes players outside the sector, who could benefit from enhanced access and (re-)use.** For instance, data analytics companies have access to the data of their clients, but cannot aggregate it and (re-)use it – this issue was detected in various sectors, such as manufacturing, automatic translation and retail. Since data aggregation from many sources is a prerequisite for developing artificial intelligence solutions, data analytics companies cannot develop innovative products and services because they do not have the right to (re-)use the data. Last but not least, data scientists could make use of data held by private players to address public interest issues and societal challenges, as also shown by the ongoing debate on "access to data for reasons of public interest"[44]. For instance, statistical offices might have a strong interest in re-using aggregated mobile phone

[42] See Annex 2 – Sectoral Case Studies

[43] See Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

[44] See for instance the Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on "Building a European Data Economy", SWD 2017/2 Final, https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy or the workshop on access for public bodies to privately-held data of public interest, held in June 2017, https://ec.europa.eu/digital-single-market/en/news/workshop-access-public-bodies-privately-held-data-public-interest

data held by telecommunication companies in order to provide more accurate mobility statistics[45].

It is important to note here that companies can be at the same time service/product providers and same-sector downstream providers, depending on the section of the value chain considered. For instance, engine manufacturers in the aviation sector fall in the data access category when they sell an engine to an airline company but they are product/service users when they buy specific components from subcontractors. The model should therefore be applied on a case-by-case basis to disentangle the relations between players

The table below presents an overview of the relevance of the main barriers for these different categories of player. Each of these problems is described in the following sections.

[45] See for instance the work carried out by Statistics Netherlands (CBS) on mobility statistics developed through usage of mobile phone data: https://www.cbs.nl/NR/rdonlyres/4EDB51ED-927A-4A69-B8F3-4DC57A44DDE4/0/Timepatternsgeospatialclusteringandmobilitystatistics.pdf

Table 2: Summary of most important problems per stakeholder category

Stakeholder	Legal uncertainties	Data Ownership	Access to data	Data (re-)use	Liability	Data portability	Interoperability	Skills	Valuing data	Unequal bargaining power	Cost of data
Product/service users											
Product/service provider											
Providers' competitors											
Same-sector downstream provider											
Data analytics companies											
(re-)users of public interest data											

Source: Deloitte

Although the value chain position of the companies helps in identifying specific barriers that can apply, as shown above, this is not the only factor determining the types of barriers businesses face. Company size and sector also matter.

Company size and sector

The **size of the company and its relative market power** are another determinant. The main distinction is between SMEs and larger companies[46]. Both categories are interested in data sharing and access. The general survey conducted by the team reveals that more than 50% of the respondents are interested or active in both sharing and accessing third party data. However, bigger companies, which are usually dealing with more information, seem to be currently more active in sharing data than SMEs. Around 37% of large companies are interested and/or active in data sharing only, while for SMEs this is the case for fewer than 20% of respondents. The reasons might be lack of resources for SMEs to dedicate to this domain, or lack of knowledge and skills.

In general however, when they are active in the data market, both SMEs and large companies usually share data for free. 50% of SMEs and 60% of large companies declare that they share data without charging although the general survey does not differentiate as to whom they share data with (e.g. analytics companies, other companies) or why. For instance, as part of its business strategy, BBVA grants access to a number of different aggregated datasets and a sandbox[47] for free through its API platform and just requires subscription if the data is processed and re-use outside the sandbox environment[48].

From different interviews and from the case studies, it emerged that sharing data for free might help companies be perceived as developer friendly and to build an ecosystem around them, fostering the development of apps related to their products and services, and thus ultimately benefiting from data openness. This is very often the case for transport or energy companies, which might have a strong interest in seeing the development of mobility apps or smart home apps based on their data. Legislative measures such as the French *Loi du 7 octobre 2016 pour une République numérique*[49] can also further incentivise or even oblige companies (and especially publicly owned companies or mixed capital companies) to open up their data[50].

---

[46] Companies with up to 250 employees are defined as SMEs. Large companies are those with more than 250 employees. See definition of the European Commission: http://ec.europa.eu/eurostat/web/structural-business-statistics/structural-business-statistics/sme

[47] A data sandbox can be defined as:" scalable and developmental platform used to explore an organization's rich information sets through interaction and collaboration", see: https://www.techopedia.com/definition/28966/data-sandbox-big-data

[48] See: https://www.bbvaapimarket.com/home

[49] See: *Journal Officiel* of 8 October 2016, LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (1), https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&dateTexte=&categorieLien=id

[50] Extension of the Directive on the (re-)use of public sector information 2013/37/EU (PSI Directive) to data held by public undertakings and private companies funded by the public sector is under consideration.

On the other hand, about 15% of companies, SMEs and large, are sharing data both for free and at a cost. Sometimes, the level of access depends on the subscription model. In the case of BBVA for instance, the unlimited access to the data comes at a cost while using the data only within the sandbox is for free.

However, some data can be accessed only upon payment. These data are acquired from companies of all sizes but more established players are clearly at an advantage as they can pay higher prices for this. Indeed, although the costs for sharing and accessing data seem to be more or less the same for businesses of different sizes, SMEs and start-ups might suffer more from higher technical and legal costs when these apply, as suggested by the data gathered through the case studies and interviews. Moreover, unequal bargaining power is definitely a greater risk for SMEs than for larger players. In the table below, we illustrate which barriers are more frequent for SMEs.

Table 3: Summary of most important problems for SMEs

Types of SME	Legal uncertainties	Access to data	Interoperability	Skills	Valuing data	Cost of data	Unequal bargaining power
SMEs sharing data							
SMEs accessing data							

Source: Deloitte

As mentioned above, the size of a company can be a factor determining the type of barrier it will face in sharing and accessing data, but this element must also be understood in the context of the company's sector and position in the value chain, as these three elements are equally important. For instance, SMEs might suffer less from unequal bargaining power in certain sectors (e.g. financial sector) because a legal framework is in place.

Therefore, our third and last hypothesis deals with the differences across sectors which might determine the relevance and extent of certain problems and effects. Indeed, as also emerged from the case studies, different sectoral conditions play a role in the existence and importance of technical and legal barriers to accessing and sharing data. For instance, technical interoperability is a major issue in the financial sector while less so for chemicals. Similarly, the question of access to data for providers' competitors and same-sector downstream providers is crucial in the automotive sector (as exemplified by the case of the car repairers) while less so in the aviation sector.

The general survey also provides additional insights into the differences across sectors. For instance, virtually all the companies operating in the health sector are willing to share (or interested in or active in) sharing their own data while this does not apply to all other sectors. Additionally, companies operating in transport and logistics are more often selling data (shared at a cost): 21% of companies in the transport and logistics sectors against an average

of 5% in the other sectors. However, the input from the general survey is not statistically representative enough to derive generalisations for each of the sectors and these data must be read in conjunction with the findings of the case studies.

To provide an overview of which barriers are relevant for which sectors, we first provide below a table that indicates with colour coding the extent to which the problems, their causes, and effects were important to the stakeholders interviewed[51]:

- **Dark blue cells** denote challenges that were identified in the case studies as very important for the sectors:
- **Blue cells** denote challenges that were of medium importance for the stakeholders interviewed as part of the case studies; and
- **Light green cells** denote challenges that seemed to be of minor importance for the interviewees.

Blank cells denote points that were not critically discussed (or not seen as a challenge) with the stakeholders in the different sectors.

[51] In addition, the Annex contains a more comprehensive table with information on the types of challenges encountered in the different types of sectors

Table 4: Importance of problems, their causes, and effects in the case studies

	Agricul-ture	Chemi-cals	Automo-tive	Energy	Retail	Telecoms	Financial services	Mobile health	RTLS[52]	Platforms	Aero-space	Machin-ery
Effects												
On Digital Single Market												
On society as a whole												
Problems												
Data sharing is impeded												
Undue costs for businesses												
Undue prices for consumer												
Causes												
Technical barriers												
Legal barriers												
Other barriers												
Horizontal causes												

Source: Deloitte

[52] Real Time Location Services, see Annex 2 – Sectoral Case Studies

Taking into account all these hypotheses and preconditions, the next section provides an analysis of the causes, problems and effects presented in the problem tree.

The problem, its magnitude and the stakeholders affected

This section discusses the existing obstacles for businesses and society in the Digital Single Market. At the most basic level, the technical, legal, and other barriers identified above lead to the following observations on problems:

- Interoperability between businesses, products, and services is not ensured;
- Access to data by businesses is not ensured;
- Businesses face uncertainties; and
- (Re-)use of data by businesses is hampered.

Data have no value in themselves, only at their point of use. To deliver value, data need to be mixed and merged with other datasets. The most innovative applications come from unpredictable usage of existing data. The data holder is not always best placed to extract value from data: this player could lack the skills, the culture or the incentives to deliver innovation. In other words, as an academic article put it already back in 2011 "the coolest thing with your data will be thought of by someone else"[53]. It is therefore important to understand which specific problems the issue outlined above cause.

Impediments to data sharing

Key messages:

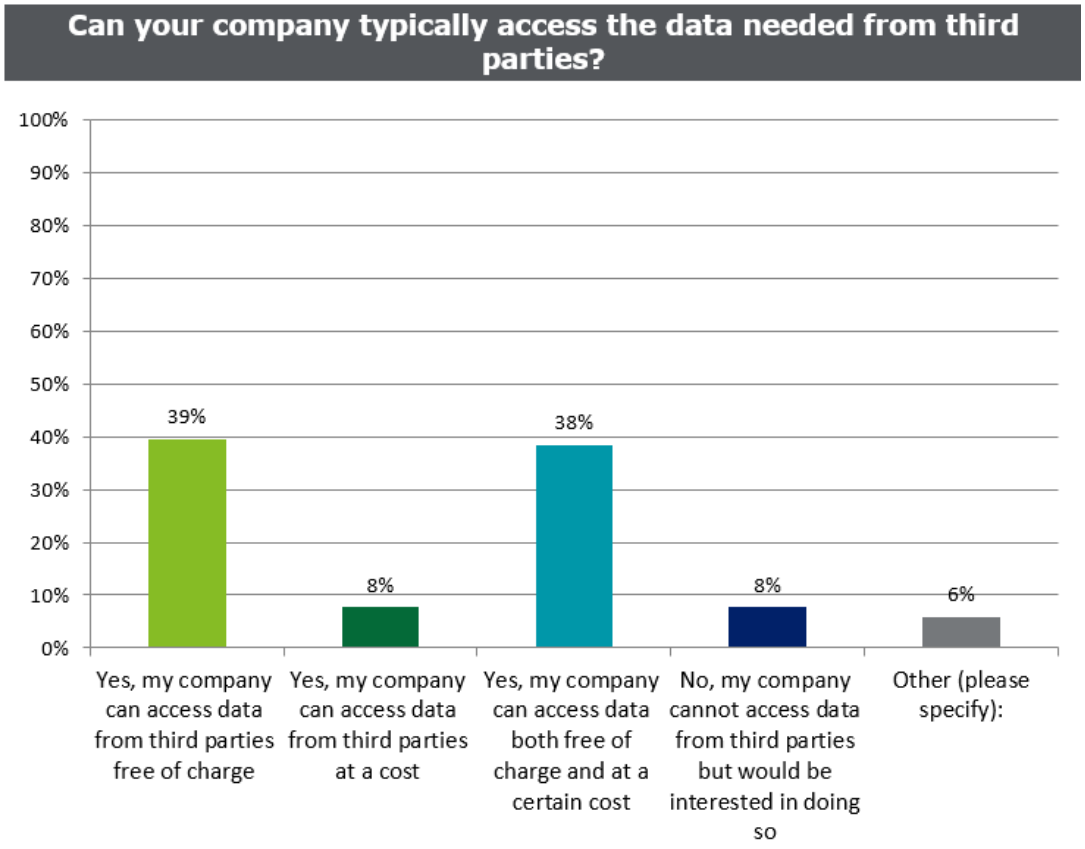
- As a result of all the barriers analysed, data sharing in Europe (and therefore the possibility of accessing data) is limited.
- However, the evidence on the magnitude of this problem is very contradictory: on the one hand, the general survey data seems to suggest that the problem is not very acute, while, on the other, interviews and workshops provided evidence that this is a major concern for a number of companies.
- The contradiction in the data can be explained in different ways:
  - Surveys report declared behaviour while other data refer to actual behaviour
  - The problems are of concern only to the limited number of intensive data sharers in Europe
  - The intensity of the problem depends on sector and position in the value chain.

In terms of the extent to which there are impediments to data sharing and the limits on the access and (re-)use of third parties' data, there is no unanimity on the magnitude and impact of this problem on the data economy. If one considers only the companies' answers to the

[53] See: Pattern, David, Stone, Graham and Ramsden, Bryony (2011) "The coolest thing to do with your data will be thought of by someone else". In: Business Librarians Association Conference. Making an impact: demonstrating value, 13-15 July 2011, Sheffield. (Unpublished) and Rufus Pollock (Open Knowledge Foundation) http://m.okfn.org/files/talks/xtech_2007/

general survey, the problem seems very limited. In fact, 85% of respondents[54] to the general survey carried out by the study team implied that **their businesses do have access to the data needed**, either for free or at a cost, as shown in the Figure below.

Figure 6: Access to data

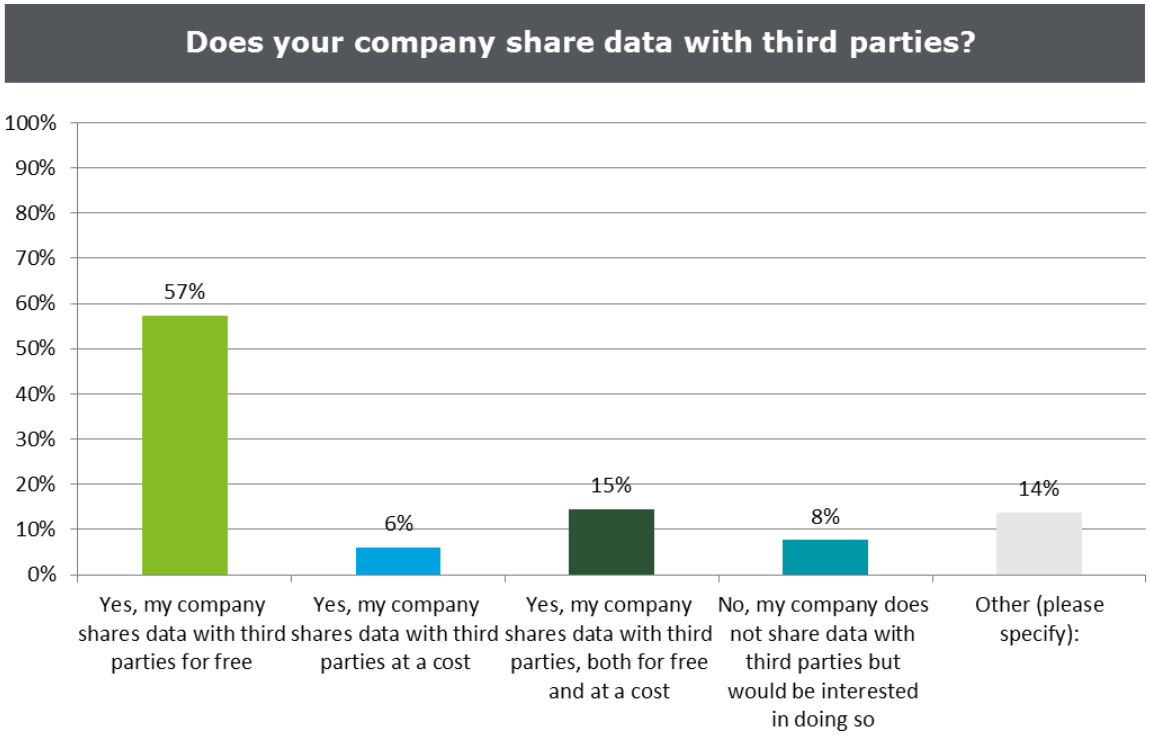


Source: Deloitte, General Survey

Moreover, the vast majority of companies (78%)[55] stated that they do make their data available to third parties.

[54] 85% is the sum of all respondents suggesting that a) they have access to the data for free (39%), they have access to the data at a cost (8%) or they have access to the data both free of charge and at a certain cost (38%).
[55] 78% is the sum of all respondents declaring that their company a) shares data for free (57%), b) shares data for a cost (6%) and c) shares data both for free and at a cost (15%).

Figure 7: Sharing of data

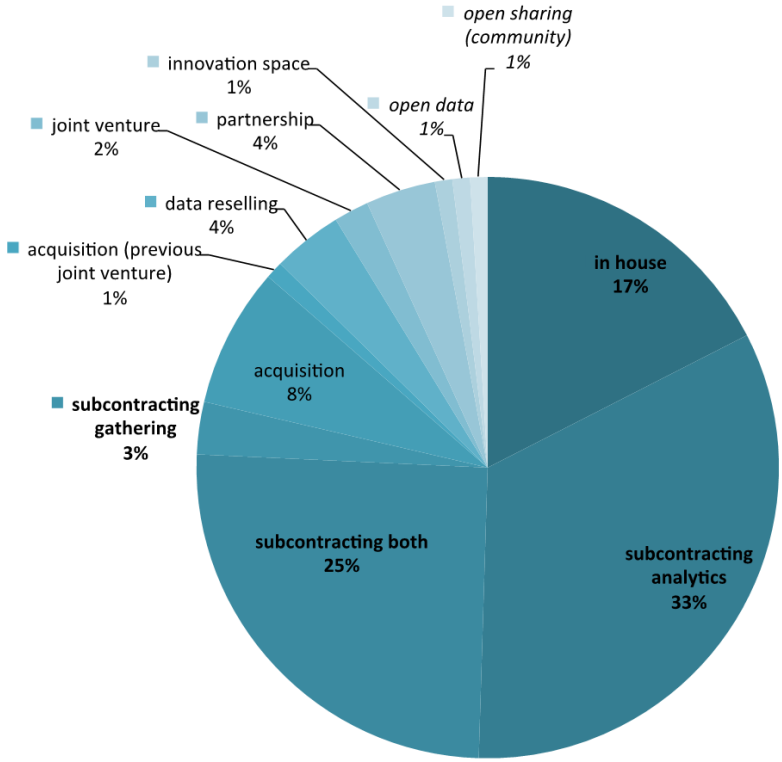


Source: Deloitte, General Survey

Yet when looking at the actual behaviour of companies implementing big data solutions, the picture is different and data sharing appears to be very rare. As can be seen from the Figure below, the vast majority of the data-sharing models of 100 businesses analysed as part of this study[56] (78%) can be characterised as 'closed', while 20% can be regarded as 'shared' and only 2% as 'open'.

[56] See First Interim Report

Figure 8: Distribution of data sharing models in the selected cases



Source: Deloitte, analysis of business models

The contradiction between the two sets of findings can be attributed to several factors.

First, the survey asked about declared behaviour, in particular with regard to data sharing, while the 100 business cases analyses looked into actual behaviour.

Secondly, the business cases analysis only looked at leading examples across sectors, while the survey covered a more representative sample of companies. Since we know that only 6% of EU companies are intensive data users, we can conclude that limited data sharing is not a major issue for the majority of companies, but mostly for the most innovative ones. And since the increasing adoption of big data solutions is expected and even pursued by policy measures, we can expect the problem to grow in the future.

Finally, as explained in the previous sections, the magnitude of this problem might depend to a very large extent on the position of the stakeholders along the value chain. Data users for instance are particularly impacted by this problem. This is especially true of those operating in the automotive sector. On the other hand, the problem might be less relevant for data users in other sectors with different market conditions (e.g. financial sector, chemicals, aviation).

Evidence from case studies:

As exemplified by the independent car repair aftermarket situation, players positioned downstream in the value chain and who have not contributed at all to the production of the data are the most affected by this problem which touches upon their vital interests. As mentioned in the previous chapter, this finding applies to different sectors to a different

extent. Indeed, in the automotive sector the problem is particularly acute due to the characteristics of the value chain (car manufacturers are competitors of the independent car repairers in aftermarket services). The issues is less acute in the aviation and machinery sectors. In fact, this problem was not found to have the same vital impact in other domains that it does in the automotive sector. However, this could also be due to the level of technological development of the automotive sector, making it a precursor in this respect.

Given these contradictory data, it is difficult to establish the magnitude of this problem in general. However, it seems reasonable to argue that **this is not a pressing problem for the vast majority of companies** (as suggested by the general survey), **but that the situation can be very different for different types of companies and across different sectors.** In this respect, the situation in the automotive sector is particularly critical.

Businesses incur undue costs

Key messages:

- Because of the barriers illustrated in the previous sections, companies incur many different types of cost when willing to share, access and (re-)use data.
- It is impossible to assess the magnitude of these costs because very little data is available and due to the 'emergence stage' of the market. However, it was possible to identify the most relevant cost categories.
- The general and specific surveys provide contradictory data on the costs companies bear. This might lead to think that the data maturity of the company determines which types of cost are more relevant.
- Costs of acquiring the right skills seem to be the most transversal type of costs, applicable to companies with different degrees of maturity, and both sharing and accessing data.
- Administration costs are also quite cross-cutting, while other types of costs are more specific to the value chain position or maturity of the company.

There is little information on the magnitude of costs incurred by businesses because of the barriers identified. Below, we present some information by way of example, coming from the general survey, in terms of categories and magnitude of relevant costs.

With respect to the categories of costs related to the technical, legal and other barriers to data sharing, accessing and (re-)use, **once again the general and specific survey provide contradictory information**. The general survey suggests that, *for companies willing to access and (re-)use data*, the most important costs are:

- Costs of technical implementation (very high for 2% and high for 37%);
- Costs of acquiring the right skills (very high for 3% and high for 24%); and
- Administration costs (very high for 4% and high for 19%).

On the other hand, according to the specific survey, for companies accessing and re-using third party data, two categories of costs seem to be the most impactful:

- Costs of buying data (very high for 76% of respondents and high for 14%)[57]; and
- Costs of legal advice (high for 94% of respondents)[58].

However, the costs of administration and the costs of acquiring the necessary skills come not far behind with 81% of "high" responses (for the administration costs) and 81% of "high" or "very high" answers (for the costs related to skills)[59].

Therefore, when looking at random European companies (general survey) or more data intensive users (specific survey), there seem to be many differences in terms of the costs these different types of businesses bear. The respondent to the general survey which might not have started using data intensively need to first establish the right conditions for doing so. This entails acquiring the right skills and the right technical material as well as bearing some administrative costs for the projects to start.

On the other hand, quite logically, for intensive data users the question of buying the data and the legal advice are more relevant, as these companies are already in the implementation phase and already have the basics in place. Moreover, as the percentages suggest, the issue of costs is far more impactful for intensive data users than for average European companies. Therefore, although to some extent contradictory, the evidence suggests that **cost types and their impact depend on the level of data maturity of the company considered.**

Similar contradictions emerged from the analysis of the general and specific surveys' insights from *data sharers*. The data from the general survey show that the most important categories of costs are:

- Costs of technical implementation (very high for 9% and high for 31%);
- Costs of acquiring the right skills (very high for 3% and high for 30%); and
- Administration costs (very high for 6% and high for 20%).

According to the specific survey on the other hand, the most important categories of costs are:

- Costs of acquiring the right skills (very high for 17% of respondents and high for 41%)[60]; and
- Administration costs (with 8% of very high responses and 42% of high)[61].

Therefore, technical implementation seems to be a major cost for the respondents to the general survey possibly only starting to share data but less so for intensive data sharers. This could, once again, be linked to the need to put the basics in place before starting to share data regularly.

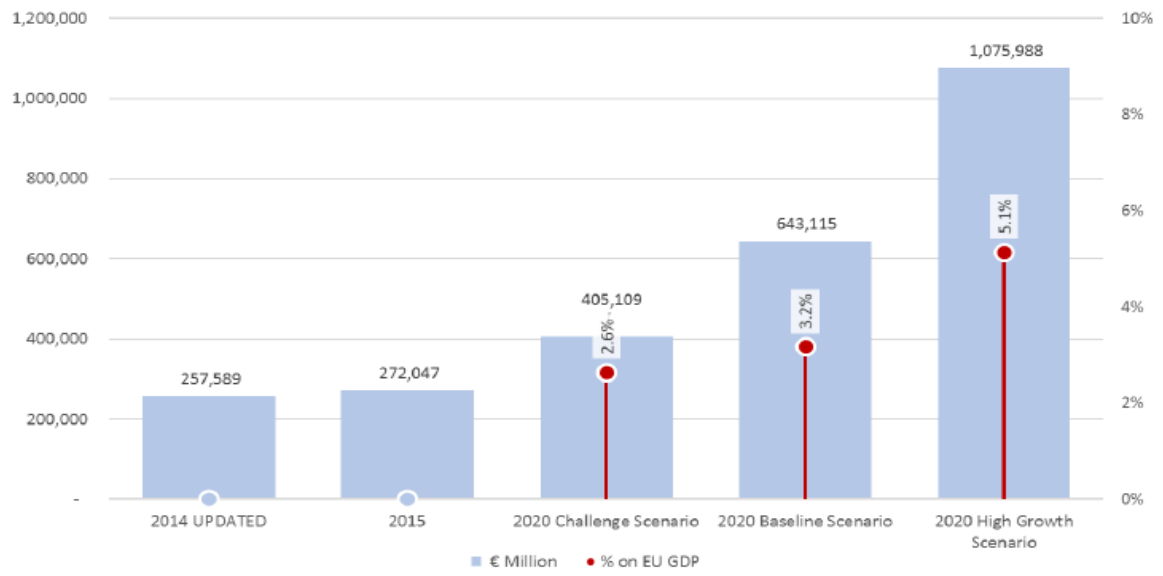
Interestingly enough, the question of acquiring the right skills seems to be a major cost for businesses situated all along the data value chain, and both for companies only starting with

[57] Results of the specific survey
[58] Result of the specific survey
[59] Ibid.
[60] Ibid.
[61] Ibid.

data driven projects and intensive data users. This confirms the analysis of IT skills shortage carried out within the framework of other European Commission initiatives[62]. Similarly, administration costs apply quite horizontally to different types of firm.

Although these macro categories of costs borne by data sharers and users can be immediately identified, their precise magnitude is difficult to assess. As shown in the figure below, a recent study carried out for the European Commission has estimated that the data economy and data market in Europe could be worth up to EUR 1,075 million by 2020 in a high growth scenario, EUR 643 million in a medium growth scenario and EUR 405 million in a low growth scenario[63].

Figure 9: Measurement of the data economy



Source: IDC and Open Evidence study, see p. 30, Second Interim Report, European Data Market Study, June 2016, http://www.datalandscape.eu/study-reports

In parallel, it has been estimated that the top 100 EU companies could save up to EUR 425 billion per year through further exploitation of (Big) data.[64] Despite a lack of further, more detailed, quantitative estimates, these can be used as an approximation for the magnitude of *annual* undue costs that EU businesses incur in the current situation due to the barriers identified in the previous sections. The actual figure is, however, expected to be even higher than EUR 425 billion per year as this estimate only refers to the top 100 EU manufacturing companies and thus excludes SMEs, as well as businesses from other sectors.

[62] See for instance the Digital Skills and Job Coalition initiative: https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition

[63] See p. 30, *Second Interim Report, European Data Market Study*, June 2016, http://www.datalandscape.eu/study-reports

[64] See: European Political Data Centre (EPSC) strategic note 'Enter the data economy': https://ec.europa.eu/epsc/publications/strategic-notes/enter-data-economy_en; European Commission (2016), The EU Data Protection Reform and Big Data, http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf.

The economic value of sharing data can be further illustrated by an estimate relating to the eGovernment plan that will also connect business registers across Europe, ensure different national systems can work together, and that the 'once only' principle applies to the input of data to public administrations by businesses and citizens. The European Commission has estimated that this approach to businesses and citizens sharing data with public authorities will potentially save around EUR 5 billion per year by 2017.[65]

Moreover, as part of its Communication on Digitising European Industry[66], the European Commission has estimated that adding services to the portfolio of manufacturing companies' smart connected products could lead to an increase in profitability by up to 5.3% and in employment by up to 30%.[67] This means that there is an opportunity cost to be borne if the data economy is not deployed to its full extent as these profitability and employment gains would not be realised (to the full extent).

Examples from the case studies:

Some of the case studies have pointed to the possibility that existing collective action problems may lead to collective sub-optimal market developments although individual short-term action is considered rational.

In the agriculture case, for instance, farmers could become more efficient in their operations through the provision of data to service providers. On the flipside, however, this could lead to a situation in which service providers could, based on the knowledge gained from information sharing by farmers, predict yields and thus – at the regional and global level – increase supply-side prices in order to become more profitable at the expense of farmers and consumers.

A similar collective action problem has been reported in the case of mHealth and largely depends on users' willingness to take up a particular service and 'pay' with their data, as well as the extent to which service providers exploit the information received.

In addition, the European Commission has estimated that approximately 90% of jobs within the EU need at least some sort of ICT skills. However, estimates show that roughly 40% of EU labour force is not (yet) properly digitally skilled.[68] This corresponds to 756,000-825,000 jobs that could potentially remain unfilled in 2020.[69] As explained above, businesses incur costs already today in relation to acquiring skilled personnel, as well as training their current staff.

[65] See: Digital Single Market Strategy / European Commission, 2015. COM(2015) 192 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192, p. 16

[66] COM(2016) 180 final. Communication on Digitising European Industry. Reaping the full benefits of a Digital Single Market. (SWD(2016) 110), p. 4.

[67] The estimates are based on work by: Crozet, M. and Milet, E. (2015) Should everybody be in services? The effect of servitization on manufacturing firm performance. CEPII working paper. See: http://www.cepii.fr/PDF_PUB/wp/2015/wp2015-19.pdf

[68] See also: Eurostat (2015): Digital skills of the labour force. http://ec.europa.eu/europe2020/pdf/themes/2016/digital_single_market_skills_jobs_26105.pdf

[69] COM(2016) 381 final: A New Skills Agenda for Europe : Working together to strengthen human capital, employability and competitiveness. SWD(2016) 195 final, p.7.

European Commission estimates show that big data used in a smart way could lead to almost 1.9% of growth in the EU.[70] Relative to EU-28 GDP in 2016, this corresponds, for instance, to approximately EUR 280 billion in opportunity costs (i.e. the monetary value of business not realised through sales) for EU businesses.[71]

Finally, the European Commission has recognised that there are also large disparities between large companies and SMEs, with the large majority of SMEs and midcaps seriously lagging behind in embracing digital innovations.[72]

Consumers pay undue prices

Key messages:

- As a consequence of the costs which companies incur because of the barriers mentioned above, consumers pay more than what they could be charged in the absence of any type of uncertainty for business.
- Quantification of these costs is not possible at this stage but it was possible to use available data to obtain reasonable estimates.
- Data monopolies and lack of competition linked to the unwillingness of data holders to share data could also entail higher costs for consumers overall.

From a theoretical perspective, it can be assumed that prices for consumers today are not as low as they could be if businesses did not face uncertainties about data sharing as a result of technical and legal barriers.

The logic behind this argument is that businesses could gain economic advantages through data sharing, such as increased efficiency, which, in turn, would lead cut their costs. Consequently, businesses that share data could also decrease prices for consumers while simultaneously sustaining their profitability.

Evidence from the case studies:

Dynamic pricing models are discussed in the agriculture (see textbox on the previous page), energy and mHealth case studies.

In the energy sector, for instance, it has been argued that smart energy will lay the groundwork for overall monitoring and control of appliances in response to energy prices. For example, a washing machine might start running when there is a surplus of energy capacity available and electricity prices are at their lowest levels. Something similar is possible in the area of mHealth: insurance fees would be adjustable depending on the general health and exercise routines of insurance policy holders.

[70] See: http://www.microsoft.com/global/eu/RenderingAssets/pdf/2014%20Jan%2028%20EMEA%20Big%20and%20Open%20Data%20Report%20-%20Final%20Report.pdf

[71] EUR 14,825 billion in 2016: http://ec.europa.eu/eurostat/statistics-explained/index.php/File:GDP_at_current_market_prices,_2006_and_2014-2016_YB17.png

[72] See: COM(2016) 180 final. Communication on Digitising European Industry. Reaping the full benefits of a Digital Single Market. (SWD(2016) 110), p. 5.

However, this could also have adverse effects on consumer prices as those consumers that do not (yet) make use of smart devices would eventually have to bear the costs of reduced prices for smarter consumers – irrespective of their energy consumption or health.

So far, however, no attempt has been undertaken to substantiate and quantify this argumentation. As mentioned above, it has been estimated that the top 100 EU companies could save up to EUR 425 billion per year through the Free Flow of Data initiative[73], with at least parts of these savings being passed on to EU consumers in the form of price reductions.

In addition, the use of smart products and services by consumers is expected to increase the possibility for consumers to compare prices between vendors. This can reasonably be assumed to put pricing pressure on vendors so that consumers would have to pay less in the medium and long run. This means that, in the current situation, consumers pay more than they might in the future.

However, concerns have been voiced about consumers' inability to put a value on their data.[74] As big data platforms manage to extract data from users with little or no financial compensation, consumers currently face net losses in economic terms, while big data companies are able to achieve large profits through the aggregation of users' data.

It is important to acknowledge that the users of big data platforms receive a non-financial or indirect financial compensation for their data – and it is inherent in a market economy that companies selling products and services try to do so at a profit. However, it is a problem of competition economics that big data platforms (such as Google, Amazon, Facebook etc.) are able to use their market power (1) at the expense of smaller providers (e.g. by manipulating sales prices by means of their purchasing power) and (2) and possibly even engage in abusive market behaviour as e.g. showcased in the agriculture case study (i.e. farmers' fear of seed providers' use of big data to influence world food market prices in order to maximise their own turnover).

Thus, while it is rational at the individual level to use big data platforms and provide respective companies with individual data that cannot be valued *per se*, individual rationality may lead to collective suboptimal outcomes (which ultimately can be calculated).

In this regard, it is also important to keep in mind that a lack of competition (i.e. where there is no alternative service offering) can be regarded as a form of user disempowerment. This argument is used in the automotive sector by independent car repairers for instance. As one of the stakeholders put in during the Smart Industry workshop "data monopolies of data

[73] See: EPSC strategic note 'Enter the data economy': https://ec.europa.eu/epsc/publications/strategic-notes/enter-data-economy_en; European Commission (2016), The EU Data Protection Reform and Big Data, http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf.

[74] See for example: Nathan Newman / Federal Trade Commission: How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population. https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf or Nathan Newman (2014): The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google. In: William Mitchell Law Review, Vol. 40, Issue 2. http://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1568&context=wmlr

holders entail smaller choice for consumers, who ultimately will pay a higher price"[75]. In fact, if certain categories of businesses are excluded from data they absolutely need, this could lead to them disappearing and therefore lower overall competition on the market. Classic economic models suggest that with more limited competition prices tend to increase. Nonetheless, one should also consider that the data revolution might lead to the restructuring of all industrial sectors and that, rather than being linked to data monopolies, changes in the value chain could be associated with the new emerging data driven business models. However, the automotive sector is currently one of those most disrupted and caution is therefore probably called for in generalising based on these findings.

This discussion on limited competition is also closely linked to 'differential pricing' strategies that may e.g. favour customers that have provided vendors with their data. This is a rapidly emerging business practice.

Consumer safety, and clear and easy compensation for damage is not fully ensured

Key messages:

- Due to the liability barrier and the limits of the current liability regime, consumer safety, and clear and easy compensation for citizens and businesses cannot be ensured.
- In fact, because of reliance on contracts and uncertainties around liability provisions, citizens and businesses might be unaware of their rights or unable to impose them through fairer contractual clauses.

The data collected for this study (See Annex 1 – Outcome of the legal mapping in particular) pointed out that the legislative framework on liability in the context of non-tangible products (data) is scattered. More specifically, citizens and businesses can to an extent rely on product liability rules and product safety rules, but this depends largely on whether data as such (absent a material carrier) can be considered a product or item of property. Furthermore, the evidence available from the legal mapping highlighted the fact that consumer protection rules on transparency, and unfair terms and practices, provide consumers with relatively robust protection even in the data economy. However, their usage and ownership of data is only weakly protected, as is the liability of any service provider, seller or trader.

Overall, there are some ambiguities and difficulties in applying the existing legal framework to the data economy. There are unresolved questions about the categorisation of data as a product or property, as liability rules do not always account for non-material damage, and there are no homogeneous rules in relation to ownership or usage rights. We note that some proposals have been made in recent years that could potentially solve a part of this problem, including notably the Commission's proposal for a Regulation on a European

[75] See Workshop on the transformative effect of access and re-use of data for smart industries, https://ec.europa.eu/digital-single-market/en/news/workshop-transformative-effect-access-and-re-use-data-smart-industries

Common Sales Law[76], the 2015 proposal for a Directive on certain aspects concerning contracts for the supply of digital content[77] and a proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods[78] (See Annex 1 – Outcome of the legal mapping). However, the work for this study has shown that the new proposals do not offer a comprehensive approach, meaning that this study will play a role in determining if and where there are additional challenges.

For citizens, this means that they may first face an unclear situation, in which it may be difficult to determine if anyone was liable for any damage they incurred and who that would be. The same can happen within a B2B context in relation to sharing and accessing data. If the legal situation is unclear, it is less likely that the situation could be resolved by the out-of-court dispute resolution mechanisms, which are often faster and cheaper compared to court procedures.[79] Thus, it is likely that parties suffering prejudice would need to spend **time** on this and that they would face **costs**, including for legal support.

Second, there may be **situations in which citizens and businesses are not able to receive compensation for damage**. Some of them may hesitate to initiate court proceedings with an unclear outcome, fearing the costs and stress involved. This may be especially true in cross-border situations.[80]

These liability uncertainties could therefore jeopardise consumer safety in the EU and especially if the liability regime were to prove inadequate in court to respond to the challenges brought by IoT, AI and autonomous systems as well as non-embedded software.

The causes of the problem

This section analyses the causes of the problems for businesses and society. It correlates with the practical barriers identified as part of the analysis of the business models and the case studies. It contains the findings from the 'reality check' of our initial hypotheses outlined above.

[76] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52011PC0635

[77] Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, see http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0634

[78] Proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods; see http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0635

[79] Cf: Commission Staff Working Paper, Impact Assessment accompanying the document 'Proposal for a Directive of the European Parliament and of the Council on Alternative Dispute Resolution for consumer disputes (Directive on consumer ADR)' and 'Proposal for a Regulation of the European Parliament and of the Council on Online Dispute Resolution for consumer disputes (Regulation on consumer ODR)', COM(2011) 793 final; Study on the use of Alternative Dispute Resolution in the European Union, Civic Consulting of the Consumer Policy Evaluation Consortium (CPEC), 2009, http://www.cc.cec/home/dgserv/sg/evaluation/pages/eims_en.htm

[80] Ibid.

Contractual and legal barriers

Key messages:

- Contractual and legal barriers are impeding the sharing of, access to and (re-)use of data in Europe but not all barriers matter to the same extent.
- 'Data ownership' does not matter as much as originally supposed at the beginning of the assignment. Around 55% of respondents identify 'data ownership' as not being a barrier or being a very small barrier while this is a very important barrier or blocking factor for only 18% of the respondents.
- Access to and (re-)use of data is a key barrier. This is especially so for a number of companies situated in the 'data user' position of the value chain. To understand this barrier, an analysis of the 'data sharer' perspective on opening up data is also crucial.
- Surveys and case study results indicate that data portability and intellectual property rights do not constitute major barriers to the expansion of the data market in Europe.
- Finally, liability does matter as a barrier, particularly bearing in mind its horizontal dimension. In fact, it affects companies in different positions along the value chain, of different sizes and from different sectors.

The key findings of our analysis of legal barriers are that "**data ownership"** (including intellectual property rights) **actually *does not yet matter* in practice for businesses[81] (and especially for businesses accessing data), and the legal aspects of the portability of data *do not yet matter***.[82]

In contrast, however, the **access and (re-)use of data *do indeed matter*** and may impose barriers to the development and implementation of innovative business models, products, and services. **This is also true of liability issues:** while there are some concerns around the consistency of existing liability rules, these should be regarded as horizontal issues across all sectors and types of businesses, with the data economy being only one example of a policy area that is negatively affected.

Overall, legal barriers are considered as expensive elements to tackle when dealing with sharing and accessing data. Indeed, around half (49%) of the data user respondents to our general survey identified the costs of legal advice as the most important cost category for them by far. An even higher percentage emerges from the specific survey: 81%. These data emerging from the general and specific surveys also indicate that there is probably an issue

[81] The European Commission Expert Group on Cloud Computing Contracts has, however, pointed out that the technical aspects of data portability, i.e. the interoperability of technical solutions, are crucial. See: Itte Overing and Maciej Gawronski (2014): Data portability upon switching. See: http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf

[82] It should be kept in mind, however, that the portability of data (i.e. the 'ability to move, copy or transfer data easily from one database, storage or IT environment to another') is an important issue for consumers. See, for instance, the 2016 study by Consumers International on *The Internet of Things and challenges for consumer protection* with regard to the right to data portability contained in the GDPR:

with the overall clarity of the legal framework in place related to access and (re-)use of data. This is due primarily to the legal uncertainty surrounding certain aspects of the data sharing and the full reliance on contracts to regulate the relationship between data sharers and data (re-)users[83].

The role of contracts in the data economy

Companies rely on contracts to regulate and govern their exchanges of data. Mostly, these contracts are based on key concepts such as 'ownership' in a generic and often undefined sense, intellectual property rights, usage rights and restrictions, and liability for the accuracy or usability of the data. These issues are addressed throughout the lifecycle of the contract, i.e. key moments throughout the process of concluding, executing and terminating contracts, including the moment of agreement, moment of transfer of property etc.

Such concepts need adjustments when applied to issues relevant for the data economy, data sharing and access. Specific challenges arise in relation to the use of technologies such as the IoT and machine-to-machine (M2M) data (cf. the separate section on these topics). In addition, the context of a contract in a data ecosystem can also cast doubts on enforceability, in particular in relation to third parties.[84]

By way of example, crypto-currency transactions are pseudonymous and largely untraceable. On the other hand, imposing limits to the use of virtual currencies (such as imposing proof of identity) may limit the freedom to contract. Moreover, and more fundamentally, the technology of block chaining – which is the basis of most cryptocurrencies – calls into question what will constitute a contract in the future: to what extent is a contractual agreement and even legislation required when a technology inherently provides stronger assurances of traceability than any contract or law could? Many questions do not have a clear answer at this stage.

As shown by the discussion held at the High Level Conference on Building a European Data Economy on the 17 October 2016[85] and during later workshops, the stakeholders are split in terms of satisfaction with this broad contractual approach to the sharing of data. Some SMEs on the one hand complained about one-side contract clauses and the burden that legal advice presents for them. As also suggested by the web-based survey, smaller players might also be more concerned than incumbents about the unequal bargaining power vis-à-vis the data holder[86]. However, there is no consensus amongst smaller companies on this topic, as overall most agree that the contractual freedom provided by this *modus operandi* is positive due to the early stage of the market. Bigger players on the other hand in

[83] As mentioned in the two stakeholder's workshops held in Brussels in October and November, contracts are a sufficient tool for most of the stakeholders for regulating their exchange of data. Nonetheless, to develop contracts, companies incur costs. This explains the answers provided to the web-based survey.

[84] In the absence of statutory rights to data (e.g. in relation to raw data not covered by database protection or intellectual property rights) it may be difficult to efficiently protect the economic interests of those who invest in data production in specific circumstances in which contractual remedies are not sufficient.

[85] https://ec.europa.eu/digital-single-market/en/news/high-level-conference-building-european-data-economy

[86] Insights from the targeted web-based survey.

general argue that the contractual framework is well suited to the current situation and the current level of development of the market[87].

Despite this cleavage across businesses, contractual relationships are the most recurrent form of agreements within the data economy. This is also acknowledged by the Member States, which are in consequence trying to facilitate contractual relationships between the different parties involved in the value chain through a number of pilot projects[88]. The Netherlands for instance has promoted an initiative aimed at developing standard contracts that can be (re-)used by the various stakeholders willing to access and share data. The standard contracts were developed collaboratively way with the inclusion of stakeholders of different sizes and positioned differently within the value chain.

The reliance on contracts for B2B sharing and accessing of data has some positive and negative consequences which will be discussed in further detail in the assessment of problems.

In the following sub-sections, we discuss both contractual and non-contractual barriers.

"Data ownership"

Although the concept of 'data ownership' emerged early in the debate on access and (re-)use of data, it seems that this concept is not as pivotal in the data economy as originally thought. One key reason is that, as it is currently conceived, the question of 'ownership of data' is largely of major concern only to the product/services providers and product/service users and, logically, only indirectly all the other players in the value chain[89]. The analysis carried out as part of this study has shown that in most use cases, the 'ownership of data' automatically remains with the service/product providers of the data[90] or that, in many cases, ownership is not clearly defined.[91]

However, it is important to understand that the concept of 'ownership' often relates to a very diverse set of claims, which may or may not combine aspects of intellectual property rights, data protection, trade secrets, contractual restrictions and other legal claims. While claims of ownership of data are often made, it is unclear and uncertain to what extent such

[87] See "High Level Conference on Building a Data Economy, summary of the discussion", http://ec.europa.eu/information_society/newsroom/image/document/2016-48/17_october_high_level_conference_report_final_40080.pdf

[88] One example of pilot project is the Ducth Dare to Share Initiative

[89] See the section on the conditions determining size and types of issues.

[90] See for instance the aerospace case study. In this sector the concept of "data sovereignty is applied" and the buyer of the tool or equipment producing the data is the owner of the data itself. The producer of the tool or equipment has only access to the data if the buyer allows this to happen.

[91] In the automotive case, for instance, interviewees have argued that ownership remain with the creator or collector of data, i.e. the driver or the manufacturer. On this matter, cf. e.g.: http://www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf; https://www.rolandberger.com/publications/publication_pdf/roland_berger_connected_car_final_060916.pdf .

claims would hold up in case of a court dispute. The result may well differ from dataset to dataset, country to country, court-to-court or sector-to-sector[92].

The demarcation of the concept of 'data' is also not clear-cut, and the interpretation chosen affects the extent to which ownership can be effective. Data can be categorised based on the characteristics of its content: e.g. personal, non-personal, government, health data, etc. However, in addition, the scoping of data can be very different: the concept can refer to individual pieces of data (e.g. single fields in a relational database), the structured files in which they are combined, the metadata describing the data or the files, the information contained in the data, the software processing it, the algorithms on which that software is based, and any resulting knowledge derived from the data.

The impact of 'data ownership' is strongly affected by this distinction. If a user is the owner of individual pieces of data or of entire files, being able to control those pieces does not necessarily ensure the ability to access or use them in any useful fashion. If the content of data is scoped more broadly e.g. to also include algorithms and knowledge resulting from data processing, the ability to use owned data would be more easily ensured. At this stage, however, such a broad concept of 'data' that includes more abstract concepts such as the underlying information and derived knowledge, or the software and algorithms used to process data, is considered to be out of scope of this assignment.

In practical terms, due also to the fact that the question of ownership only directly concerns two of the players in the value chain (service or product provider and the user of the service), the issue is also not always decisive nor critical. More important is the ability to have the right to access and use the data for specific purposes with sufficient clarity (see following section).

Account also needs to be taken of the fact that data may be subject to very different claims and restrictions, depending on whether it relates to personal or non-personal data, such as data on health, finances, scientific research, administrative data, etc. It is important to fully consider and capture these nuances when examining the ownership of data and the possibility of streamlining the data sharing and access, as potential solutions will depend on the context.

Working definition of 'data ownership[93]':

In general terms, ownership is a legal instrument of society to allocate goods or rights to one or more persons, allowing them to exclude other persons from taking certain actions in relation to those goods or rights. Ownership is alienable: it can be transferred from one person to the next.

In the context of this study, **'data ownership' is therefore understood as an alienable legal construct permitting one or more persons (the 'owners') to control access to or use**

[92] See for instance the development of a de facto data sovereignty regime in the aviation sector, as mentioned in the First Interim Report

[93] The working definition of ownership provided here does not constitute a legal definition but rather the illustration of the meaning that this term has in relation to the exchange of data within the value chain.

of a single piece or set of data elements to the exclusion of others.

It should be stressed that this is the study's internal working definition. No examples have been found of official legal definitions in Member State law. Furthermore, like any traditional ownership right (such as ownership of physical items), ownership of data is not absolute and unlimited, since legislation may have an impact on the ability to control access to or use of the data. As a practical example: ownership of digital data does not imply that one may without consequences ignore data protection law, engage in unfair commercial practices, or destroy data subject to retention obligations.

Although, as part of a targeted consultation by DG CNECT, approximately 80% of businesses indicated that "data ownership" issues are very important or important to them[94], businesses do not see data ownership as an impediment to developing innovative business models and selling related products and services to customers. This is confirmed by the insights emerging from our general survey: **around 55% of respondents identify 'data ownership' as not being a barrier or being a very small barrier while this is a very important barrier or blocking factor for 18% of the respondents only**. The remaining respondents replied that this is a "considerable" barrier (27%). In addition to the relevance of the position in the value chain for understanding the importance of the 'ownership' issue, the sectoral dimension also has some influence on the magnitude of the barrier.

Evidence from the case studies:

In the aviation sector the question of 'ownership' does not seem to be relevant as there is no debate between product provider (engine manufacturers) and product user (airline companies) that the product user is the de facto 'owner' of the data. The situation in the agricultural sector is rather different. In this case ownership of data is spread across different types of actor within the precision agriculture value chain and the debate around 'ownership' has been much more important. Nonetheless, in the agricultural sector, data ownership is not a problem per se but it always depends on the recipient of the information and the products or services the data are (re-)used for, as well as on the remuneration of data generators.

As suggested by the evidence emerging from the case studies as well as by the survey result, the access to the benefit generated from analytics and the use of the data is much more important than data ownership.

However, as data ownership is defined differently in the different sectors and across different types of firms, the differences in the importance of the ownership concept could be explained by a different understanding of the concept[95]. Indeed, as stressed above, the study team has provided its own working definition in the absence of an existing common definition. Furthermore, the ownership concept is in practice bundled with contractual access and use rights that undermine the exclusivity that the owner may expect to enjoy.

[94] European Commission (2015): DSM Free Flow of Data Initiative and emerging issues of data ownership, access and usability, p. 8. See: http://ec.europa.eu/newsroom/document.cfm?action=display&doc_id=12205

[95] In this particular case, only 2 SMEs see data ownership as a blocking factor

Evidence from the case studies:

"Data ownership" is an issue that businesses often exclude from their contracts as it is not clear to them how to allocate 'ownership', to whom, or under which circumstances in order to avoid losing customer loyalty, and without harming one's own business interests.

In the insurance sector, for instance, it has been argued that EU manufacturers of wearable technology might refrain from sharing data in order not to lose the trust of their current customers; insurance companies see data ownership and trust as one of their key selling points with customers.

Thus, instead of sharing data with each other, ownership de facto often stays with the data provider (in this case, the insurance holder) in order not to put current core business at risk (e.g. by losing customer loyalty).

Instead of clearly defining ownership in contracts, businesses thus often define access and usage rights to different contract parties.

Moreover, there seems to be legal uncertainty surrounding data ownership in certain sectors in relation to data produced by machines or devices, as well as non-personal data (e.g. in the area of finance). Initiatives such as My Car My Data[96] try to clarify these issues by advocating stronger and more exclusive rights to the vehicle owner's data – although this, too, can be problematic, as the owner of the vehicle is not necessarily the person driving it, i.e. the owner is not necessarily the person to whom the data most directly relates.

In the agricultural domain too, farmers' organisations are lobbying along similar lines, to avoid their data being used in a manner that harms their interests (e.g. by using crop yield data for commodities speculation).

Therefore, although the absence of an ownership right to data, as well as the difficulty in defining data access and use ('ownership') rights in contracts are not perceived by businesses as the main barrier to data exchange, the consumers' perspective and the risks borne by businesses deploying innovative business models with data have been pushing for a clarification in this domain.

The analysis of relevant legislation in 13 Member States[97] shows that the existing legal concepts of ownership cannot be readily applied to digital data as such, and/or that data is not subject to traditional property rights. The principal justification in countries in which this position can be deduced from applicable law is that ownership rights imply a degree of exclusion, where the owner holds factual power over the owned thing that cannot be shared without impacting the original owner's factual rights. Digital data lack this quality: since factual access to the data is sufficient to allow a recipient to take any action they desire without impacting in any way the factual power of the original holder, the ownership paradigm is not appropriate for digital data. Ownership cannot be readily applied in this perspective to

[96] See: http://www.mycarmydata.eu/

[97] Belgium, Estonia, Germany, Finland, France, Italy, Latvia, Lithuania, the Netherlands, Poland, Romania, Sweden, and the United Kingdom

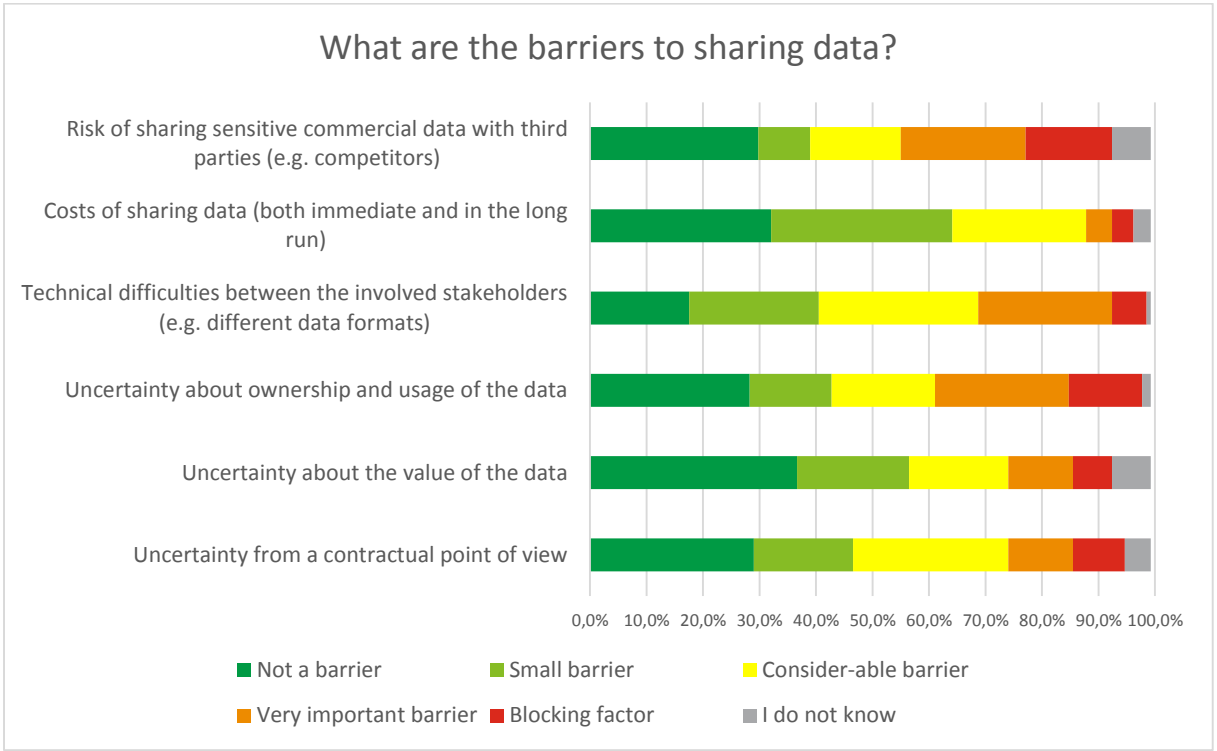
goods that can be infinitely reproduced without necessarily creating any repercussions for the rights of the initial holder.

This position is not held universally, however, and several countries indicated that there is some discussion still on the topic. The principal counterarguments are that ownership can also exist for intangible rights (such as intellectual property rights), and/or that digital data has clear economic value that is subject to ownership. This appears to be, however, the minority position among the Member States.

Access to and (re-)use of data

While the uncertainties about the concept of 'ownership' of data do not represent a major barrier for the data economy in Europe, as described in the previous sections, **barriers to access and (re-)use of data** are far more important. The assessment of these barriers requires an understanding of the reasons why data are not shared more widely in Europe. It is therefore important also to look at this issue from the perspective of the data sharers to analyse what prevents them from sharing data more freely. The outcome of the general survey provides some key insights into this dimension and can help establish a list of causes for the limited access and (re-)use of data.

Figure 10: Barriers to sharing data



Source: Deloitte, General Survey

In general, **companies do not share their data because they are afraid of doing so for one or more of a number of reasons**. As the figure above suggest, first and foremost, companies are **afraid of sharing sensitive information** and losing their competitive advantage without even realising it. This is a blocking factor for 15% of businesses, a very important barrier for 22% and a considerable barrier for 15%, while this is a small or non-existent barrier for 48%

of the remaining respondents[98]. This means that at least one company in two does not feel confident in sharing its data due to this risk. The finding is supported by the data collected through the interviews: many incumbents do not want to take the risk of opening up their data to third parties when they do not yet have enough incentives to do so[99]. The price of data and remuneration can be incentives in this respect, but only if the perception of the risk is not too high and if the downsides of sharing the data are not too many. Indeed, as one of the financial incumbents argued, "whichever price I might impose on the data, it will never be able to cover up the reputational costs that I will suffer if my clients start mistrusting me"[100].

Moreover, in the absence of very strong reasons for doing so, companies might be particularly **wary of sharing data with other downstream players** in the same value chain who could possibly be competitors. For instance, in the automotive sector, car manufacturers seem to have a limited incentive for sharing data with independent car repairers beyond what is legally binding. Similarly, many incumbents in the financial sector are not willing to share their aggregated data with start-ups and SMEs due to fear of competition in certain domains. Therefore, a high perception of risks and limited incentives could explain why many service/product producers or users do not share their data more.

Linked to the risk perception, there is also the question of **uncertainty about 'ownership',** usage of the data and what others will do with it. This is a major issue for 35% of respondents (blocking factor – 12%, very important barrier – 25%) and also relates to the question of **data liability** which will be further developed in the next section. Without certainty and precise information on what third parties will do and what can do with their data and in the absence of strong remedies for sanctioning unfair practices and behaviour, companies are very careful in opening up their data. The uncertainty around 'ownership' and (re-)use of data is therefore strongly linked to the fear of disclosing sensitive information and the uncertainty around liability.

In addition to companies' fears, technical difficulties can also play a role. Although this is not a very frequent blocking factor (6% of respondents only) it is a very important barrier for 23% of data sharers participating in the general survey. Hence, interoperability and other technical barriers should not be underestimated, especially when taken together with considerations linked to risk aversion and legal uncertainties. The combination of all these reasons could lead to limited data sharing overall.

On the other hand, as the figure above also suggests, **the issue of valuing the data or the costs of making it available are not the most important barriers**. Indeed, although these issues were often mentioned during the interviews, they were rarely considered to be blocking factors as business can overcome them if they are really interested in doing so. Indeed, the costs of sharing data can be considered as affordable if data sharing is believed to be a strategic investment and if data valuation can be addressed through experimenting with

[98] Insight from the general survey.
[99] See case study on Finance.
[100] See Financial sector case study

pricing and testing willingness to pay. Moreover, as already mentioned, when data are shared, they are very often shared for free for reasons related to business strategy, corporate social responsibility or some other form of corporate self-interest. However, it is worth noting here that, overall, the barrier of valuing data in the data economy presents some particularities which are further described in the section concerning the other barriers.

Similarly, the **barrier related to contractual uncertainties is not seen as particularly significant**. Indeed, although contractual uncertainties can lead to significant legal costs (see section on the problem assessment), these contractual issues are something that businesses also experience in other domains and that they are more comfortable solving.

Therefore, companies have multiple reasons to be wary of sharing data, but the lack of data sharing is not the only cause of a general lack of access and (re-)use of data. Indeed, it is also important to note here that, even when data are theoretically accessible to interested businesses and data users/(re-)users, they might still be too expensive from their perspective.

In the specific survey, around 80% of respondents belonging to this category identified the question of the costs of data as a blocking factor for them. Similarly, 76% of them also consider the costs of buying data as "very high"[101]. Therefore, **the costs of access** to the data can be considered as a major obstacle for intensive data users and (re-)users. Nonetheless, this problem should be seen in proportion. In the general survey, a majority (52%) did not consider the price of data as a problem at all. Only 11% mentioned it as a very important barrier or blocking factor. Therefore, once more the contradictory results of the two surveys seem to suggest that the magnitude of the problem is very different for intensive data users/(re-)users (targeted survey) than for business as a whole (general survey).

Clearly, however, it is crucial for businesses to compare the price asked for accessing and (re-) using data with the costs associated with (self-)generation of such data, as well as reasonable expectations for a return on investment. The reason for this is that, e.g. under given competitive circumstances, it may be rational for a business to increase prices (compared to the 'normal' level) for the access to and (re-)use of data by third parties in order to prevent data (re-)use and the extraction of additional value from a good (i.e. deterrent/prohibitive pricing).

Finally, there are questions around **the conditions for data (re-)use**. (Re-)use of third party data is normally defined by contracts and restricted as far as possible. This issue is particularly relevant for data analytics companies that would like to (re-)use and aggregate certain datasets obtained while carrying out projects for specific firms in order to provide additional services to their clients[102]. In virtually every case, (re-)use of the data for purposes other than those of the contract established between the client and the data analytics company is not permitted. This also happens within the aviation sector. Each time manufacturers wish to use the data obtained (contractually) from the airline companies for a new purpose, this triggers a renegotiation of the contract leading to delays and the need for resources. There-

[101] Insights from the web-based survey

[102] See the case study on Chemical Sector, Annex 2 – Sectoral case studies.

fore, even when access to the data is possible and can be resolved through the contractual relationship between the parties, (re-)use remains very complicated.

Evidence from the case studies:

In the aviation sector, aircraft manufacturers advocate more access to data in order to be able to extend predictive maintenance and increase safety for travellers and airlines. However, due to the fear of giving their competitors a competitive advantage, airlines which hold the data are not willing to share it other than within the framework of a service contract and under specific security conditions. This means the data cannot be fully exploited to increase the safety of the components overall.

Similarly, in the chemical industry companies sharing data with analytics service providers tend to restrict the possibility for the latter to (re-)use these data, even in aggregated form, to provider further services. This is due to the perception that allowing third parties to (re-)use such data will reduce the competitive advantage of the company sharing the datasets.

Again, it is important to acknowledge that the EU data economy is still emerging and that businesses are still trying to find their role and niche within this emerging field. At this stage, businesses are eager to survey the field of available and accessible data with new business models shaping up along the way. Inaccessibility of data and problems in re-using it impede numerous potential business models from getting established in the market[103]. However, from a macro-perspective, the businesses themselves do not yet seem to be ready to make effective and efficient use of the data available and accessible as products and services are still at the development stage.[104]

Liability in the context of data exchange

Issues around liability were also emphasised by the analysis as another barrier to the development of innovative business models, products, and services. Compared to other barriers that are much more stakeholder, SME or sector-specific, **liability seems to be a transversal concern touching upon businesses' situation at different stages of the value chain and in different sectors**. In this respect, it is a truly horizontal barrier although it applies differently for different players:

- For product/service providers in fact, the issue of liability is linked to the risk of sharing data with third parties who could misuse this data.

[103] As illustrated in the first interim report (case study on aerospace and on chemicals), airplane producers suggest that more predictive maintenance services could be offered if data were more accessible to them. Similarly, in the chemicals sector, data companies argue that they would produce much more useful insights if they could access more datasets and aggregate them.

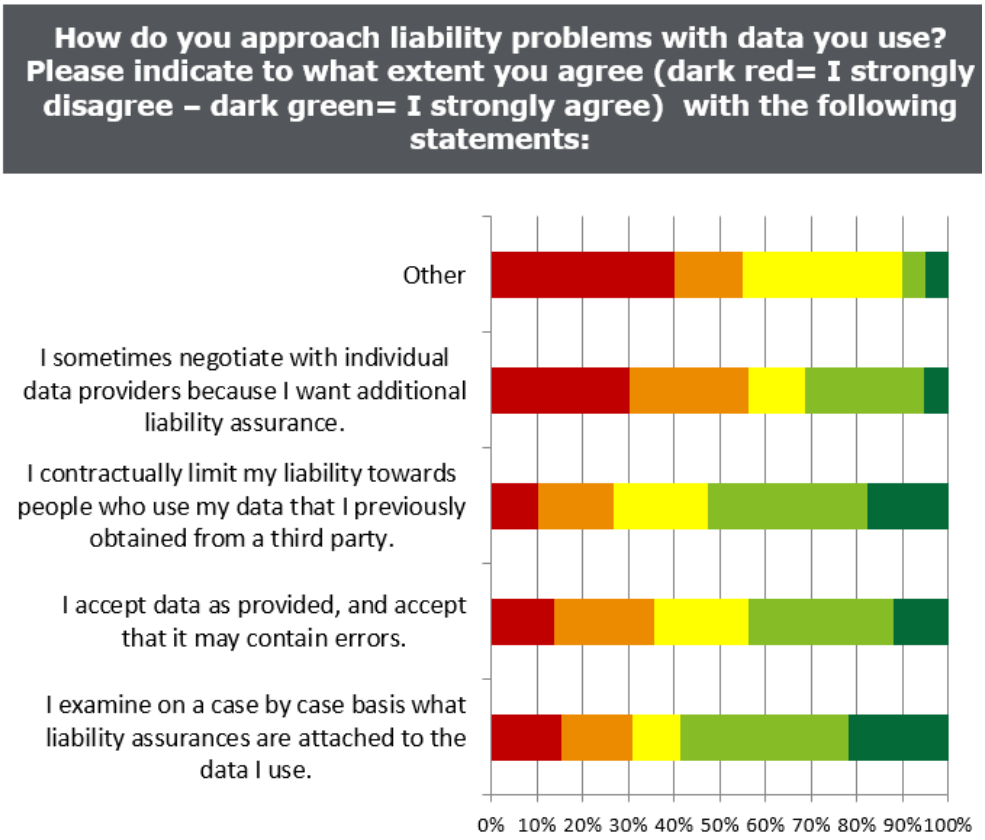
[104] In the chemicals sector for instance, chemical companies are all focusing mostly on the use of data for improving operational processes, as this is the area in which data have proved to be more useful in the past. New business models and the use of data in other domains is still in its infancy.

- For those players interested in accessing data, the question is rather what happens if the data they receive from data sharers are incorrect, and if they provide a wrong service to their customers based on that.

Moreover, the liability barriers also touch upon the contractual and extra-contractual liability of IoT and autonomous systems, as well as artificial intelligence and robots. This is addressed in a separate problem assessment within this chapter.

Given this context and the overall relevance of the liability issue, the general and targeted survey tested several hypotheses as to how companies approach liability in the data economy, as shown in the Figure below.

Figure 11: General survey - approaches to liability



Source: Deloitte, General Survey

As the data in the general survey suggest, companies tend to decide on a case-by-case basis and through contractual means which liability assurance they need and wish to have. This may result also from the legal uncertainty about the overall liability regime.

Indeed, as part of the European Commission's 2015 public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy[105], respondents were almost evenly divided on whether they had experi-

[105] See: https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud

enced situations suggesting that the liability regime in Section IV of the eCommerce Directive (Art. 12-15)[106] was not fit-for-purpose or had negatively affected the market's level playing field. In fact, our analysis shows that it is clearly not an instrument that governs all relevant aspects of the data economy. Specifically, its liability regime relates to specific services rather than to data, and does not relate to quality requirements or expectations in relation to data, or to the consequences of any shortcomings on this point. None the less, it provides a baseline with which all Member States have been required to align.

Currently, businesses can work out individual liability regimes through their contractual arrangements within the limits of the 1985 Product Liability Directive (PLD)[107], national law, as well as jurisdiction. This is also confirmed by the specific survey data. Indeed, amongst the data (re-)users, around 90% consider liability to be a very small barrier and 42% of them normally "contractually limit liability towards people who use their data previously obtained from a third party". However, there was a very high number of "don't know" answers relative to the other questions, suggesting that liability is rather an emerging barrier which has

Evidence from the case studies:

Businesses largely seem to tend to preclude liability from their contractual arrangements in order to avoid stepping into a legal grey area: while strict *product* liability is a legal concept, the data economy revolves around the use of data as a *service* (and not a product).

As such, product liability rules can offer a supporting shield in the data economy, but in the absence of a material carrier to which the data can be linked – which is particularly relevant in the IoT market as will be discussed subsequently – this depends largely on whether data as such (absent a carrier) can be considered a product or item of property.

The question of liability is also seen differently in the diverse sectors. In the **financial sector**, the major threat for data holders consists in misuse of the data opened up, potentially leading to a drop in the customers' trust in the bank and therefore reputational losses. These are seen as the main concern for financial players with respect to liability.

In the **chemicals sector**, on the other hand, the data companies fear being held accountable for bad decisions taken following the data-driven recommendations they provide. For this reason, the ultimate decision on whether to implement a certain recommendation or not is in the hands of the chemical company itself.

Finally, in the **aviation sector**, the question of liability is linked to the question of further access to data. Indeed, aircraft manufacturers and component suppliers would like to gain more direct access to data but not to be held liable for any prediction (in terms of safety or maintenance) based on them. Indeed, due to the large amount of data to be processed (including in real time), they would be incapable of ensuring constant and timely monitoring to ensure early detection of irregularities in all planes using their components.

of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'); http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031

[107] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374

so far been sufficiently settled through contractual means.

These findings make clear that the PLD has harmonised liability law only to a limited extent. National tort law traditions and practice in the Member States remain important. There has been continuous academic work since the PLD was passed on extra-contractual liability in Europe, for instance by the European Group on Tort Law (EGTL). In 2005 the EGTL published *Principles of European Tort Law* (PETL)[108]. These principles have had some influence on jurisprudence and legislation in recent years. While the PETL do not address the new challenges in the data-driven economy, the European Group on Tort Law has made a further contribution with an analysis on *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (European Product Liability, intersentia 2016)[109].

The General Product Safety Directive applies to products that are supplied or made available to consumers (and thus not to professional users and businesses) in the framework of service provision for use by them. It is clear that pure information and digital data as such fall outside the scope of the Directive. However, material items that use and integrate those data – again this is relevant to the IoT context – are affected by the application of the Directive. However, the Directive does not contain any provision on the consequences of the damage and the liability for producers and distributors of products.

The absence of a concept of service liability is seen as a barrier for the development of business models, as SMEs in particular cannot afford legal proceedings in relation to their business models (e.g. in order not to become insolvent). On the other hand, large enterprises seem to be adapting rather slowly to the new data service environment as they – quite naturally – examine potential business areas very carefully in order not to endanger their current core business.

National and EU legislative frameworks on liability

The national and European legislative frameworks that apply to contracts in the data ecosystem face multiple challenges. Firstly, they are based on concepts – ownership, intellectual property, personal data, consent, liability – which do not necessarily apply clearly or unambiguously to a complex business model where data is automatically collected, combined, enriched, updated, modified, exchanged, (re-)used and deleted.

Secondly, existing laws may not sufficiently take into account the different positions of market players, notably the situation of SMEs, entrants and start-ups, as well as inequalities in bargaining power, etc. More specifically, while the legislation as such is objective, it can have repercussions that are unfair to some market players, or that simply result in a market situation that is suboptimal from a societal perspective.

In this way, the legislative frameworks may hamper the smooth performance of the data

[108] http://civil.udg.edu/php//index.php?id=129&idioma=EN

[109] http://intersentia.com/en/european-product-liability.html

value chain contract, e.g. through legislative gaps or inadequate provision, or simply fail to achieve results that are optimal for society as a whole.

The possible inadequacy of the legislative frameworks might also affect the principles of intellectual property rights (IPR). As has been pointed out, the data economy is developing and changing too fast for EU IPR processes to keep up. For instance, an interviewee from the financial sector argued that it would take around three years in the EU to patent algorithms. By the time the algorithm is patented, it is very likely not to be usable anymore in the patented form. Hence, since the role of intellectual property rights seems to be in a state of flux, legal uncertainty about liability for products and services in the data economy seems to be an important barrier. It is important to notice here that many of the uncertainty issues around liability are currently governed by the use of certification schemes and interoperable technical solutions rather than contractual arrangements to avoid liability claims. This is discussed in more detail subsequently.

Liability in IoT and M2M contracting

At present, stakeholders face legal uncertainty with regard to the liability aspects in the context of IoT, both in terms of contractual and extra-contractual liability. While existing national legislation may provide some solutions based on existing private law regimes relating to human intervention, particular problems may occur in relation to completely autonomous systems (e.g. autonomous robotics). Liability rules that apply to data infrastructure providers who control smart products also deserve particular attention.

Finally, the legislative framework that applies to M2M contracting is currently also not clear, and may cause legal uncertainty. However, there is a strong consensus that M2M contracting can fall within the scope and flexibility of existing contract law, provided that the M2M contracting process is organised in such a manner (legally and factually) that the behaviour of a software agent can be ascribed clearly to a person (human or legal entity).

In practice, contractual terms that are accepted by participants in an M2M ecosystem of course play a crucial role on this topic, since they enable the conditions, procedures and liabilities to be clearly set out.

As is the case of interoperability barriers, data liability affects data sources and data (re-)users differently. For the former, the main question relates to possible claims over mistakes in the data provided to the (re-)users. For the latter, the extent to which this is important depends on the sector.

Evidence from the case studies:

In the financial sector for instance, banks argue that, as data sources, they are reasonably sure of the quality of the data they provide and therefore do not see this as a major concern. However, in other sectors, such as health or transport, the question of the quality of data provided is more sensitive due to the nature of the data themselves and the types of decisions that could be based upon them (e.g. self-driving cars or connected medical devices).

Similarly, for the data (re-)users, the question of the liability in the event of issues with the data depends on the kind of service they offer (apps aggregating bank account data or

health monitoring devices). Sometimes fintech start-ups for instance inform their customers of the possibility of mistakes in the service provided which is the result of the quality of data received or, possibly, technical errors on their part. (Re-)users argue that it is usually clear who was the cause of the issue and therefore applying liability clauses can be relatively straightforward.

Data portability

Differences exist between sectors on the legal situation of data portability. In some sectors, the right for third parties to access and use certain data – although not necessarily through a portability right that allows data to be transferred to a competitor – is already a legal obligation. In the area of finance under Payment Services Directive 2, access to payment systems and to accounts maintained with a credit institution must be granted on specific terms[110]. This is an access and use right of the original data, and thus not a data portability right as such. Under Art. 35 of the PSD2, porting of data – or not – is possible, whereas the General Data Protection Regulation (GDPR) is the first legal instrument to formally rely on the concept of data portability[111].

Portability within the meaning of Art. 20 of the GDPR has an second meaning in addition to data access because it covers a specific situation in which a natural person (the data subject) may go to the actual data holder and ask for his/her data to be transferred (ported) to another entity, to the extent that this is technically possible. This is a competition-enabling mechanism, but not through a top-down access obligation as in PSD2, but by giving the 'data subject/owner' the relevant legal tool which s/he may use.

Its importance should not be overstated, however: the right is granted *only*:

- to data subjects (thus excluding any companies),
- in relation to personal data that these subjects have entrusted to data controllers themselves (thus excluding any derived, enriched or otherwise modified data), and
- when the processing was based on consent or on a contractual obligation (thus excluding any processing based on a public interest task, legal obligation, etc.)

Draft guidelines on the scoping and application of the data portability right under the GDPR were published by the Article 29 Working Party in December 2016[112].

Although data portability is important for businesses in sectors that are not (yet) governed by legal obligations, it was emphasised during the research for this study that it is not a priority concern compared to other issues.

---

[110] O.J. L 337, 23 December 2015, p. 35. Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[111] O.J. L 119, 4 May 2016, p. 1. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. p. 1.

[112] Guidelines on the right to data portability, WP 242, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Evidence from the case studies:

The data emerging from the case studies show that data portability is a concern only for some specific sectors and in specific cases. For instance, in the banking sector, data portability is a problem for those financial institutions (only a small minority) having recourse to Cloud Service Providers (CSPs) to store their data. In this particular situation, switching a CSP entails a major investment on the part of the bank because portability is not automatically ensured. However, SMEs and start-ups interviewed did not acknowledge this issue and argued that CSPs are rather effective in ensuring portability overall.

In the energy sector, the issue of portability relates to possible use of different suppliers and different smart meters, which has to be possible by law.

Apart from these two very precise cases, data portability was not mentioned in other sectors as a key barrier to overcome in order to ensure more data sharing, accessing and (re-)use.

The main reason is that businesses see data portability rather as a 'feature' than an 'enabler' of innovative business models, as well as products and services. This means that data portability can only be of importance if businesses have a product or service in place that is actually up and running (i.e. collects, stores and uses data in a certain structured format). It seems that most businesses are still very much in the testing phase of such data-based business models and therefore do not yet know if and how data portability is an issue.

Moreover, as soon as customers want to move, copy or transfer data, it becomes much more a matter of technical interoperability than a legal barrier.[113]

Legal uncertainty can also be identified in relation to the absence of a data portability regime for non-personal data, and the inapplicability of the data portability right to companies (since data portability under the GDPR is a right granted to data subjects, i.e. natural persons).

Intellectual property protection

Exclusive protection awarded through intellectual property rights did not emerge as a key barrier preventing further development of the data economy. In this respect, both the findings from the case studies and the academic debate on the topic converge. Indeed, Intellectual Protection Rights to the data was very rarely mentioned by the interviewees and the data sharers. When it was, this was only in very specific and particular cases, when it was argued that IPR was not really helpful and that the Database Directive[114] or the Trade Se-

[113] As part of the European Commission's 2015 public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, a small majority of respondents sees the need to strengthen the capacity of online platforms to address switching. See: https://ec.europa.eu/digital-single-market/en/news/first-brief-results-public-consultation-regulatory-environment-platforms-online-intermediaries

[114] See: Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML

crets Directive[115] are more relevant tools for companies in protecting their algorithms and datasets against appropriation by third parties. Elaborated algorithms were identified as a possible exception.

Similarly, academia has been debating the relevance of intellectual property protection in relation to the question of 'ownership', access and (re-)use of data. As recently argued by the Max Planck Institute for Competition and Innovation "any recognition of a new intellectual property right as a particular form of regulation of the market is in need of an economic justification."[116] From the academic debate, it seems that this economic justification has not been found yet within the context of the data economy. Therefore, companies do not seem to rely on IPR in this area and do not see this as an obstacle for sharing, accessing and re-using data and academia has not agreed yet on the necessity of using IPR to further stimulate B2B data exchange.

To conclude, the reality check showed that IPR does not really matter when it comes to the emerging barrier to the data economy.

Technical barriers

Key messages:

- Technical barriers might have a strong impact on data sharing, accessing and (re-)use.
- Interoperability emerged as a serious concern for businesses, irrespective of their position along the value chain and their size. Some sectors are more advanced than others in terms of standardisation efforts, but in general interoperability was mentioned as a concern for all sectors considered.
- Portability on the other hand has only a more limited impact as a barrier and was only discussed in very specific cases and more often from the service/product users' perspective.

The key finding of our analysis carried out so far is that **barriers stemming from (insufficient) interoperability or other technical issues indeed matter** and constitute one explanation for limited access and (re-)use of third party's data by businesses.

Working definition of 'interoperability':

The latest draft revision of the European Interoperability Framework defines interoperability as "*the ability of disparate and diverse organisations to interact towards mutually*

[115] See: Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943

[116] Position Statement of the Max Planck Institute for Innovation and Competition of the 26 of April 2017 on the European Commission consultation on "Building the European Data Economy", Max Planck Institute for Innovation & Competition Research Paper No. 17-08,

beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems"[117]. Interoperability barriers may be related to, for example, the lack of standards to facilitate the adequate storage, transfer and processing of data, aspects linked to the reliability (quality/security) of data services provided (including when these services are accessed from or used in another country).

The case studies have revealed that interoperability – or the lack thereof – is a crucial prerequisite for data exchange to take place effectively, as well as to be as efficient as needed to produce/provide services for acceptable market prices. Nevertheless, each industry sector in the data value chain has its own specificities.

It is particularly true that interoperability is critical if one looks at the future of smart industries, as standardisation is one of the preconditions for the emergence of a strong Industry 4.0 in Europe[118]. Furthermore, this is confirmed by the result of the general survey carried out for this study. Indeed, 51% of the data users and (re-)users who responded to the general survey identified **lack of interoperability and technical standards as a blocking factor**, **or very important or considerable barrier** preventing them from deploying new business models[119]. This percentage increases significantly according to the data from the specific survey targeting start-ups and data analytics companies. In fact, amongst these more innovative businesses, 86% of respondents identified technical barriers as a major obstacle[120]. Therefore, it can be argued that the more intensively companies use data, the more technical barriers and interoperability issues are seen as important obstacles for access and (re-)use of data.

Moreover, interoperability and technical barriers not only constitute barriers to exchange of data, but they are also one of the most important drivers of costs, especially for SMEs, but also for incumbents willing to open up their data[121]. During the interviews, it was very often argued that merging different datasets and making them interoperable is one of the most resource-intensive activities for data (re-)users and that, even within the same value chain, datasets are rarely interoperable by default. This results in a need to multiply the efforts when a company wishes to integrate different datasets.

Evidence from the case studies:

Lack of interoperability can be found in the aviation sector, in which the different components of aircraft (developed by different manufacturers) very often produce non-interoperable data. It is then up to the airline companies to ensure interoperability be-

[117] European Interoperability Framework, 2010, see: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

[118] Industry 4.0, Study for the ITRE committee, European Parliament, 2016, see: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf

[119] Final result of the general survey.

[120] Final result of the specific survey.

[121] See Case study on the Financial Sector, Annex 2 – Sectoral Case Studies

tween the different components.

Similarly, in the finance sector the data from different European credit bureaus are not interoperable by default. SMEs and start-ups working with these data need to spend time and resources in polishing them before being able to provide services to their clients.

Finally, as also discussed during the Smart Industry Workshop organised by the European Commission[122], interoperability is still not entirely ensured in the energy sector, although this domain is much more advanced than the others in terms of standardisation activities.

These examples from the interviews confirm the data emerging from the general and targeted surveys.

Interoperability is also a crucial technical enabler of (legal requirements for) data portability for both businesses and consumers. Technical data portability and interoperability issues are e.g. common in the cloud-computing environment, as well as in relation to online platforms and have been identified by market players as frequent barriers. If interoperability is linked to formalised standards, portability refers mostly to open specifications: "using quality metadata creates not only quality data in the sense that it is unambiguous, but it also creates portable data, data that can be easily moved from one application to another and preserved over time independently of software."[123] Open standards and metadata definitions are important in reducing data portability barriers and hence increasing the (re-)use and preservation of data. This relates to the use of varying (non-compatible) standards resulting in the same type of data from diverse sources presented in different data formats.

Portability barriers were sometimes mentioned during the interviews and especially in relation to cloud computing and to the possibility of switching cloud service providers. As also suggested by the public consultation carried out by the European Commission, data portability seems to be in high demand and in low supply in the current data market[124]. Nonetheless, technical portability of data did not emerge as a significant blocking factor for further access and (re-)use of data for businesses. According to our analysis, this issue was mentioned mainly by product/service users (who are the main beneficiaries of mandatory portability rules as imposed for instance by the General Data Protection Regulation) and never as a blocking factor. In this respect, interoperability seemed to be a much more relevant barrier.

Data **interoperability matters for both data sources and data (re-)users but from different perspectives and to a different extent.** For data (re-)users, interoperability is key for their business models, especially when these are based on aggregation of data from different sources (through APIs or web scraping). The results of the targeted web-based survey confirmed this. Indeed, 81% of the data users and (re-)users identified technical interoperability

[122] Workshop on the transformative effect of access and re-use of data for smart industries, see: https://ec.europa.eu/digital-single-market/en/news/workshop-transformative-effect-access-and-re-use-data-smart-industries

[123] P. M. Benson, Data Portability, the antidote to data 'lock-in" — It is about the data - the quality of the data, 2009; http://eccma.org/docs/ECCMAWhitePaper-Data%20portability.pdf

[124] Public consultation on Building a Data Economy, see: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-building-european-data-economy

as one of the highest category of costs to be borne for developing new products and services[125]. For fintech start-ups for instance, the lack of interoperability of banks' data results in interoperability being one of their major costs drivers. The same applies in the chemicals sector where data companies invest up to 50% of their time to polish data before being able to analyse it and extract insights.

For data sources on the other hand, interoperability matters less, as also shown by the web-based survey. In fact, interoperability was not mentioned as a considerable barrier by data sharers in the targeted survey[126]. This shows that it can be an issue and it can entail additional costs when setting up APIs and data sharing solutions, but it does not have the same impact that it has on (re-)users.

To conclude, many interviewees acknowledged that there is a **general trend towards greater openness of data through APIs and open standards**, which is driven by market forces. The extent to which a given sector is more or less advanced is influenced by the extent to which there have already been industry-level initiatives in the area of standardisation. The automotive sector is clearly more advanced than, for instance, the aviation sector in this domain. It is also worth mentioning that the rise of IoT technologies will further increase the availability of industrial data for B2B sharing. This could be seen as a risk leading to the emergence of even more technical and interoperability issues, or it could conversely strengthen the need for solutions in this area and contribute to this trend of greater openness.

Evidence from the case studies:

Stakeholders across all industries see varying (non-compatible) standards as (potential) barrier for both the development of innovative products and services and of business models based on data.

In addition, differences between industries and in the cross-border context hamper the collaboration between different types of business and of sales in the Digital Single Market.

Moreover, the development and sales of innovative products and services, as well as the implementation of new business models usually necessitates investments in IT infrastructure. Depending on the size of the business and the IT legacy (i.e. the system that has been used so far) of each organisation, such costs can today appear exaggerated compared to the current benefits such products or services may yield

It is important also to understand that interoperability not only refers to the actual exchange of data but that devices need to be able to mutually check the 'correctness' of the data received in order to avoid detriment to the end-user. This is important in the context of liability claims (see also the section on legal barriers).

[125] Final result of the web-based survey

[126] Only 33% of data sharers consider interoperability as a considerable barrier while for 32% of them it is a very small barrier or not a barrier at all.

Other barriers

Key messages:

- Of the other barriers, unequal bargaining power is probably the most important although it relates mainly to the category of 'data access' stakeholders. However, there was no stakeholder consensus on either the seriousness of the unequal bargaining power problem or the possible solutions.
- Problems related to skills and issues in valuing data are much more widespread across all companies and sectors, they do not have the same negative effects of unequal bargaining power.
- Procurement barriers may also exist but only in specific cases and related mainly to portability of data.

Apart from the technical and legal barriers discussed above, the case studies also revealed that there are other possible explanations for limited access and (re-)use of data, and the limited B2B data exchange. These are in particular:

- Unequal bargaining power;
- Uncertainties about valuing data;
- Lack of skills; and
- Issues with procurement.

These barriers are described in more detail in the following sections.

Unequal bargaining power

The problem of unequal bargaining power amongst players along the value chain applies in particular to two stakeholder categories:

- Providers' competitors and same-sector downstream providers; and
- SMEs and start-ups.

Although this issue is not specific to the data economy itself,[127] and SMEs and start-ups did not raise it very frequently during the interviews and within the context of the case studies, this barrier emerged from the workshops as one of the major constraints. This was especially the case of providers' competitors and sector downstream providers.

Indeed, unequal bargaining power combined with lack of access to data creates a difficult situation for companies depending on third party data to offer their products and services. In this respect, the sector also plays a role. Certain markets (e.g. aviation) have a more complex value chain in which the status of partner or competitor is not fixed once and for all. Moreover, in the aviation sector after-sales services are provided most often by the manufacturers themselves, as product users (airline companies) do not develop these services internally.

This flexibility of roles and positions within the aviation sector, coupled with less competition between manufacturers and users in the after-sales market, makes access to data less com-

[127] Some of the SMEs interviewed argued that the unequal bargaining power is a normal condition of the market, and, from the perspective of smaller companies, the data economy is not the exception in this respect.

plex in most cases. Indeed, all players (including same sector downstream providers) can find themselves at some point de facto 'owning' the data someone else would like to have access to.

Similar conditions are not met in the automotive market in which the car manufacturers alone can produce the vehicle and repair it through the network of their authorised repairers. The lack of bargaining power of the providers' competitors and same-sector downstream providers is much more impactful, as these players cannot provide any incentive (besides remuneration) to manufacturers to convince them to open up the data be-yond what is currently imposed by legislation.

Therefore, as suggested by the evidence emerging from the case studies, the inequalities in the bargaining power might be a greater or lesser obstacle depending on the sector considered.

It is also important to note here that, when discussing this particular barrier, stakeholders often refer to competition law remedies. Some question the effectiveness of such legal remedy in this context while others suggest that competition law could be helpful in sanctioning abuse of market power on the part of certain data holders and breaking any data monopoly. Overall, in this domain there was no stakeholder consensus on either the seriousness of the unequal bargaining power problem or the possible solutions.

Valuing data

There is great uncertainty among stakeholders in relation to valuing data. However, **valuing data *matters*** as a barrier to the development of innovative business models.

A company or a data owner must put a value on its own data to claim a price for it. However, it is not always fully clear a priori what amount of money should be charged and what pricing models should be used in order for businesses to receive proper remuneration over time for giving other competitors access to and the possibility of (re-)using their data. The difficulties in valuing data can be linked to many different factors including:

- Lack of knowledge and skills of the data sharers;
- Uncertainties about data potential (and especially the value of data when combined with other, unknown, datasets).

Thus, businesses still tend to keep their data in order not to grant potential competitors (future) economic advantages based on (the analysis of) data those competitors would have never had access to in the first place – without themselves receiving a proper remuneration.

It is crucial to acknowledge this. As the future financial benefit of a certain set of data is not known today (the value is highly uncertain and only established at the point and moment of use – 'experience goods'), businesses are uncertain about the price they should charge for access and (re-)use of this set of data. Instead, businesses tend to keep the data for themselves with large enterprises trying to develop their own business models through which value can be extracted from data. This finding is consistent with theoretical economic models: traditional economic theories predict that uncertainty leads to hierarchy-based (in-house and acquisition) rather than market solutions (reselling). Thus, within the current context,

players may decide deliberately to adopt strategies to protect their own work and to preserve their competitive advantage[128].

Even when companies decide to actually share and sell data, they try to protect themselves through specific pricing strategies. In fact, according to the OECD, there have been instances in which data holders attributed higher value to the data than the market is ready to pay[129]. This seems also to be the perception of the data users and (re-)users, as shown by the results of both our surveys. Indeed, from the general survey it emerged that around 26% of respondents consider the cost of acquiring data as a considerable or very important barrier, or a blocking factor. The targeted survey presents an even higher percentage of respondents (81%) underlining the cost of data as being a major problem. This is once again logical as data-analytics and data-based businesses are those most affected by the question of data pricing. Another important problem linked to the value of data is related to the lack of data brokerage services. Such data marketplaces (such as for instance DAWEX[130] or WhoApi[131]) could help to provide both access to relevant datasets and to assign their value. However, at this stage, there do not seem to be enough of such services[132].

Skills and procurement obstacles

An additional aspect identified during our research is that data sharing and use may sometimes be hindered by a **lack of knowledge/skills**. For businesses to be able to maximise the use of their data, they firstly need to *know* about the possibilities data brings and secondly need the *skills* to implement any data analytics[133]. However, while the European Commission has estimated that approximately 90% of jobs within the EU need at least some sort of ICT skills, estimates show that roughly 37% of EU labour force is not properly digitally skilled (yet)[134]. As this and other studies suggest, not all businesses have the knowledge and skills to decide on and implement effective strategies of how to make the best use of their data. A survey carried out in 2012 by the Economic Intelligence Unit further suggests that, according to the businesses studied in that survey, the second biggest barrier to using data to make decisions is the difficulty in finding persons with the right skills to analyse the data (men-

[128] For instance, some researchers do not release their data to protect their publishing capacity, or businesses do the same to avoid favouring existing and/or potential new competitors.

[129] For instance, 'economic experiments and surveys in the United States indicate that individuals are willing to reveal their social security numbers for USD 240 on average, but the same data sets can be obtained for less than USD 10 from data brokers in the United States such as Pallorium and LexisNexis" (OECD, 2014, Data-driven Innovation for Growth and Well-being: Interim Synthesis Report). However, data can be highly valued by the market: when a large Las Vegas game business went bankrupt, its customer data were valued by creditors at USD 1 billion, far more than any of the physical properties in Las Vegas. (http://www.information-age.com/it-management/strategy-and-innovation/123460149/future-data-economy-how-measure-true-value-your-data-assets)

[130] www.dawex.com

[131] whoapi.com

[132] For a list of Data Marketplaces see: http://www.datalandscape.eu/data-landscape-type/data-marketplaces

[133] OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, p. 253, http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en.

[134] Estimates from 2015, See Commission Staff Working Document, Europe's Digital Progress Report 2016, https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/10102-2016-187-EN-F1-2-ANNEX-2.PDF

tioned by 51% of the respondents)[135]. Participants from the retail and consumer goods industries considered this issue the most important barrier.

The general and targeted surveys conducted for this study also confirm the importance of this issue of skills within the context of the data economy. Indeed, 27% of respondents to our general survey and 71% of respondents to the targeted survey stressed that acquiring the right skills is one of the major costs for their businesses. Once more, the difference between the general and the targeted survey is very telling. Data analytics companies and start-ups need a range of data skills which are very hard to find on the market, and especially in Europe – as mentioned above, and which therefore have higher market prices. Sometimes, companies even have recourse to outsourcing to free-lances and profiles from outside the EU in order to find precisely the skills they need[136].

The skills needed are a higher education degree in economics, mathematics, physics, or other relevant field of science, plus familiarity with the industry concerned.[137] The combination of all these skills is difficult to obtain.

Example from the case studies:

The analysis of the chemical industry showed the importance of skills for maximising the potential of big data. The relevant skills are a prerequisite for generating business value based on data. Advanced analytics requires software programmers as well as analysts who can combine chemicals domain knowledge with software capabilities. To give an example, a chemical company has recruited 10 PhDs in computer sciences supported by a team of advanced analytics experts to work alongside its own business intelligence and analytics staff[138]. The main challenge is not only identifying the need for those types of skill and discovering those scarce talents but also, for senior executive mind-sets, to take the advice from those typically young colleagues (often in their twenties).

Finally, interviewees sometimes also mentioned procurement barriers as possible obstacles to the B2B exchange of data. This applies mainly to storage of data and the possibility of switching Cloud Service Providers, especially within highly regulated sectors (e.g. Finance, Health). Indeed, in these sectors, companies might face some limitations in buying services from providers outside Europe, for instance, and in making sure that their data storage is compliant with the legislation. Although this is not a blocking factor for the cases examined, barriers in terms of procurement can prevent SMEs especially from freely deploying their data strategy.

---

[135] Economist Intelligence Unit (2012), The deciding factor: Big data & decision making, commissioned by Capgemini, 4 June, https://www.capgemini.com/resource-file-access/resource/pdf/The_Deciding_Factor_Big_Data_Decision_Making.pdf.

[136] As emerged from an interview with a European start-up providing smart home services.

[137] Economist Intelligence Unit (2012), The deciding factor: Big data & decision making, commissioned by Capgemini, 4 June, https://www.capgemini.com/resource-file-access/resource/pdf/The_Deciding_Factor_Big_Data_Decision_Making.pdf.

[138] See Annex 2 – Sectoral Case Studies

The effects of the problem

This section discusses the effects for businesses and consumers of the problems raised above. More specifically, the following effects have been identified:

- Effects on the Digital Single Market: innovation and competitiveness are hampered within the Digital Single Market; and
- Effects on society: there is less freedom of choice for products and services, and digital inclusion cannot fully be ensured.

These two effects are further described below.

Effects on the Digital Single Market (innovation and competitiveness)

Key messages:

- The barriers and problems identified have a direct effect on the innovation potential and performance of the Digital Single Market (DSM).
- By affecting the most innovative businesses in Europe, in particular, these barriers are slowing the innovation path of the DSM, thus limiting European competitiveness in data markets.

Successful data market players excel in the creation of new, innovative start-ups and in the increased competitiveness of EU businesses in the global markets, thus triggering economic growth and the creation of new high-skilled jobs. As underlined by many business reports, "removing barriers faced by digitally intensive firms can increase GDP, wages, sales and employment at the same time."[139] In the current situation, the impediments to data sharing are expected to affect development of the Digital Single Market directly in these ways, i.e. the will have a negative effect on innovation and competitiveness. This is particularly true if one considers that highly innovative companies (the most intensive data users) are those which suffer more from the barriers and problems analysed above.

The **potential of data-driven business models for innovation** has been analysed in recent OECD publications. It was highlighted in a 2015 study on data-driven innovation that "data are an increasingly significant resource that can drive value creation and foster new industries, processes and products."[140] This is valid across sectors, including traditional non-data driven sectors (e.g. agriculture)[141]. Although data was also important before the digital revolution, its potential for economic growth has been given a new impetus.

[139] *Putting Data to Work. Maximising the Value of Information in an Interconnected World*, Business Roundtable, http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf

[140] OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, p. 132, http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en.

[141] OECD (2016), Maximising the Economic and Social Value of Data – Understanding the Benefits and Challenges of Enhanced Data Access, p. 6. The following article presents examples of data-driven innovation in the health sector: http://www.informationweek.com/government/open-government/9-healthcare-innovations-driven-by-open-data/d/d-id/1317530

There are three main reasons[142]:

- **The exponential increase in the volume of available data**: as our world is becoming increasingly digitised, the amount of available data has been increasing quickly. For example, sensor networks and IoT connected devices generate huge volumes of data.
- **The development of data analytics**: the means of analysing and making the best of the existing data, including analytics/algorithms and cloud computing, have been increasing as well.
- **Changes relating to the creation of knowledge and decision-making**: the first two factors facilitate new ways of creating knowledge based on data, which can then be used by businesses for making decisions. Indeed, many businesses already use big data to support or even automate their decisions and those who do tend to generate higher outputs.[143]

It can be expected that economies in which these factors apply to a greater extent will be more likely to benefit from data-driven innovation. This does not mean that all factors need to apply fully for data-driven innovation to occur in a given country or market, as they could also benefit from data products stemming from other countries/markets. Yet, in an ideal situation, capacities to supply and use data and analytics exist at the same time: "a well-functioning supply side is a precondition for the development of a thriving data ecosystem, while a well-functioning demand side enables data-driven entrepreneurs to use data and analytics to innovate goods and services across the economy." [144]

Consequentially, any barriers to the supply and use of data and analytics potentially hinder innovation. This includes the technical, legal and other barriers identified in the previous section, as they impede data sharing and use, thus decreasing the opportunities for businesses to exploit their own and external data for making decisions and developing more business models.

[142] Based on OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, pp. 132 ff., http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en.

[143] The OECD quotes a survey by the Economist Intelligence Unit (2012), which found that almost 60% of business leaders use big data to support decisions. Almost 30% use it for decision automation (OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, p. 150, http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en).

[144] OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, p. 132-133, http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en.

Evidence from the case studies:

At the macro-level, several case studies have pointed to the potential impacts of barriers to the data economy.

For instance, in **agriculture**, less technology shrewdness or financially equipped farmers could face competitive disadvantages in the Internal Market compared to large-scale farming companies or networks that are able to share the financial burden of investments in the necessary hard- and software.

In the **retail sector**, the case study argues that the DSM today already faces a de facto monopoly of Google and Apple – non-EU enterprises – who have developed programming standards that are used by the entire industry with no real incentives to invest in the development of own standards to increase competition. The case study on the financial sector, on the other hand, argues that data sharing imposed by legal obligations (under PSD2) could contribute to disrupting the entire sector – thus spearheading competition and innovation.

Conversely, however, **mHealth** stakeholders argued that the adoption of early regulation might focus too much on issues that would in the future be easily solved via market mechanisms – thus neglecting the potentially disruptive effects of data sharing legislation.

However, as impacts are long-term effects by definition, the current costs imposed on businesses and slowing the development of the Digital Single Market cannot be regarded as 'value that is taken away from the market now' but rather as 'value that the market cannot realise at the moment'. More analytically, this means that the costs for businesses and consumers equal business opportunities foregone (i.e. opportunity costs)[145] and mean the Digital Single Market is not achieving its growth potential. This means that, as businesses and consumers face undue costs, the Digital Single Market is not evolving as fast as it could because of the technical, legal, and other barriers discussed For instance, a 2013 report estimated that "if cross-border data flows were seriously disrupted in the European Union, the negative impact on its GDP would be between 0.8 to 1.3% and EU manufacturing exports to the United States could decrease by approximately 11%."[146]

It is always challenging to assess opportunity costs quantitatively. However, some of the estimates available on costs for businesses that may shed light on the impact on the Digital Single Market have already been mentioned in the section on the assessment of the problems. They include the estimates on the growth of the data economy in Europe and on the efficiency gains firms could achieve through further exploitation of data[147].

[145] Cf. OECD (201 6), Maximising the Economic and Social Value of Data – Understanding the Benefits and Challenges of Enhanced Data Access, p. 4.

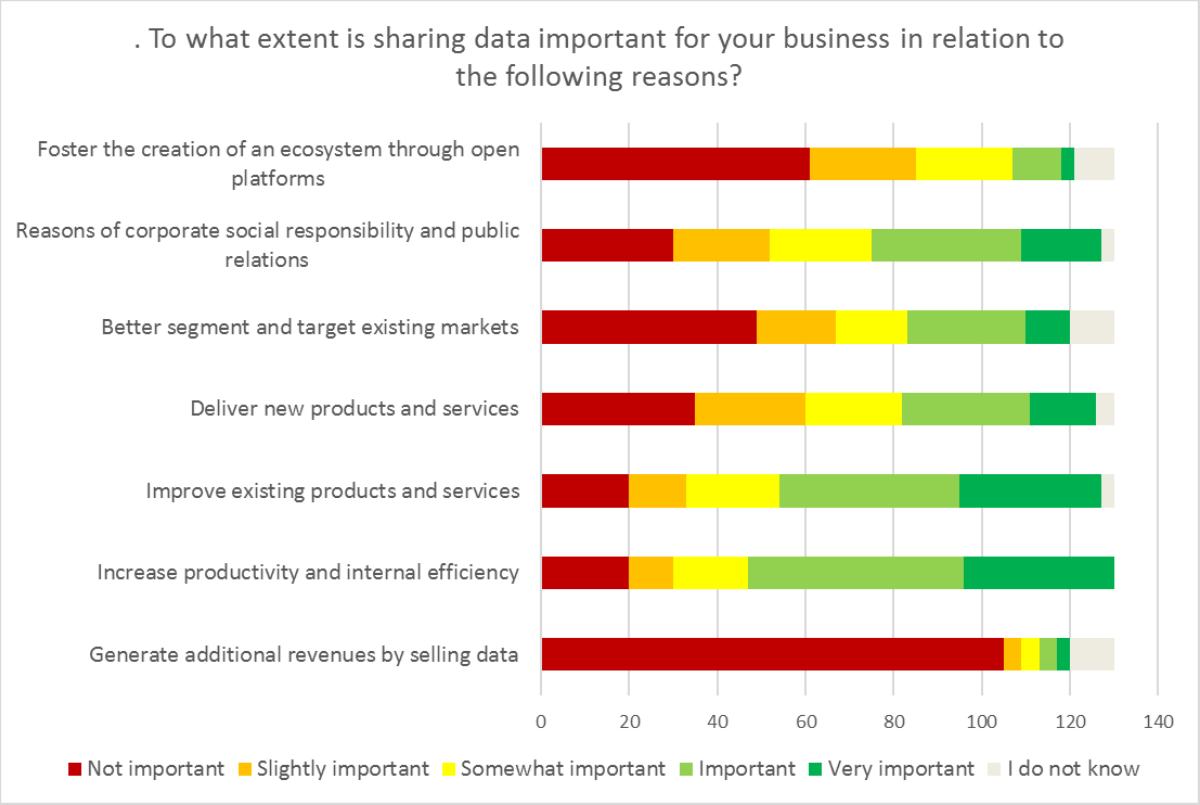
[146] Matthias Bauer et al., *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, European Centre for International Political Economy, March 2013, 3.

[147] See See p. 30, *Second Interim Report, European Data Market Study*, June 2016, http://www.datalandscape.eu/study-reports and European Political Data Centre (EPSC) strategic note 'Enter the data economy': https://ec.europa.eu/epsc/publications/strategic-notes/enter-data-economy_en; European

When looking at survey data, there are clear distinctions to be made between the benefits identified by companies in both sharing and accessing data. Companies were asked about the importance of data sharing and data accessing for their businesses in relation to different factors on what was de facto a scale of one to five. Multiple choices were possible.

As the figure below suggests, the main benefits of data sharing lie in productivity and internal efficiency, followed closely in improving existing products and services. At the other end of the spectrum, benefits in terms of data monetisation and creation of an ecosystem are perceived as much less important, while public relations/CSR motives, as well as better targeting and creating new products and services, are between the two.

Figure 12: Reasons for sharing data



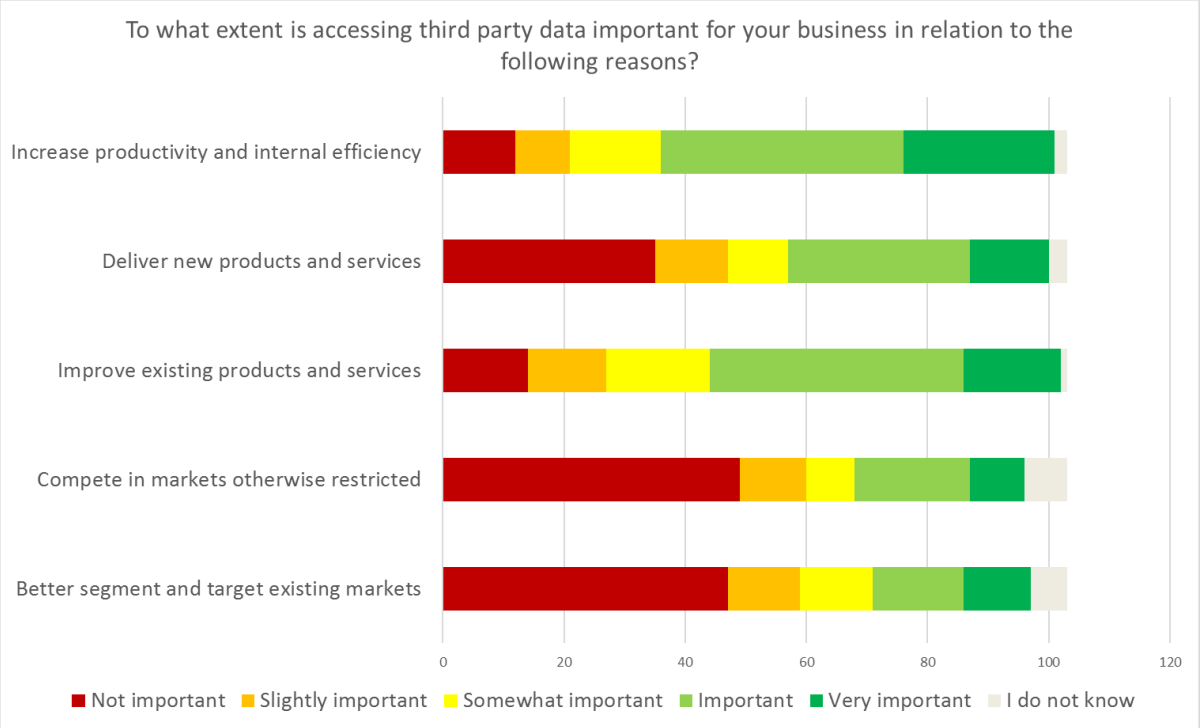
Source: Deloitte, General Survey

When looking at accessing third party data, the results are similar but with some noticeable differences. Productivity improvements and incremental innovation to existing products are still the main benefits, and more so than new products and services. However, there is a far greater polarisation of opinion around the average importance of the delivery of new products and service than for other questions: 34% of respondents assert that data access is not important, while 42% consider it important or very important.

On the other hand, better market segmentation and competing in new markets appear to be less important.

Commission (2016), The EU Data Protection Reform and Big Data, http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf.

Figure 13: Reasons for accessing data



Source: Deloitte, General Survey

In summary, this analysis confirms that, on the one hand, in general at this early stage of the market companies are focusing more on short-term gains and internal use of data for process optimisation than on disruptive innovation. Therefore, for this type of company, the negative effects linked to the barriers to data sharing and access are more limited.

However, on the other hand, for a small number of highly innovative companies, accessing third party data is very important for disruptive innovation and for making the Digital Single Market competitive on the global stage. Therefore, there is a case for arguing that these barriers hamper the potential of the Digital Single Market by constraining, in particular, those companies (intensive data users) which would contribute the most to making it highly innovative.

Effects on society (freedom of choice and digital inclusion)

Key messages:

- Side-effects of the data economy could consist in limited freedom of choice for consumers and limits to digital inclusion.
- If data holders have unlimited power over their data and create data monopolies, consumers might see their freedom of choice of products and services reduced, as some product and service providers will disappear.
- The barriers and, for instance, the lack of skills or costs could mean that not all stakeholders will able to benefit equally from the data economy. There is a risk of some being excluded.

The data economy is expected to have a vast impact on EU society. Potential positive impacts range from better information for citizens to increased freedom of choice for consumers, as well as *more democracy* through the use of eGovernment solutions.

However, the data economy may also be considered to have negative impacts on society as a whole, especially as long as businesses, consumers, and public authorities alike face technical and legal uncertainty or grey areas that may e.g. conflict with Fundamental Rights, such as the right to privacy and the security of data processing activities.

Evidence from the case studies:

As part of the agriculture case study, for instance, concerns were voiced in relation to the impact of digitisation on freedom of choice for and prices paid by consumers. The issue here is that, although data sharing can have positive benefits for the efficiency of operations and thus decrease production costs, market actors could also use the information collected to bet against markets and only focus on products that are bought by the (vast) majority of consumers. In both cases, the adverse effects of efficiency would be apparent and impact negatively on society compared to today.

Similarly, independent car repairers argue that, if the issue of their access to vehicle data is not solved, consumer choice will be dramatically reduced as consumers will only be able to buy repair services from the car manufacturers themselves. Therefore, the barriers identified in the previous sections can lead to a reduction in consumer welfare.

Moreover, digital inclusion is regarded as an issue. There seems to be differences in the speed at which the data economy and the necessary supply of skilled labour are evolving. As indicated above, estimates show that, in 2015, roughly 37% of EU labour force lacked the requisite digital skills[148]. Unaddressed, this could result in 756,000 to 825,000 jobs for ICT professionals potentially remaining unfilled in 2020[149]. With respect to data, recent studies suggest that, if the market evolves according to the current trends, there will be a gap corresponding to 536,000 data workers in 2020[150]. On the other hand, if the take-up of the data economy accelerates, the gap will be even bigger (corresponding to over 30% of the demand for skilled data jobs)[151]. These estimates suggest that the magnitude of the problem will increase further in the years ahead and that data shortages are to be expected if no action is taken.

Evidence from the case studies:

Several interviews, especially from SMEs, provided concrete examples of data-related jobs and positions already remaining unfilled because of the scarcity of relevant profiles. In

[148] See Commission Staff Working Document, Europe's Digital Progress Report 2016, https://ec.europa.eu/transparency/regdoc/rep/10102/2016/EN/10102-2016-187-EN-F1-2-ANNEX-2.PDF

[149] COM(2016) 381 final: A New Skills Agenda for Europe : Working together to strengthen human capital, employability and competitiveness. SWD(2016) 195 final, p.7.

[150] See: *European Data Market Monitoring Tool*, IDC 2015; http://www.datalandscape.eu/european-data-market-monitoring-tool

[151] Ibid

some cases, the solution was to outsource these positions outside the EU, where there is a larger spare skill supply[152].

As matters currently stands, the existing technical and legal barriers are expected to affect negatively the achievement of the potential positive impacts of the data economy while simultaneously contributing to negative impacts. This means that the current barriers contribute to increasing the societal opportunity costs, i.e. the *benefits foregone of what could already have been achieved*.

Liability of IoT, robots and autonomous systems: the problem, its causes and effects

This section contains the problem assessment on issues relating to the liability of IoT, robots, and autonomous systems. It follows the same structure as the problem assessment on access and (re-)use of data.

Problem tree: the logical links between the problem, its causes and effects

Key messages:

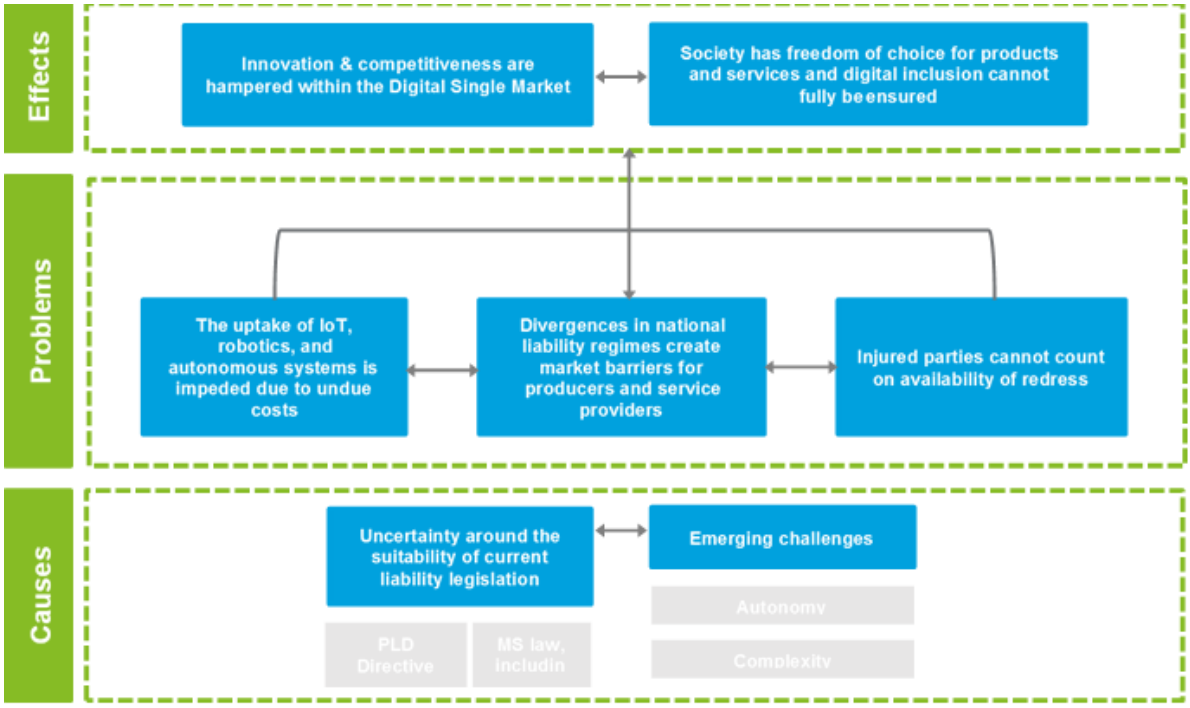
- The main hypothesis of this study is that the development and uptake of the IoT, robotics and autonomous systems in the EU is hampered by deficiencies in liability legislation. This is due on the one hand to their non-deterministic autonomy, and on the other hand to their complexity.
- This leads to certain problems affecting businesses (both manufacturers and those using the devices) and consumers.
- Different companies will face different barriers in the IoT, robotics and autonomous systems' markets, and therefore the analysis of the context (that is to say the market development stage of the company/business considered) and preconditions (meaning the sector, position in the value chain and size of the company) are also important elements for a sound problem assessment.

The main hypothesis underlying this study is that the development and uptake of the IoT, robotics and autonomous systems in the EU is hampered by deficiencies in liability legislation. More specifically, liability legislation is currently based on certain assumptions on the nature of products and services, and on the role and responsibilities of the stakeholders surrounding them. These do not necessarily hold true of the IoT, robotics, and other autonomous systems market.

This understanding is depicted in the figure below.

[152] See case study on finance and recent data on shortage of IT skills from Eurostat, http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises

Figure 14 : Our understanding of the problems related to IoT, robots and autonomous systems liability, their causes, and impacts (problem tree)



Source: Deloitte

The problem tree should be read from the bottom to the top. Each of the elements mentioned in the problem tree is described in-depth in the following sections.

Before embarking on the analysis, it is also important to note here that, for the purposes of this study, the following working definitions were applied:

- 'IoT' refers to the 'Internetworking' of/within physical device(s), allowing them to collect, exchange or otherwise process data (semi-)autonomously based on sensors, actuators or algorithms in order to support certain functionalities; and
- 'Robotics' refers to mechanical or virtual agents embedded in physical devices that allow the devices to act (semi-)autonomously.

Examples include complex forms of robotics such as self-steering drones and self-driving cars, but also household domotics (such as robot vacuum cleaners and lawnmowers etc.), and industrial robots such as maintenance/construction robots.

Examples of IoT include smart energy grids (e.g. measuring and communicating electricity production and consumption), smart cities (e.g. using sensors to only use city lighting when there are people nearby), and smart agriculture (e.g. using sensors to detect soil humidity, produce growth and detect possible crop diseases).

From a technical perspective, both the IoT and robotics devices are fundamentally data-driven. They depend on data collected via sensors, which are either integrated in the devices themselves or provided from external sources. This data is then processed through an internal logic by a control centre, which can similarly be integrated into the device itself or external, e.g. via a cloud service or remote artificial intelligence. The logic can be either static or

evolutive, meaning that parts of the processing logic may change as a result of prior usage. Finally, based on this processing, the device can actuate in its environment, either through a physical action, or by providing further data to external sources (such as online services or other robots or IoT devices). Complexities can therefore occur in each of these three stages: the initial collection of data, the processing activities and the actuation.

It is clear that these are not operating in an unregulated space; on the contrary, there is a wide body of law at the EU and national level governing their safety. Depending on the type of robots, they can be governed by the Machinery Directive, Medical Devices Directives, the Low Voltage Directive, the Toys Directive, the Radio Equipment Directive, Electromagnetic Compatibility Directive, or the OSH Framework Directive, among others[153].

Defined in this manner, the IoT and robotics or other autonomous systems display certain characteristics that can cause liability challenges. Firstly, they relate to **physical devices**, which can interact with objects in the physical world. Their actions and the consequences thereof –including potential harm – are not necessarily limited by a digital or otherwise virtual environment. They can have a physical impact, potentially implying material/physical damage/harm. This characteristic as such is not problematic as it applies to other types of products as well.

However, the second characteristic is that the devices which are relevant to this study are **(semi-)autonomous and/or self-actuating**, in the sense that they can act upon their environment without being fully controlled by a human being (e.g. they can act based on a stimulus –algorithms, actuators, sensors- that are only partially controlled by a human being). In that sense, the IoT devices and robots being considered in this study could be described as **non-deterministic:** their actions and the potential consequences are not fully defined and predictable when they are taken into use. If the behaviour of a device or robot is fully deterministic, in that all its actions are static and pre-programmed – as is the case e.g. with kitchen robots or even complex assembly robots on manufacturing production lines – liability issues are easier to address; such devices are therefore outside the scope of this study.

A complex facet of this problem of non-determinism is the potential of robots or devices to be **self-learning or self-modifying**. This implies that they may be able to integrate past experiences (in the form of historical data) to adapt their future behaviour: pre-programmed routines may be modified, or the application of the routines may result in new behaviour, without the owner or controller of the device being able to predict the new behaviour.

[153] See a broader overview of relevant legislation at http://www.newapproach.org/Directives/DirectiveList.asp, an overview of standards at https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_en, and http://ec.europa.eu/information_society/newsroom/image/document/2017-30/felicia_stoica_-_the_existing_eu_safety_framework_with_regard_to_autonomous_systems_and_advanced_robots__iot-systems_6210B836-9707-D592-D33613EE1C6F086A_46145.pdf for an overview presentation of the main features of this framework.

The devices and robots under examination in this study are thus **data-driven**, not in the sense that they are programmed – which would be true for deterministic robots as well, but in the sense that they are dependent on sensors or external data sources to provide information to them. They then actuate this information in their environment based on nondeterministic pre-programmed routines. This creates attribution challenges: to which entity (human or company) is the behaviour of a robot or device assigned, and who is to be required to bear the liability for any damage caused?

This characteristic of non-deterministic autonomy is the first key challenge to liability law: as will be further examined below, existing liability rules are based on an assumption of static products whose use is predictable for their owner or user. Can the same rules be applied in situations where the owner or user may have no reasonable way of knowing how their property will behave?

The characteristic of non-deterministic autonomy is not the sole cause of the problem. **A second characteristic of the IoT, robotics and autonomous systems market is its complexity.** This is on the one hand due to the technological complexity of the devices themselves, making them, and potential safety and liability issues, difficult to assess, and on the other hand due to interdependencies: the devices interact with other devices, software and data streams in a way that makes it difficult to determine where a defect has occurred, even after harm has been clearly established.

As will be further described below, there are a number of concepts which describe how liability claims can be structured:

Table 5: Theories on which liability claims can be based

Basis for liability claims and concepts of damage	
Contractual liability	**Extra-contractual liability, including Torts**
Compensatory (actual) versus punitive versus nominal – Direct versus indirect – Intentional versus unintentional and (grossly) negligent - Incidental, special, strict or consequential – Material (including physical and lethal harm) and immaterial (including notably lost profits, lost business opportunity and reputational harm)	

Source: Deloitte

Without attempting to address every detail, these concepts can be summarily described as follows:

Table 6: Differences between different types of liability

Type	Description	Example
Contractual liability	Any liability assumed by a party to a contract or in relation to a contract. Such liability occurs when a party to the contract fails to perform in accordance with	A connected car's sensor mechanisms fail to perform as agreed between the manufacturer of the car and the manufacturer of the sensor. The manufactur-

Type	Description	Example
	the terms. . Contractual liability may be the result of explicit statements in a contract in which the party delineates its obligations and/or liabilities, but it can also simply be the result of the application of the law to a failure to perform a contract as required. As such, contractual liability is of course largely shaped by the terms of the contract.	er of the sensor will be contractually liable to the manufacturer of the car.
Extra-contractual liability	Any liability for damage caused by an injuring person to an injured person outside the context of any contract that may exist between them. Extra-contractual liability will thus generally apply when intentional or negligent acts or omissions are the cause of damage to a third party. Extra-contractual liability includes but is not identical to tort law. 'Tort' is a broad term originating from English common law that encompasses a number of legally recognisable non-contractual causes of harm, defined by jurisprudence or statute; it is thus not a generic and neutral term. To avoid misunderstandings, the more generic concept of extra-contractual liability is used in this report[154].	A connected car's sensor mechanisms fail to detect a pedestrian, who is run over as a result. The driver of the car will be liable to the pedestrian for his/her failure to control the vehicle as required, assuming that no legislation is in place exempting a driver from their obligation to control a vehicle when driving a connected car.

Source: Deloitte

Contractual and extra-contractual liability can be imposed or mandated by specific legislation, notably when the law requires that certain types of liability are assumed or forbids certain types of liability being disclaimed; in this case, the liability is referred to as **statutory liability**. By way of example: if a connected car's sensor mechanisms fail to properly detect its lanes, causing it to swerve off the road and into a tree, and resulting in an injury of the driver, the driver can claim damages from the car manufacturer on the basis of product liability legislation[155].

[154] The same rationale was followed in the Book VI – Non-contractual liability arising out of damage caused to another, from the Principles, Definitions and Model Rules of European Private Law Draft Common Frame of Reference (DCFR); see http://ec.europa.eu/justice/contract/files/european-private-law_en.pdf

[155] Assuming that the driver might reasonably expect that the autopiloting function should have been capable of keeping the vehicle in lane; this can be strongly affected by the manufacturer's communication and assurances on this point.

Contractual liability generally presents no challenges that are unique to the IoT, robotics and autonomous systems. Issues of fairness and market power can certainly arise, as can doubts on the appropriateness of contractual liability limitations and exclusions, but these issues are relatively general in nature and do not necessarily indicate a problem that must be addressed. **Extra-contractual, specifically product liability law, as a form of statutory extra-contractual liability, are affected by the complexity of the IoT, robotics and autonomous systems**: extra-contractual liability generally requires that a fault, damage and a causal link between both are proven, and product liability law requires that the injured party prove the damage, the defect, and the causal relationship between the two. In both cases, the complexity of the device and the entire ecosystem around it can make it highly challenging for even experts in the field to determine if and where a fault or defect existed. **This is the second key challenge to liability law: to the extent that compensation requires proof of a fault or defect, the complexity of the IoT, robotics, and autonomous systems will make it substantially harder to provide such proof, thus potentially undermining the effectiveness of product liability law**.

These two challenges – non-deterministic autonomy and the complexity of proving causality - create problems in the application of liability laws to the IoT, robotics, and autonomous systems. This can have a negative impact on the Digital Single Market and the EU society.

In the following sections, we examine the identified problems, their causes, and effects closer. Illustrative evidence is provided by way of example to underpin the findings.

Determinants of the type and magnitude of problems

Key messages:

- The IoT, robotics, and autonomous devices market are not a 'one-size-fits-all' market. The type of product strongly affects the risk profile, the type of harm that can result, and the complexity of ensuring appropriate and effective liability assurances.
- In terms of position in the value chain, companies can be manufacturers, importers, vendors or users of robots or devices. Each of these categories has its own characteristics in terms of liability needs and risks. This affects the importance of certain barriers.
- Especially when focusing on non-deterministic autonomous devices, this is an emerging market in which even the stakeholders do not have a clear perspective on likely liabilities and how to manage them.

Each of these important elements is detailed below.

Diversity of the market

The market for IoT, robotics and autonomous devices can be examined on the basis of a number of axes – essentially the characteristics of the products in question – which also impact the resulting liability issue that the stakeholders face.

Axis 1 - Autonomy

This first axis relates to the degree of autonomy that a device has to actuate in its environment, and specifically to the degree of human involvement in either steering the device directly, or in controlling the flow of information that allows the device to determine its actions. The Table below covers semi-autonomous and autonomous devices. Non-autonomous devices – where a human controls the device fully at all times, are out of scope of the present study.

Table 7: Liability-related differences between IoT, robotics and autonomous devices with differing degrees of 'autonomy'

	Semi-autonomous	Autonomous
What?	Human controls operation of the device *e.g. smart car with lane support – speed control*	Device operates fully independently *e.g. smart car – self-driving*
Implication?	Driver bears some liability	Liability must go 'elsewhere'

Source: Deloitte

The table above illustrates the different degree of challenges for these archetypes of devices in relation to liability: if a human controls the device to a substantial degree, the human can be expected to bear at least part of the liability. This becomes more complex in a fully autonomous device: liability could be attributed to the owner of the device, its user, the manufacturer, the entity that brought it to market, the entity that chose to use it for a specific application area, etc. Conceptually, liability could even be attributed to the device itself, although this would require prior intervention to ensure that devices have the means to compensate victims (e.g. by endowing them with 'capital', comparable to limited liability corporations, or by requiring third parties to provide coverage for the device through e.g. insurance mechanisms).

Axis 2 – Determinism

The second axis relates to the degree to which the actions of the device are fully pre-programmed or determined algorithmically.

Table 8: Liability-related differences between deterministic and non-deterministic IoT, robotics and autonomous devices

	Deterministic	Non-deterministic
What?	The actions of the device are fully pre-programmed, possible inputs are known and possible outcomes are fully predicable *E.g. a manufacturing robot is used on a manufacturing production line. It assembles known outputs from known inputs.*	The actions of the device are determined algorithmically; neither the inputs nor the outcomes are exhaustively defined *E.g. a logistics robot moves crates based on an automated reading of its environment. The shapes and weights of crates are not known in advance, nor is the*

	Deterministic	Non-deterministic
		environment from/to which the crates are moved
Implication?	Liability issues are nearly perfectly foreseeable except in the event of defects	Even without defects, unforeseeable liability issues can occur

Source: Deloitte

As the introductory sections above have indicated, liability issues are more likely to occur with non-deterministic devices. Self-learning or self-modifying devices are significantly more likely to be non-deterministic: their capability to change their behaviour may over time result in different outcomes for inputs that are identical (i.e. faced with exactly the same sets of inputs, a robot may, after a certain amount of time, begin to behave differently in response to the inputs due to learned or modified behavioural rules). This can create bigger liability challenges since the use of the device cannot necessarily predict its behaviour, and may thus be unable to correctly predict risks and liabilities.

Axis 3 – Dependence

The third axis relates to the degree to which the actions of the device depend fully on data derived from its own sensors or on external data.

Table 9: Liability-related differences between self-contained IoT, robotics and autonomous devices and such that rely on external data

	Self-contained	External driver
What?	Device depends fully on its own sensors to determine its actions *e.g. agricultural drone detects soil humidity and irrigates when needed*	Device relies on external data to determine its actions *e.g. agricultural drone obtains soil humidity data from land sensors and irrigates on that basis*
Implication?	Drone errors originate solely from drone; liability is relatively simple to attribute	Drone errors may have external causes; liability can be highly complex to attribute as it may not be clear where a fault or defect occurred

Source: Deloitte

The case of fully self-contained robots or devices is relatively simple, since an injured party does not necessarily need to consider the breadth of an ecosystem in which there are many potential causes of harm. However, self-contained devices rarely operate in full isolation: the example of an agricultural irrigation drone will typically depend on a software environment that analyses data and feeds it back to the drone. If the drone behaves in a manner that causes harm, the defect may be with the software environment rather than the drone. In such cases, an analysis of the drone would show no defects.

Axis 4 - Operating environment

The fourth axis relates to the degree to which the devices operate in a clearly demarcated or unbounded space.

Table 10: Liability-related differences between bounded and unbounded IoT, robotics and autonomous devices

	Bounded	Unbounded
What?	Device operates in a clearly demarcated and homogenous space *e.g. delivery robot in a storage facility*	Device operates in an unbounded or heterogeneous space *e.g. delivery drone in public airspace*
Implication?	Risk can be managed within the space	Risk may escape its spatial boundaries

Source: Deloitte

The risk and liability management of bounded robots and devices is easier. A first step is of course ensuring that the bounds are real, e.g. by physically limiting mobility of the device, energy constraints, operational and logical constraints, and so forth that reasonably bind the device to a knowable and relatively controllable space. Once this is done, measures must be taken that limit risk exposure and liability, and the potential bearers of liability must provide acceptable resources to meet their liability risk (through capital, insurance, etc.). Whether this is possible or not is use-case specific: the example of drone delivery services through public airspace is not capable of being bounded, other than by the range limitation of the drones. Such unbounded cases therefore do not permit risks and liabilities to be defined or managed easily.

Axis 5 – Risk context

The fifth axis relates to the degree of risk that devices' errors may pose for their owners, businesses, the environment, or society at large etc.

Table 11: Liability-related differences between IoT, robotics and autonomous devices in low and high-risk environments

	Low	High
What?	Device errors are (relatively) low impact *e.g. vacuum robot short-circuits and causes fire*	Device errors are (relatively) high impact *e.g. nuclear facility maintenance robot short-circuits and causes fire*
Implication?	Liabilities are foreseeable and manageable	Liabilities may escalate

Source: Deloitte

Some robots and IoT devices have relatively low potential for harm due to their risk context. House domotics may endanger the physical integrity or security of their users and their living environment (up to and including death, e.g. in the example of fires), but have less potential for causing damage outside of that risk context. Robots or devices that operate in a high-risk

environment such as nuclear facilities or Seveso sites can create harm that extends far beyond their bounded environment. Furthermore, it should be noted that multitenancy – i.e. cases where multiple independent devices operate in a shared environment – can affect risk contexts, since actuation of one device might affect the risk context of all other devices. Thus bounded devices do not necessarily imply low liability risks.

This axis is relative: networked devices can cause harm outside their risk context due to security issues. By way of example: the October 2016 large-scale attacks from the Mirai botnet, resulting in a 620 Gbps DDNS attack that temporarily crippled Amazon, Netflix, Reddit, Spotify, Tumblr and Twitter were found to be driven by weaknesses in IoT devices – mainly security cameras – from XiongMai Technologies. A design flaw in these devices made them vulnerable to abuse by hackers. This shows that risk contexts need strong measures to avoid breakouts.

Conclusions in relation to the axes

The axes above aim to illustrate that the IoT robotics, and autonomous devices markets are not a 'one-size-fits-all' market. The type of products strongly affects their risk profile, the type of harm that can result, and the complexity of ensuring appropriate and effective liability assurances.

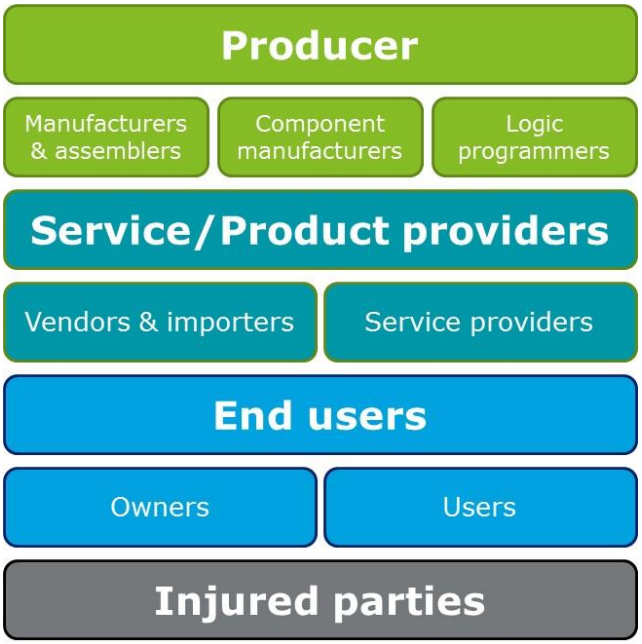
These observations may seem trivial, but they are crucial to understanding liability challenges. The concepts of IoT and robots are extremely broad, covering vast ranges of application areas and use cases, with very different risk profiles. It is therefore also difficult to conclude that there is a problem horizontally in relation to all IoT devices or in relation to all types of robotics: even leaving aside the challenge of finding a functional definition of these concepts, the reality of liability can be very different.

Therefore, the sections below will examine not only the IoT and robotics market in greater detail, including the relevant stakeholders, but also the characteristics of the legal framework for liability and precisely which provisions cause the problem in this emerging market.

Diversity of the relevant stakeholders

Examining the stakeholders in the IoT robotics, and autonomous devices market from a liability perspective – i.e. examining only those that are likely to be impacted by liability for specific defects or incidents, and thus excluding e.g. regulators, standardisation bodies, supervisors and representative organisations – the following picture emerges:

Figure 15: Mapping of types of stakeholder in the context of IoT, robotics and autonomous devices



Source: Deloitte

The graphic above describes the stakeholders in four categories, which can overlap:

- The **producers** are the entities that manufacture an IoT device, robot or autonomous system, either by:
  - manufacturing it from scratch or assembling it from pre-existing components;
  - manufacturing the physical components that will constitute the device or robot; or
  - providing the logic (the programming routines) that will drive all or part of the device or robot.
- The **service or product providers** are those who will offer a product or service in the market consisting of using the robot or IoT device. This includes:
  - direct vendors and importers, i.e. those who will simply buy a robot or device and sell it in unmodified form;
  - service providers who will offer a service that contains, integrates or uses the robot or IoT device. A key distinguishing element is that the customer does not necessarily or only become the owner of a device or robot, but enters into a service agreement with the service provider, e.g. for collection or analysis of data from the robot or device, or in relation to the use of a robot or device.
- The **end users,** i.e. those who buy a robot or device as end-users (without the intent of building their own product or service around it, since those would be service/product providers in the category above), or those who use a robot or device without necessarily owning it, e.g. as the beneficiaries of a service around the robot or device.
- The **injured parties,** i.e. those that suffer harm in relation to the use of a robot or device. Note that these are not necessarily owners or users; injured parties can simply be passers-by who were nearby when an incident occurred. Various categories of injured party could be distinguished based on the types of damage they have suffered;

the Product Liability Directive e.g. covers only damage caused by death or by personal injuries, and damage caused to private property other than the defective device itself. Other types of damage include nonmaterial damage, such as reputational harm, loss of profits or business opportunities, etc. Loss and corruption of data are presently not unambiguously categorised as one or the other.

This overview of stakeholders shows the complexity and nuances of the IoT, robotics and autonomous devices ecosystem. This is relevant from two perspectives. Firstly, in the sections below, we will examine to what extent the problems in relation to liability are addressed by current liability legislation. The overview above shows the stakeholders whose interests can be affected by liability concerns. Therefore, we will need to determine if and to what extent liability legislation recognises their role and interests.

Second, the overview also demonstrates that liability in relation to the IoT, robotics and autonomous devices is not purely a matter of product liability law. An extensive ecosystem of services is being built around robotics, and the IoT, and an approach that focuses exclusively on product liability thereby risks overlooking the most important part of the challenge. The fact that the data economy is moving increasingly to a service-based model rather than an ownership model implies that discrimination can arise which can affect the IoT and robotics as well: the buyer of a device might be legally protected under product liability laws, whereas a person who uses the robot or device as a service is largely subject to standardised terms and conditions. The behaviour might be economically identical, but still receive different and unequal treatment without a rational justification. To address this, at a minimum, a single understanding is needed on the scoping of the 'product' concept in the data economy, and the extent to which it encompasses services that are an intrinsic part of the usage of a robot or device.

Innovation-driven markets are (only) emerging

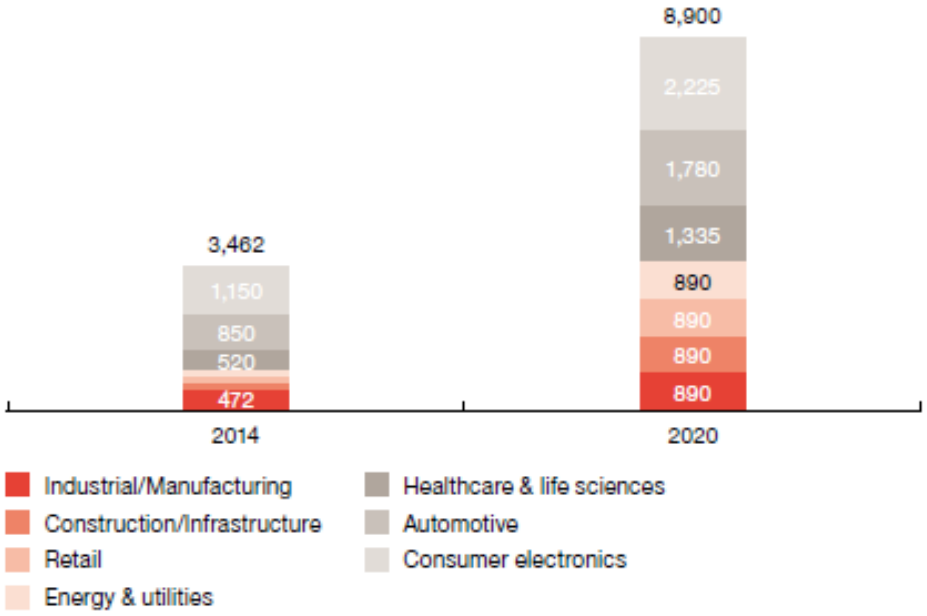
In the sections below, the causes and drivers of the problems in the market will be identified, followed by an assessment of the problems and the resulting effects. A challenge in this respect is that the IoT, robotics and autonomous systems market can be qualified as an emerging market in which rapid innovation is constantly ongoing.

Gartner, for instance, estimated in 2015 that, in terms of hardware spending, consumer applications would amount to USD 546 billion in 2016, while the use of connected things in the enterprise would hit USD 868 billion in 2016. This was projected to increase to USD 1,534 billion and USD 1,477 billion in 2020 respectively.[156]

PwC has estimated that the global IoT market will grow from USD 3,462 billion in 2014 to USD 8,900 billion in 2020 with the consumer electronics market taking the largest share of the overall value.

[156] See: http://www.gartner.com/newsroom/id/3165317

Figure 16: Estimated IoT market values today and in 2020 for different industry sectors

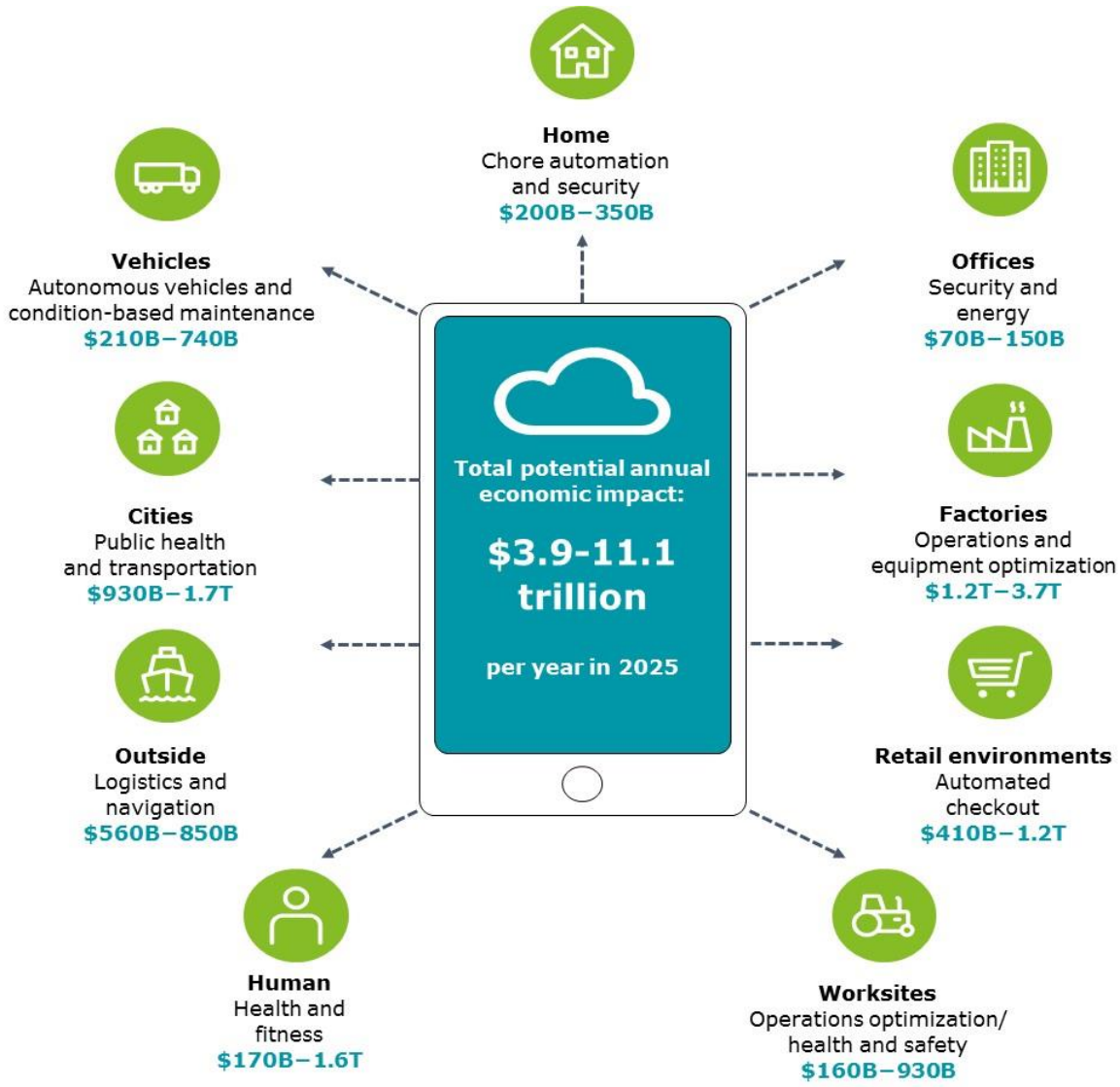


Source: Industry Forecasts Compilation, 2020 forecast from IDC, PwC analysis[157]

In 2015, McKinsey estimated a potential global economic impact of as much as USD 11.1 trillion per year in 2025 for IoT applications.

[157] See: http://www.pwc.nl/nl/assets/documents/pwc-internet-of-things-semiconductors.pdf

Figure 17: Projected annual economic impact of IoT appliances in nine different sectors (in 2025)



Source: McKinsey[158], adapted by Deloitte

This rapid but unpredictable growth expectation comes very much to the fore when consulting the stakeholders on the categorisation and quantification of problems and of potential solutions: recurring themes are the lack of quantitative estimates and the absence of experience with liability challenges, and the request to avoid sweeping revisions to the legal framework in a manner that singles out the IoT or robotics specifically and could harm European innovation in a quintessentially global market.

The emphasis of this study is therefore to ensure that the legal framework for managing liabilities in the IoT and robotics market is fit for purpose, addressing the problems identified

[158] See: https://www.mckinsey.de/files/unlocking_the_potential_of_the_internet_of_things_full_report.pdf

above – resulting from the non-deterministic autonomy and complexity of this market – without negatively impacting innovation and competitiveness in Europe[159].

The next section provides an analysis of the causes, problems and effects presented in the problem tree taking into account all these hypotheses and preconditions.

The problem, its magnitude and the stakeholders affected

The description of the current state of play results in three specific categories of problem:

- Undue costs are impeding the uptake of IoT, robotics and autonomous devices by producers, service providers and end users;
- Divergences in national liability regimes constitute market barriers for producers and service providers; and
- Injured parties cannot count on the effective availability of redress in the event of harm.

Undue costs are impeding the uptake of IoT, robotics and autonomous devices

There is only a limited amount of information available on the magnitude of costs incurred by businesses as a result of the barriers identified. Logically, however, the fact that legal uncertainties exist with respect to key questions, such as the applicability of product liability law, the concept of a defect for self-learning or evolutionary products, and the impact of the behaviour of end-users creates compliance and risk management costs for manufacturers of IoT devices and robotics, and for service providers offering services around IoT devices and robots that could be avoided or at least mitigated.

Furthermore, in the public consultation on Building a European Data Economy on the topic of emerging challenges of the Internet of Things and robotics liability[160], 67% of 99 producer respondents to the question claimed to factor in the risk of being held liable for damage when deciding on the price of their IoT/robotics device. However, results of the questionnaire also show that 51% of 92 producer respondents acknowledge not taking any insurance coverage to cover compensation claims in the event of harm. Thus, either producers are highly confident of their ability to satisfy liability claims or they are unable to quantify them appropriately.

From a theoretical perspective, if producers and service providers must price in unpredictable potential costs of liability (as seems to be the case), then it can be anticipated that prices for consumers today are not as low as they could be if businesses did not face uncertainties.

The logic behind this line of argument is that there could be economic advantages for businesses if they were be able to price liability risks correctly. This in turn, would lead to decreasing costs for them. Consequently, businesses that share data could also reduce prices to consumers while simultaneously maintaining their profitability.

[159] Commission Communication COM(2017) 9 final on 'Building a European Data Economy'; SWD(2017) 2 final. See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0009&from=EN

[160] See https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-building-european-data-economy for a summary of the outcomes.

So far, however, no attempt has been undertaken to substantiate and quantify this argumentation.

Divergences in national liability regimes constitute market barriers for producers and service providers

The sections above have shown that, while product liability law is harmonised through the Product Liability Directive[161], there is a wide margin of ambiguity when applying this Directive to the context of IoT and robotics. This is particularly the case for self-learning and evolutionary products and non-deterministically autonomous products. Furthermore, outside the context of product liability law, legislation in relation to extra-contractual liability and torts is not entirely harmonised; Member States may have no legislation or jurisprudence in relation to the IoT or robotics at all, or they may apply traditional doctrines relating to responsibilities for goods, hazardous items and stewardship. Whatever the outcome may be, a producer of IoT devices and robots or a service provider offering services around such devices or robots would need to identify these rules on a per country basis, and is thus facing market fragmentation and high compliance costs.

Furthermore, divergences may widen as Member States adopt specific legislation to address specific cases of robotics or IoT devices. The UK Government has announced[162] a review of its legislation to permit the use of self-driving vehicles under a mutual insurance scheme; a specific legal proposal has been drafted[163] and is under discussion. In Germany, the Justice Ministers of the German Federal States adopted a resolution in June 2017 calling for legislative action in the area of extra-contractual liability for the operation of autonomous systems[164]. Similarly, the website http://dronerules.eu – co-funded by the EU – is specifically designed to provide information visitors "about the basic requirements and applicable drone-related laws and regulations across the EU, Norway and Switzerland". The examples illustrate the risk of fragmentation: in the absence of EU level intervention, national-level legislative initiatives can create rules that differ from country to country, thus increasing costs of compliance for service providers that aim to operate across the EU.

Injured parties cannot count on availability of redress

Key messages:

- Due to the liability barrier and the limits of the current liability regime, access to compensation cannot be ensured.
- In fact, because of evidentiary complexities around claims in relation to IoT, robot-

[161] See: Directive 85/374/EEC on liability for defective products; extended by Directive 1999/34/EC to also cover agricultural and fishery products. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374

[162] See https://www.gov.uk/government/news/new-measures-set-out-autonomous-vehicle-insurance-and-electric-car-infrastructure

[163] See https://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0143/cbill_2016-20170143_en_1.htm

[164] See https://www.justiz.nrw/JM/jumiko/beschluesse/2017/Fruehjahrskonferenz_2017/I_2_Bericht_der_Laenderarbeitsgruppe_-Digitaler_Neustart.pdf

ics and autonomous systems, consumers might reasonably be unable to obtain compensation even in clear and demonstrable cases of harm.

Overall, there are some ambiguities and difficulties in applying the existing legal framework to the data economy. For citizens, this means that they may first face an unclear situation, in which it may be difficult to determine if anyone was liable for any harms they incurred and who that would be. If the legal situation is unclear, it is less likely that the situation could be solved by out-of-court dispute resolution mechanisms, which are often faster and cheaper for citizens compared to court procedures.[165] Thus, it is likely that they would need to spend **time** on this and that they would face **costs**, including for legal support.

Second, there may be **situations in which citizens are not able to receive a compensation.** Some may hesitate to initiate court proceedings with an unclear outcome, fearing the costs and stress involved. This may be especially true in cross-border situations[166].

These liability uncertainties could therefore jeopardise consumer safety in the EU, especially if the liability regime proved inadequate in courts to respond to the challenges brought in by IoT, robots, AI and autonomous systems as well as non-embedded software.

The causes of the problem

The section above established the problem in relation to the liability around the IoT, robotics and autonomous systems. This section analyses the causes of the problems for businesses and society, and contains the findings of the 'reality-check' of the initial hypotheses outlined above.

Below, we first examine briefly how current liability law applies to the IoT and robotics, both from the perspective of product liability law (which is harmonised at the EU level) and from the perspective of extra-contractual liability law and torts (which are not); and secondly how the unique characteristics of the IoT and robotics – the nondeterministic autonomy and complexity –are addressed in particular. If there are indeed gaps, these can be considered as causes of the problem.

Uncertainty around the suitability of current liability legislation

The central hypothesis of the problem tree is that current liability legislation is incapable of addressing the unique characteristics of the IoT and robotics market. Therefore, as a first step, our study examined the application of liability rules in this market. The principal challenge in relation to assessing liability in the European data economy – and the main reason why the introductory section above cannot provide clear definitions that would be universal-

[165] Cf: Commission Staff Working Paper, Impact Assessment accompanying the document 'Proposal for a Directive of the European Parliament and of the Council on Alternative Dispute Resolution for consumer disputes (Directive on consumer ADR)' and 'Proposal for a Regulation of the European Parliament and of the Council on Online Dispute Resolution for consumer disputes (Regulation on consumer ODR)', COM(2011) 793 final; Study on the use of Alternative Dispute Resolution in the European Union, Civic Consulting of the Consumer Policy Evaluation Consortium (CPEC), 2009, http://www.cc.cec/home/dgserv/sg/evaluation/pages/eims_en.htm

[166] Ibid.

ly valid across the EU – is that there is no horizontal, i.e. universally applicable, framework providing for liability rules, or even for definitions of crucial liability concepts. Liability rules have been defined in relation to consumer protection, as will be described further below, but these rules do not of course apply in a business-to-business context.

The Product Liability Directive

Product liability in the EU has since 1985 been principally governed by the Product Liability Directive167. In the sections below, we examine more closely what implementing choices Member States have made in relation to liability that affect the data economy, and specifically to what extent robotics and the IoT have been the object of legislative initiatives. Prior to conducting this assessment however, it is useful to examine the key characteristics of the Product Liability Directive.

Scoping – the concept of a 'product' (Article 2 of the Directive)

As its name suggests, the Directive addresses liability in relation to 'products', defined in the Directive as 'all movables' marketed in the EU. As such, it can be applied to any material products that incorporate digital data, such as physical carriers, but its applicability to purely digital 'products' that do not have any corporeal form is disputable. This is a critical scoping challenge when determining the impact of the Directive in the data economy: software as such, or more broadly any digital data that has not been stored on a physical carrier (e.g. software or data files downloaded from the Internet), do not unambiguously qualify or are disqualified as a 'product'.

This issue affects the IoT and robotics in two ways:

- Firstly, insofar as data is considered an intrinsic part of a product (such as a robot or IoT device), consumers might be protected by the Directive, since errors in the data could be considered a defect in the product. If the data is provided by an external source, or if a court simply holds that the data was defective, but the device or robot was not, a consumer is unlikely to be protected, especially if that external source is assessed by national law as providing a service;
- There could be a similar problem with the provision of services (including services for the use of a robot or IoT device): if a person is injured by a robot or IoT device which is used as a part of a service, then the injured person would have to demonstrate that the injury was as a result of a defect in the product (i.e. in the robot or the device itself) in order for product liability law to apply. The service provider might instead argue that the injury was a result of a problem with the service as a whole, including e.g. from errors in the software driving the service, and therefore that product liability law does not apply. In that case, damages might be addressed under (potentially much more favourable) terms of service;

[167] Directive 85/374/EEC on liability for defective products; extended by Directive 1999/34/EC to also cover agricultural and fishery products. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31985L0374

The fact that the data economy is moving increasingly to a cloudified subscription based model rather than an online purchasing model implies that discrimination might arise, where economically identical behaviour receives different and unequal treatment without a rational justification. To address this, at a minimum a single understanding is needed on the scoping of the 'product' concept in the data economy. As noted above, the national implementation and interpretation of these rules is examined in the sections below.

Objective – the concept of 'defectiveness' (Articles 1 and 6 of the Directive)

The Product Liability Directive's central legal effect is to ensure that the producer of a product 'shall be liable for damage caused by a defect in his product' (article 1). The concept of 'defectiveness' is scoped in article 6: a product is defective 'when it does not provide the safety which a person is entitled to expect, taking all circumstances into account'; referencing examples of these circumstances, the Directive mentions among other points the presentation of the product, the use to which it could reasonably be expected that the product would be put, and the moment when the product was put into circulation.

It is worth emphasising the very narrow focus of liability: the Directive aims only to attribute liability when the safety of a product is not adequately assured. This triggers a number of concerns that also affect the IoT and robotics.

Table 12: Concerns related to the focus of the Product Liability Directive

Area of concern	Explanation
Focus on product safety	Firstly, the Directive only focuses on safety. It does not consider the functionality or fitness for a given purpose of a product[168], unless the lack of functionality or fitness for purpose would create safety concerns. This is a policy choice: the Product Liability Directive aims only to ensure safety.
Assessment of product safety	Secondly and more importantly, the Directive is agnostic on how the safety of a product must be assessed. This can create challenges both for consumers and producers: for innovative product categories – such as notably IoT devices and robotics – it may be difficult to determine which assurances a consumer is entitled to expect, and which tests a producer should be required to apply before bringing a product to the market.
'Expected' safety 'Expected' safety	Thirdly, there is a more fundamental question, which is that the Directive uses the criterion of the safety 'which a person is entitled to expect'. Particularly in the context of the IoT and robotics, it is unclear precisely what legitimate safety expectations might entail. Software (and the devices and robots that are driven by the software) can be evolutionary and self-learning, meaning that it may be impossible for producers or users to predict precisely how a product will behave. Are such products inherently unsafe and in violation of the Directive? Or even more far-reaching: do such products inherently exclude any liability for the producer, since article 7(b) excludes liability if 'it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards'? A literal reading of this provision would allow safety issues created by learned behaviour to fall outside the scope of the Directive, since the resulting defect manifestly was not present when the product was put into circulation, unless learning behaviour that does not contain safeguards against potentially harmful behaviour is qualified inherently as a defect. Furthermore, the Directive also excludes damages where the producer can prove that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered (Article 7 (e)). This is particularly relevant as an exemption for rapidly developing technologies such as the Iot, robotics and autonomous devices, where it might be easier to argue that it was impossible for certain defects to be known to the producer.
Updates and functionality revi-	A more basic manifestation of the same concern is the question of updates and functionality revisions: software (again including IoT devices and robots running the software) can be patched, updated or revised, by the producer or by third parties, in a way that can affect the

[168] "Whereas, to protect the physical well-being and property of the consumer, the defectiveness of the product should be determined by reference not to its fitness for use but to the lack of the safety which the public at large is entitled to expect; whereas the safety is assessed by excluding any misuse of the product not reasonable under the circumstances."

Area of concern	Explanation
sions	safety of the product. Ideally, updates close safety holes through patches, but new code can also create new bugs and safety risks, or may simply add or remove functionality in a way that changes the risk profile of a product. Is a product defective simply because it has no update capabilities? This is unclear: while the Directive does clearly state that a 'product shall not be considered defective for the sole reason that a better product is subsequently put into circulation', it could reasonably be argued that at least some software-driven products must have the capability of having software security problems fixed. Inversely, to what extent can a producer disclaim liability when a user refuses to apply an update that has been made available? Arguably, the refusal to apply available security updates constitutes elevated risk behaviour that should shift some of the liability back to the user, but again the Directive does not explicitly consider this issue. It does, however, contain in article 7.2 the rule that liability of the producer 'may be reduced or disallowed when, having regard to all the circumstances, the damage is caused both by a defect in the product and by the fault of the injured person or any person for whom the injured person is responsible'; this rule however focuses on the situation where a contributory fault lies with the injured person (or person for whom that injured person is responsible), not with the user of the product.
Circumstances that must be taken into account to assess the safety of a product	Finally, the Directive is open in describing the circumstances that must be taken into account to assess the safety of a product (as noted above: including the presentation, the use to which it could reasonably be expected that the product would be put, and the time when the product was put into circulation), but particularly in an IoT and robotics context, the products may be created with a relatively open-ended use case in mind. An IoT device, such as a camera or sensor, is relatively open-ended in terms of functionality, but safety concerns can arise depending on their use (e.g. linking the camera or sensor to a drone or self-driving vehicle). It is not clear to what extent outlier use cases must be considered, and what the implication is for manufacturers. The recitals to the Directive note that 'safety is assessed by excluding any misuse of the product not reasonable under the circumstances', but this still leaves a relatively wide margin of appreciation in practice.

Source: Deloitte

Target of liability – the 'producer' and the role of product chains (Articles 3 and 5)

The Product Liability Directive fundamentally attaches the liability for defective products to the 'producer', defined in article 3 as the 'manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer.' For the IoT and robotics market it is important to note that a manufacturer can, therefore, create both finished products (e.g. consumer products and functioning robots) and component parts thereof (e.g. sensors or actuators used by the products).

Furthermore, article 3.2 adds that 'any person who imports into the Community a product for sale, hire, leasing or any form of distribution in the course of his business' shall be deemed to be a producer; this is crucial in an internationalised market. In the aforementioned Mirai botnet case, the producer of the cameras was a Chinese legal entity; however, any importer of the cameras would also be considered as a producer with the same liability. This is important for ensuring the effectiveness of the legal regime, given that consumers will not typically be able to avail themselves of legal remedies against non-European manufacturers.

Matching this coverage against the identification of stakeholders from the sections above, the producers and importers are directly covered. Furthermore, the Directive adds that, where the producer of the product cannot be identified, "each supplier of the product shall be treated as its producer unless he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product" (article 3.3). In this way, vendors are also directly covered. The main class of stakeholder not covered by product liability legislation are the service providers that offer a service built around a robot or IoT device. This is a policy choice rather than an oversight; the Directive aims to address product liability; not service liability. However, as noted above, this may reduce the effectiveness of the Directive in the long term: much as entertainment migrated from a product market (buying CDs and DVDs) to a service market (subscribing to streaming services), the robotics and IoT market may see a similar trend.

Damage and evidence (Articles 4, 9 and 10)

The Directive introduces the concept of strict (faultless) liability on the part of the producer of the product, requiring however that the injured party proves the damage, the defect, and the causal relationship between the two (article 4). The injured party does not, therefore, have to prove any negligence or fault on the part of the producer. As noted above, joint and several liability of all operators in the production chain is established, with exemptions if a producer proves the existence of certain facts explicitly set out in the Directive.

The evidentiary problem was already highlighted briefly above, but it is worth reiterating the point. For traditional products without a strong software/data component – i.e. simple household items or mechanical devices that are devoid of external data inputs or built-in logical systems – the causal link between a defect and the resulting damage can be relatively obvious and simple to prove. This is however not the case for software/data-driven products such as IoT devices and robots, where it will be impossible for the average person to assess

the interactions between the software and hardware components. The link between a certain unexpected behaviour and the resulting damage may be easy to prove, but it will be significantly more complex to prove that the unexpected behaviour is the result of a 'defect' as defined in the Directive.

Equally importantly, the Directive governs liability from producers towards injured persons. The injured person may be the user or owner of the product, but this is not necessarily the case; indeed, it is far from certain that the injured person knows who the user or owner is. It is arguably a strength of the Directive that it is not a requirement for liability to attach itself: it is enough that the injured person be able to identify the producer (which may admittedly be challenging enough), and that he or she can satisfy the evidentiary burden. However, especially in an IoT/robotics context, the injured person may not be capable of identifying the producer *or* user. One might consider the particular cases of self-driving vehicles or drones causing physical or property damage and then removing themselves from the scene: in such cases the injured person may not even be capable of identifying the product, let alone the producer of the product. Thus, the evidentiary difficulties are not limited to the technical issues of proving whether the product was defective; they may relate to more trivial issues such as linking a product to a producer.

Furthermore, the Directive explicitly defines 'damage' falling within its scope as '(a) damage caused by death or by personal injuries; (b) damage to, or destruction of, any item of property other than the defective product itself, with a lower threshold of 500 EUR'. Thus, only material damage is covered. This excludes a significant component of the data market, especially if digital data is not considered 'an item of property': if a malfunctioning piece of software (including software embedded in an IoT device or robot) corrupts or destroys certain data but causes no other material harm, it is unclear whether the Directive would apply. This is an ambiguity that should be resolved, preferably in tandem with the question of whether software and data as such qualify as a 'product'.

Finally, the Directive contains a liability limitation that may be particularly relevant for the IoT/robotics market: liability for material property damage or destruction only falls under the Directive 'provided that the item of property: (i) is of a type ordinarily intended for private use or consumption, and (ii) was used by the injured person mainly for his own private use or consumption'. This is logically defensible for static and immutable product types that can be expected to function in the same location and in the same manner throughout their lifetime, but it is significantly less obvious for self-actuating products that may move through a broader part of the world without much external control. Since the property damage they can cause does not seem to be limited to items for private use or consumption, there seems to be no prima facie reason to limit property-related liabilities to items for private use or consumption.

Conclusion – principal observations in relation to the Product Liability Directive

The Product Liability Directive is the main instrument available at present for guidance on how to allocate extra-contractual liability at European level. However, it poses a number of

open questions in the European data economy that have been described more extensively above, and which can be summarised as follows:

- **Scoping:** while IoT devices and robots would be likely to qualify as 'products' under the Directive, this is less obvious for software and data that have not been stored on a material carrier. A clarification on this point is advisable to ensure that digital content (including in the context of providing a service) is considered a product.
- **Defect:** it is unclear how evolutionary and self-learning products are to be assessed under the Directive, and more generally what frameworks (including standards and assessment procedures) can be used by producers to assess product safety. In addition, the Directive does not consider the behaviour of the owners or users of the devices, including the question of whether they apply available updates. The Directive's concept of 'product' would need revision.
- **Liability target, evidence and procedures:** the Directive focuses on the role of the injured person and of the producers, and requires the injured person to prove the defect, damage and causality. This however assumes that the injured person can easily identify the product and its producer. This is not obvious, nor is it likely that an injured person would be reasonably capable of proving any defect without expert assistance for the reasons outlined above.
- **Damage covered:** the Directive applies to damage caused by death or by personal injuries, and to damage to, or destruction of, any item of property other than the defective product itself, excluding however any property that is not ordinarily intended for, or actually used for, private use or consumption. There is a need to clarify whether digital content qualifies as an 'item of property' within the meaning of the Directive. Furthermore, the restriction to private items may be unreasonable in the context of self-actuating products that do not operate in a closed private sphere.

State of play in the Member States: product liability law and the complementary role of extra-contractual liability and torts

This study has assessed whether the Member States have intervened legislatively at the national level in relation to the IoT or robotics, and/or whether relevant doctrine or case law impacts the issue of liability. An overview of national responses is in Annex 1 – *Overview of national legal state of play*. Summarising the main trends briefly, it is clear that no specific legislation has been implemented yet in relation to autonomous devices, the IoT or robotics nor in relation to the liability for such devices.

Secondly, the legal correspondents indicated the applicability of the extra-contractual liability rules that apply to the custodian, steward, controller or owner (the terminology varies) of a specific device. Thus, **the assumption is always that a device can be attributed to one or more persons under whose control it operates** (or should be operating), and to which strict liability applies. In several countries heightened liability obligations apply in relation to products that are hazardous or that would be considered as "sources of increased risk" for bystanders, and that these would be likely apply to e.g. users of autonomous vehicles.

The overview also shows that the evidentiary burden can be challenging for victims, who may need to rely on experts to assess defects; this is a procedure which is not harmonised at the EU level. In some Member States, evidentiary rules or practices exist that soften this burden. French law holds that a person claiming compensation for damage caused by a thing will have to prove that the person responsible for compensating for the damage sustained should be identified as the custodian ('le gardien') of the thing. The custodian is the one who had custody ('la garde') of the thing, meaning that (s)he had the use, management and control of the thing. To facilitate evidence, the owner of the thing is presumed to be the custodian, but evidence to the contrary is admissible. This evidentiary rule facilitates the process for the victim, who can rely on the assumption that the owner will be held culpable if the owner cannot show that another person should be held to be the custodian.

Italian doctrine supports this perspective on the basis of article 2049 of the Civil Code (about liability of principals and clients – "padroni e commitment") and on article 2051 of the Civil Code (about liability of the custodian for the things under his/her care).

Latvian doctrine similarly holds that laws on losses caused by something being thrown or poured into the street or another place where people walk or stay, or by inadequately fastened objects falling from a house onto the street can be applied.

Several Member States also have specific laws on dangerous activities or hazardous behaviour that doctrine holds likely to apply to robotics and autonomous devices, although no case law has yet been presented to substantiate this theory.

In Italy article 2050 of the Civil Code states that the person who performs dangerous activities must compensate for the damage arising from those activities. The Lithuanian Civil Code holds that "a person whose activities are connected with potential hazards for surrounding persons (operation of motor vehicles, machinery, electric or atomic energy, use of explosive or poisonous materials, activities in the sphere of construction, etc.) shall be liable to compensation for damage caused by the operation of potentially hazardous objects which constitute a special danger for surrounding persons, unless he proves that the damage was caused by superior force or it occurred due to the aggrieved person's intentional or grossly negligent actions.[169]"

Similarly, the Estonian Law of Obligations states that if damage results from a dangerous characteristic of a thing constituting a major source of danger or from an extremely dangerous activity, the person who manages the source of danger is liable for having caused the damage regardless of the person's culpability. A thing or an activity is deemed to be a major source of danger if, due to its nature or to the substances or means used in connection with the thing or activity, major or frequent damage may arise from it even if it is handled or performed with due diligence by a specialist.

Liability in such 'hazard-based systems' then initially falls on the controller of a potentially hazardous object, with exceptions if the controller can prove that they lost control due to

[169] Unofficial translation

the unlawful action of other persons. In such an event, liability is instead allocated to the person or persons who engaged in the unlawful activity, or can give rise to joint and several liability in the event of shared fault between the controller and the third party. There is, however, no specific case law on hazard-based rulings applying to the issue of robotics, but the experts consulted agreed that this offers a potential solution.

Generally, and in conclusion, **liability rules currently applied to the IoT and robotics have the following characteristics and shortcomings**:

- Extra-contractual liability rules **depend on attribution of damage to a controller or custodian**. This is **effective provided that liabilities remain of a magnitude that the controller or custodian can manage and that identification is possible**. If robots obtain a degree of autonomy that could structurally create greater damage than the controller or custodian could assume, victims might not be able to obtain appropriate compensation. In those cases, an alternative approach might be needed.
- Extra-contractual liability rules **do not provide for a defence against liability claims on the basis of the lack of foreseeability and or preventability of harmful behaviour.** Significant autonomy (through machine learning or automated updates) could result in liability on the part of the controller or guardian, even though the behaviour causing the damage might not have been reasonably foreseeable for the controller or custodian.
- There is **very little harmonisation of evidentiary rules in relation to damage caused by robots.** Some Member States have useful rules in place, such as the refutable presumption of liability of the owner of the robot, or the application of hazard-based systems to robotics (creating again a presumption of liability for the users of hazardous devices). However, these are far from universal rules, resulting in an uneven and unpredictable landscape. Furthermore, these rules assume that an owner can be readily identified – an issue that could admittedly be remedied to some extent by the recommendation of the Report of the EU Parliament's Committee on Legal Affairs to create a robot register – and that the attribution of initial liability to an owner is fair and effective. As the foreseeability issue mentioned above noted, this is not certain.
- As the previous bullet points show, there is a misalignment between general extra-contractual liability rules and product liability rules. There is absolutely non harmonisation of the former across the Member States, whereas the latter are more homogeneous. This can create a case where an injured party who has no recourse to compensation on the basis of product liability law might be able to obtain compensation instead on the basis of general extra-contractual liability laws (either from the producer or the owner/controller of the device), depending on which Member State is competent to hear the claim.

Thus, there is some indication of current liability laws being unable to address liability challenges in relation to the IoT and robotics coherently.

Emerging challenges – autonomy and complexity

The sections above have examined the application and applicability of liability legislation to the IoT, robotics and autonomous systems. Two issues deserve specific scrutiny as a potential cause of problems: the autonomy of IoT, robotics, and autonomous systems, and the impact of their complexity on the effectiveness of liability law.

Autonomy

The emerging issue of robotics, in particular, has triggered significant debate on the appropriateness and capability of the present legal framework for dealing with the autonomy of robots and IoT devices. The Report of the EU Parliament's Committee on Legal Affairs with recommendations to the Commission on Civil Law Rules on Robotics[170] indicates notably in relation to liability that "the development of autonomous and cognitive features – e.g. the ability to learn from experience and take independent decisions – has made them more and more similar to agents that interact with their environment and are able to alter it significantly."

It is indeed the perceived autonomy of robots and IoT devices that causes some degree of concern: whereas robots have been in continued use for decades to assist humans in tightly defined tasks (such as routine manufacturing processes and household tasks), a concern exists that more complex robots and devices would be able to use their capabilities to take actions beyond clearly predefined and well-understood parameters, thus creating risks – and therefore liabilities – that may be hard to foresee.

This element was labelled in the preceding sections as nondeterministic autonomy, where the actions of a device are determined algorithmically, while neither the inputs nor the outcomes are exhaustively defined. Self-learning or self-modifying devices are significantly more likely to be nondeterministic: faced with exactly the same sets of inputs, a robot may after a certain amount of time begin to behave differently in response to the inputs due to learned or modified behavioural rules.

As the European Parliament Report mentioned above notes, "the more autonomous robots are, the less they can be considered simple tools in the hands of other actors (such as the manufacturer, the owner, the user etc.); whereas this, in turn, makes the ordinary rules on liability insufficient and calls for new rules which focus on how a machine can be held – partly or entirely – responsible for its acts or omissions; whereas, as a consequence, it becomes more and more urgent to address the fundamental question of whether robots should possess a legal status."

Scoping the concern is complex, since there is no universal definition of a robot. The closest approximation is probably that to be found in the relevant ISO definition[171], which defines a robot as an "actuated mechanism programmable in two or more axes with a degree of autonomy, moving within its environment, to perform intended tasks." The definition emphasises the robot's ability to move and act upon its environment with a certain autonomy, in turn defined as the "ability to perform intended tasks based on current state and sensing,

[170] See Report of 27 January 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)); see http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0005&language=EN

[171] ISO 8373:2012 - Robots and robotic devices — Vocabulary; see https://www.iso.org/obp/ui/#iso:std:iso:8373:ed-2:v1:en

without human intervention." The aforementioned Report also recognises this, calling for a definition that considers the following characteristics:

- the acquisition of autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and the trading and analysing of those data
- self-learning from experience and by interaction (optional criterion)
- at least a minor physical support
- the adaptation of its behaviour and actions to the environment;
- absence of life in the biological sense;

This focus makes it clear that the autonomy and self-modifying elements – in other words, the nondeterministic nature of robotics, and other devices – are the main triggers for concern. The overview above showed that Member State legislation does not yet take this concern into account. There are no specific rules in relation to robotics that consider the autonomy of devices, and indeed liability rules and their application in practice build on the assumption that any damage caused by a robot must, like any damage caused by any other device, machine or object, be attributable to a person (human or legal entity).

This is undoubtedly driven also by the consideration that the liability of a robot or device would only be a meaningful concept if robots were first to be given a personhood that allows them to accumulate wealth. In the absence of wealth, direct liability of robots (as opposed to the liability of their manufacturer, owner, operator, steward or other person behind the robot) excludes the possibility of recourse for the victim, as the robot or device has no assets that can be used for compensation. Thus, attributing liability to robots is only feasible with a more fundamental legal overhaul that allows one category of object (robots) to own other categories of objects (money or other assets). This is a step that current law has not taken.

The application of current law to robotics could cause significant problems, because, *inter alia,* it disregards the element of autonomy, which is the main reason of policy concern for robotics. The overview of national laws above indicated the current approach, and thus also some of the main shortcomings and pitfalls. The general approach found in the Member States is that liability for damage caused by an object (including a robot) would be attributed to the persons who have the object under their care, guardianship or in their custody (reported e.g. in Belgium, the Czech Republic, Estonia, Luxembourg among others). Paragraph 2937 of the Civil Code indicates that "if the thing causes the damage by itself, the person who should have supervised the thing, or its owner, may be held liable;[172]" thus, the attribution of liability for an autonomous thing such as a robot would be linked to the person who had a duty of care or supervision of the object. This leads to the question of what level of supervision is required when autonomous devices are used. One of the benefits of autonomous devices is that they do not require constant supervision.

The latter clarification that liability can result not only from care but also from negligence in respect of the duty of care is both illustrative of the current approach, but also of a potential

[172] Unofficial translation

weakness in the current legal framework: liability issues can be solved based on the consideration that there is always a person who supervised or should have supervised a robot. This approach is legally consistent and comprehensive, but also implies that the possibility of full nondeterministic autonomy is not recognised in the legal systems that were reviewed.

Complexity

A second emerging issue is the complexity of the IoT and robotics, which calls into question the effectiveness of liability law concepts which are based on defects. Liability legislation is predicated on the proof of a defect or fault linked causally with specific damage. This becomes more impractical when the complexity of a case increases, since meeting the evidentiary burden requires greater access to highly specialised expertise that is unlikely to be available.

For complex products such as IoT and robotics, the final product (the 'thing' or the robot) can include many components, some physical and some logical. Any one of these may be causing a particular defect. As a result, becoming involved in a discussion of which manufacturer or importer bears liability is a daunting prospect. The Product Liability Directive admittedly adds that the liability of a producer shall not be reduced when the damage is caused both by a defect in product and by the act or omission of a third party, but this provision does not solve the more basic question of identifying the producers and seeking compensation from them.

This evidentiary problem is not an inevitable part of liability law, or at least it can be substantially mitigated in practice. Strict liability regimes exist in which a designated person or entity is presumed liable for certain types of damage, even in the absence of any proven defect or fault. Motor vehicles are a common example, where the owner of the vehicle is held liable for accidents involving the vehicle; in combination with mandatory vehicle insurance, this approach ensures access to compensation for victims and separates injured parties from the evidentiary discussions.

Following to some extent in that track, Assistant Professor Andrea Bertolini[173] has argued for a more fundamental shift in product liability law, moving from the current fault-centred perspective (that emphasises the link between a defect or fault, damage and the burdensome barrier of evidence between the two) to a risk management based approach that places the liability burden on the party better positioned to minimise costs and litigation, provide compensation and ensure product safety.

This perspective is to some extent also supported by a RAND report on Autonomous Vehicle Technology[174], which noted that autonomous vehicle (AV) technologies "may undermine the

[173] See: https://www.santannapisa.it/it/personale/andrea-bertolini

[174] Anderson, Kalra, Stanly, Sorensen, Samaras and Oluwatola, RAND Report on Autonomous Vehicle Technology - a Guide for Policy Makers, 2016; see http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-2/RAND_RR443-2.pdf, notably p. 115-116

degree to which a driver must necessarily be at fault for a crash. Currently, the driver is generally considered exclusively responsible for control of the vehicle. Hence, we commonly speak of crashes as being caused by one or more at-fault drivers. In the vast majority of crashes, we ascribe blame to one or more drivers rather than to design features of the car. AV technologies will likely dilute the sense that drivers are directly and solely responsible for their automobiles. [...] This shift in responsibility from the driver to the manufacturer may make no-fault automobile-insurance regimes more attractive. While the victims in these circumstances could presumably sue the vehicle manufacturer, product-liability lawsuits are more expensive to bring and typically take more time to resolve than run-of-the-mill automobile-crash litigation. No-fault systems are designed to provide compensation to victims relatively quickly, and they do not depend upon the identification of an "at-fault" party." It should be noted of course that this transition as described in the RAND report is likely to be a gradual process, since the responsibility of car owners is currently commonly designed as a strict liability of the car owner.

Responses provided in the context of the public consultation on Building a European Data Economy on the topic of emerging challenges of the Internet of Things and robotics liability[175] are instructive on evidentiary complexities. Only a very limited number of respondents – around 5% of the 97 producer respondents to the question have so far been held liable for damage in the context of IoT and autonomous systems (e.g. robotics). Even conceding that the number of responses is not sufficient to draw conclusions on the impact of the market as a whole, this number appears remarkably low: either such devices are implausibly unlikely to cause damage, or more injured parties are not inclined to seek compensation for damage that they have suffered.

Among the 18 respondents who acknowledged having suffered harm from IoT or robotics, the main reason for them not launching compensation procedures was the procedural cost being too high in relation to the damage suffered. This is not sufficient in and of itself to conclude that the procedural costs relate significantly to evidentiary burdens, but a separate question on this topic grants some credence to this hypothesis: 60% of the 138 respondents to the question (consumers/users) believe that an IoT/robotics device should be equipped with an event data recorder to track what the device was doing when the damage occurred. This would not be a useful suggestion if evidence was presently sufficiently readily available. Thus, there is some empirical support for the assessment that the complexity of the IoT and robotics raises evidentiary challenges that call into question the effectiveness of liability law in this market.

The effects of the problem

This section discusses the effects of the problems for businesses and consumers raised above. More specifically, the following effects have been identified:

[175] See https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-building-european-data-economy for a summary of the outcomes.

- Effects on the Digital Single Market: Innovation and competitiveness are hampered within the Digital Single Market; and
- Effects on Society: There is has less freedom of choice for products and services, and digital inclusion cannot fully be ensured.

These two effects are further described below.

Effects on the Digital Single Market (innovation and competitiveness)

Key messages:

- The barriers and problems identified have a direct effect on the innovation potential and performance of the Digital Single Market (DSM).
- By affecting the most innovative businesses in Europe, in particular, these barriers are slowing the innovation path of the DSM, thus limiting European competitiveness in data markets.

Successful IoT and robotics market players excel in the creation of new, innovative start-ups and in the increased competitiveness of EU businesses in the global markets, thus triggering economic growth and the creation of new high-skilled jobs. As underlined by many business reports, "removing barriers faced by digitally intensive firms can increase GDP, wages, sales and employment at the same time."[176] In the current situation, the impediments to a clear and common understanding of the liability surrounding the IoT and robotics are expected directly to affect development of the Digital Single Market, i.e. negatively affect innovation and competitiveness.

The section above on the emerging nature of data-driven markets contains some quantitative information on the potential development of the global IoT market values today and in 2020 for different industry sectors, as well as the projected global annual economic impact of IoT appliances in nine different sectors in 2025. The IoT market of 2020 is valued at USD 8,900 billion in 2020, whereas the global annual economic impact of IoT appliances (i.e. everything related to the development of IoT appliances) is estimated to be as high as USD 11.1 trillion per year in 2025.

The realisation of these market values could be regarded as an opportunity cost today and in the future should they not be realised. Ultimately, this means that the entire economy would miss out on the related revenues.

Consequentially, any barriers to the further development and adoption of IoT and robotics potentially hinder innovation and the competitiveness of the European market. This includes the liability uncertainties identified in the previous sections, as they impede the development and adoption of the IoT and robotics, particularly from a cross-border perspective.

As previously mentioned however, as impacts are long-term effects by definition, the current costs imposed on businesses and slowing the development of the Digital Single Market

[176] *Putting data to work. Maximising the value of information in an Interconnected world*, Business Roundtable, http://businessroundtable.org/sites/default/files/reports/BRT%20PuttingDataToWork.pdf

cannot be regarded as 'value that is taken away from the market now' but rather as 'value that the market cannot realise at the moment'. More analytically, this means that the costs for businesses and consumers equal business opportunities foregone (i.e. opportunity costs)[177] and impede increasing growth rates of the Digital Single Market. This means that, as businesses and consumers face undue costs, the Digital Single Market is not evolving as fast as it could if the technical, legal, and other barriers discussed above would not impede higher growth rates.

Effects on society as a whole

The societal effects are expected to be similar to those outlined previously in relation to the access and (re-)use of data.

Baseline scenario: the likely development of the problems

The data economy is expected to have vast impacts on EU society. Potential positive impacts range from better information of citizens to increased freedom of choice for consumers, as well as *better* democracy through the use of eGovernment solutions.

However, the data economy can also be considered to have negative impacts on society, especially as long as businesses, consumers and public authorities alike face technical and legal uncertainty or grey areas that may e.g. conflict with Fundamental Rights, such as the right to privacy and the security of data processing activities.

Without policy action, the barriers and problems are likely to remain in place and be addressed bilaterally or multilaterally by businesses in the next few years. As pointed out above, this implies slower development of innovative businesses while also having effects on society as a whole (e.g. freedom of choice, consumer protection). We describe below what the situation could look like, from the business and consumer perspective, if no policy options were adopted to address the barriers identified here.

Businesses' perspective: the likely future development of the problems

Key messages:

- If policymakers do not intervene in relation to the barriers and problems identified above, the data market will continue to evolve according to the theoretical market development model.
- Technical barriers will slowly be addressed at the industry and sectoral level but at different speeds in the different sectors.
- Contracts will continue being the main vehicle for data sharing and access, and contractual barriers will be addressed on a case-by-case basis, thus leading to dispersed approaches to the same legal concepts and to the persistence of unequal bargaining power between the parties.
- Businesses will continue to have a case-by-case approach to liability through their

[177] Cf. OECD (2016), *Maximising the Economic and Social Value of Data – Understanding the Benefits and Challenges of Enhanced Data Access*, p. 4.

contractual arrangements within the boundaries of the 1985 Product Liability Directive (PLD) and this legal basis might prove inadequate in the event further development of IoT, robots and autonomous system technologies.

In summary, the European Data market overall is still emerging and translated into the theoretical model discussed in Chapter 3 on the state of play of the market, this means that European businesses are mostly in the 'emergence phase' of the market. However, the level of maturity differs by type of business and sector. Some business and sectors in fact can already be found in the 'breakthrough phase', in which some of the emerging barriers have already been addressed or are in the process of being tackled. This is the case of sectors in which, for instance, interoperability standards are being developed at the industry level (e.g. energy sector, telecommunications, automotive) and in which legal measures have been adopted regulating the use of data in certain situations (e.g. the financial sector). This means of course that the rate at which the technical, legal and other barriers identified in Chapter 3 are removed will vary.

Without EU intervention, **technical barriers**, i.e. interoperability and portability standards and practices, will continue to be slowly developed by industry on a case-by-case basis. While some sectors are already at a stage in which the different stakeholders in the value chain are sitting together to develop such standards (e.g. automotive, energy) this is not yet happening for most of the others (e.g. aviation). This means that, in the next few years, there will be a multi-speed situation, leading to differences between industries. Moreover, if the standards are developed at the industry and sectoral level with no EU intervention, there will be a lack of cross-industry standard development. This is particularly challenging, as new applications and new products and services are more and more often based on the merging of datasets coming from different domains. This will therefore increase the interoperability challenge in the future and, if no action is taken, technical barriers will slow the innovative process. Moreover, technical barriers are normally very expensive to address at the individual firm level, especially for SMEs. Therefore, in this baseline scenario, those sectors in the 'emergence phase' of the market will remain in this phase longer than needed.

In terms of the evolution of the **legal barriers**, there is a distinction to be made between different types of contractual and non-contractual issues. On the one hand, given the current strong reliance on contractual tools for sharing and accessing data, it is very likely that with no EU intervention contractual relationships will remain the key vehicle for organising and structuring commitments within the data economy. This means that data ownership, access and (re-)use will be defined on a case-by-case basis and through bilateral relations. This will lead to pragmatic and de facto arrangements, as is already the case in certain sectors (e.g. the pragmatic 'data sovereignty' rule in the aviation sector). Per se, this might not slow the transition to the 'breakthrough' market phase, as is the case now, but it will pose some challenges for SMEs who are not necessarily equipped to bear the costs of such a contractual approach and they might lack the negotiation and bargaining power to get access to the data they need.

Without intervention, the power of deciding who gets access to the data and on which terms, will remain in the hands of the *de facto data owner,* which is likely to be the entity

with the most significant commercial power. This might hamper the experimentation and development of new business models. Furthermore, there is a risk that some Member States may choose to interfere legislatively in some market segments, creating fragmentation in the internal market.

Liability is also currently addressed by contractual measures. For this reason, it has not emerged as a major blocking factor in the development of exchange of data practices[178] although the uncertainty surrounding liability contributes to the legal costs for businesses, which have been identified as very high[179]. Here again, in case of no EU intervention, liability clauses in contracts will remain the main tool at the disposal of businesses when negotiating access and (re-)use to third party data. This might have consequences from a consumer perspective (as discussed below) but also from a business perspective. Indeed, businesses will continue to work out individual liability regimes through their contractual arrangements within the boundaries of the 1985 Product Liability Directive (PLD) and this legal basis might prove inadequate to deal with further development of IoT, robots and autonomous systems technologies. Furthermore, the EU acquis presently contains no consistent answer to the applicability of these rules to pure data services and to the extra-contractual liability in relation to them. As a result, these issues are governed by national law, resulting in market fragmentation.

Finally, with respect to the **other barriers**, the issues of unequal bargaining power, valuing data, finding the right skills and innovative procurement procedures, will also have an impact on the market development and take up of new data services and product. The impact of these barriers in the baseline scenario is, in general, more limited than that of the legal and technical barriers, with the only possible exception being the unequal bargaining power and the problem of skills.

The question of valuing data for instance can be considered to be intrinsic to the early stage of the development of the market and will most likely be solved through market based mechanisms. These will adjust to demand and supply once businesses are ready for the breakthrough phase. Similarly, the question of procurement could be solved in the next few years by the market without policy intervention except in the case of highly regulated markets (e.g. finance) in which it is the regulatory framework which poses a problem[180].

The skills gap and the lack of suitable profiles for data-related jobs is likely to increase, however. As recent studies show, "there may be a lack of up to 500,000 Information and Communication Technologies (ICT) professionals in 2020,[181]" and this will of course have an impact on the ability of firms to share and (re-)use data, and therefore on the innovation and competitiveness of the Digital Single Market.

[178] Reputational losses linked to possible misuse of the data shared, even when covered by contractual liability clauses, were, however, mentioned by interviewees as a possible blocking factor.
[179] See the section on Assessment of Problems
[180] See Annex 2 – Sectoral Case Studies
[181] See: https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition

Similarly, the question of the **unequal bargaining power** might also have profound effects and especially if this leads to the exclusion from the market of a number of companies (data (re-)users, competitors and same-sector downstream providers) and therefore to a limitation of competition and less freedom of choice for consumers. It was argued that this scenario might be likely in the automotive sector for instance.

To summarise, Europe's data economy will develop at different speeds depending on the sector and the stage they are at in market development. Although all industries will most likely transition to the breakthrough phase over the next few years, the challenges listed above will result in an uneven situation in which there will be some players (from SMEs and from certain sectors such as aviation or chemicals) starting from a disadvantaged position and unable to immediately reap all the benefits of the data economy, and others which, due to their position in the value chain, might be excluded from the market.

Consumers' perspective: the likely future development of the problems

Key messages:

- In the baseline scenario, consumers will continue paying higher prices than needed and will continue facing difficult access to compensation for liability.
- The safety of data-driven products and services might also be put at risk if the liability regimes proved to be inadequate in the future.

From a consumer perspective, the legal, technical and other barriers identified in Chapter 3 have two main consequences at the current stage. First, businesses are transferring to consumers the costs that they bear as a result of these barriers and consumers therefore pay undue prices. Second, due to the lack of clarity on extra-contractual liability, in particular, consumers are confronted with obstacles when trying to claim compensation for damage relating to data-based products and services.

In the baseline scenario, consumers will continue to face the costs and obstacles they face now as businesses will continue passing on their costs of data sharing and access to them, as the legal liability framework will not be clarified. Indeed, as argued in the previous section, in the baseline scenario, business will still have to invest resources in overcoming autonomously and bilaterally/multilaterally the technical, legal and other barriers. This will involve bearing costs that the consumers will also pay.

At the same time, in the specific context of liability and due to the fact that this issue is tackled at the contractual level by companies exchanging data, consumers will continue to face an unclear situation. Moreover, the limits of the PLD might result in a lower level of safety of data-driven services and products over time if the legal uncertainties around this increase. Therefore, if no policy intervention is foreseen, these problems will persist in the years ahead and this will continue to have a concrete impact on consumers and citizens.

4 Policy objectives and policy options

This chapter contains a description of the policy objectives which could be pursued in relation to the barriers, problems and effects identified above. It also presents a list of relevant policy actions.

Policy objectives

The policy objectives set out the political priorities and aims for action in the relevant field.[182] The definition of policy objectives is an essential step of each Impact Assessment as they, in accordance with the *Better Regulation Guidelines*, support:

- The creation of a logical link between the problems identified and the solutions considered;
- The clarification of the relationship between the specific goals of the initiative considered and the horizontal EU objectives and/or any other relevant agreed policy goals;
- The explanation of any trade-off between different policy objectives;
- The definition of the criteria for comparing the different policy options and the indicators to measure performance and progress towards the objectives; and
- The establishment of the criteria to be considered as part of the proposed monitoring and evaluation framework for the policy measure implemented.

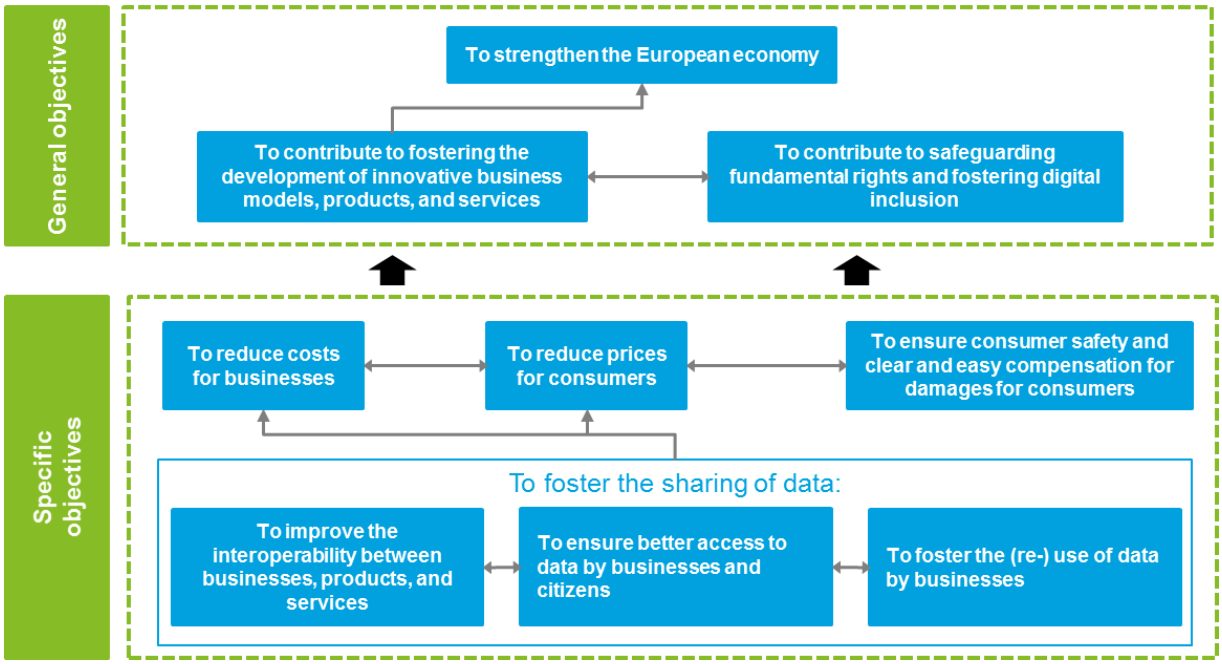
Policy objectives are normally identified at the following levels:

- *General objectives* refer to Treaty-based goals and constitute a link with the existing policy setting;
- *Specific objectives* relate to the specific domain and set out what the Commission wants to achieve with the intervention in detail; and
- *Operational objectives* deal with deliverables or objectives of actions.

[182] European Commission, Better Regulation Guidelines, 19 May 2015, SWD(2015) 111 final, pp. 21-22 (http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm); European Commission, Better Regulation "Toolbox", complementing the Better Regulation Guidelines presented in in SWD(2015) 111, pp. 80-81 (http://ec.europa.eu/smart-regulation/guidelines/docs/br_toolbox_en.pdf).

Operational objectives tend to pre-empt the solution (e.g. if a specific legislative instrument needs to be clarified). Therefore, it is not always appropriate to define the operational objectives directly after the analysis of the problems, but rather after identifying the preferred option by means of which the general and specific objectives would be achieved.

Figure 18: Objectives tree



Source: Deloitte.

Policy options

This section describes the policy options identified based on the problems as described in chapter 3 and to achieve the policy objectives presented above. We first provide an overview in a matrix and then describe each option in more detail in the following sub-sections.

Beyond the default non-interventionist option, the policy options can be divided into soft (non-regulatory) policy options, and hard (regulatory) policy options. Each of these can be further broken down further into actions, which target the barriers to the data economy generically, actions that target specific topics that affect the data economy, and actions that target specific sectors, including the IoT and robotics in particular.

The following matrix maps intervention types (left column) against the problems to be addressed (top row). It is of course conceivable that the answers to the individual problems differ, e.g. that no action would be appropriate for certain problems (thus essentially leaving resolution up to the market), while others would need to be addressed through non-regulatory measures or new legislation. Thus, it is thinkable that a combination of the different options would be proposed. Each cell in the matrix is described in more detail below the table.

Table 13: Policy option matrix

Title of Policy Option	Data access/use rights/data ownership	Portability	Liability	Interoperability and standardisation
0. No intervention				
No measures taken	No specific action	No specific action	No specific action	No specific action
1. Non-regulatory intervention				
1A: Horizontal intervention– **issuing guidance and disseminating best practices on**:	Recommended access/right to use data, including model contract clauses	Recommended portability rights, including scoping of portability and model contract clauses	Recommended liability provisions, including model contract clauses and best insurance practices Identifying appropriate standards for safety assessments and certification	Recommended data formats and/or APIs/web services
1B: Sector specific intervention – **issuing guidance and disseminating best practices on**: (Note: **implies establishment of sector specific expert/working/coordination groups**)	Recommended access/right to use data, including model contract clauses in a specific sector (e.g. targeting specifically scientific research or publicly funded initiatives)	Recommended portability rights, including scoping of portability and model contract clauses in a specific sector (e.g. targeting cloud computing)	Recommended liability provisions, including model contract clauses and best insurance practices Identifying appropriate standards for safety assessments and certification (e.g. in relation to the IoT or robotics)	Recommended data formats and/or APIs/web services in a specific sector (e.g. targeting the cloud, scientific research or publicly funded initiatives)
1A and 1B: Coordination and Cooperation	Establishing Member State specific coordination and cooperation mechanisms to address cross-border data economy challenges Increased funding for innovation and research, including in particular in relation to industrial/big data platforms			
2. Regulatory intervention				
2A: Horizontal intervention: introducing and amending (existing) **legislation on**:	Data producer rights *and/or* Rights to data access and usage	Mandatory data portability rights (comparable to GDPR, but also for non-personal data)	General revision of liability law (such as product liability legislation and/or product safety law)	Mandatory data formats and/or APIs/web services to be provided generically
2B: Sector specific intervention: introducing **legislation on:**	Data producer rights in a specific sector *and/or* Rights to data access and usage in a specific sector	Mandatory data portability rights (comparable to GDPR, but also for non-personal data) in a specific sector	Sector-specific legislation on minimum liabilities to be borne by certain service providers in certain sectors (e.g. public sector, financial services, IoT, etc.)	Mandatory data formats and/or APIs/web services to be provided in a specific sector

Source: *Deloitte*

Policy option 0: No intervention

The default option is not to take any specific action. This implies that no specific regulatory intervention is undertaken (no adoption of new legal instruments), and that no non-regulatory actions (standardisation efforts, stakeholder coordination, funding new research etc.) are undertaken either.

This does not necessarily imply that no actions are undertaken at the EU level that affect the European data market. By way of example: policy action on data protection, e-commerce, product liability reform and so forth would be likely to continue, and be likely to have an impact on the data economy. However, none of these would include measures that aim to resolve any of the emerging barriers, as described in the problem assessment.

Policy option 1: The non-regulatory option

Policy Option 1 aims to address the issues identified in the problem assessment though non-regulatory measures. These can comprise a broad package of actions, which can be applied selectively or cumulatively, and which can be applied either to a specific sector or context, or generically.

As indicated in the overview matrix above, the non-regulatory option could be applied both horizontally without singling out any particular sector, industry or context (which might be referred to as **Option 1A**), or it could be focused on specific sectors, industries or contexts (which could be described as **Option 1B**).

Policy option 1A: Non-regulatory measures across different sectors

The following actions, in particular, could be integrated into a non-regulatory policy approach:

Encouraging the identification and dissemination of best practices

This action can target both policy makers and industry. It is principally an awareness raising measure, aiming to improve knowledge and understanding of the options available in the data economy, and to provide sample implementations of specific choices (such as model contractual clauses or appropriate risk assessment standards and methodologies). In each case, it would be necessary to couple these best practices with the expected effects of certain choices, so that stakeholders can make choices that reflect their priorities.

For policy makers (including legislators at the national level), the action would target the identification and promotion of those national laws and policies which are most conducive to encouraging innovation in the data economy, and which are particularly capable of balancing the interests of all stakeholders (including individual citizens and SMEs, who might otherwise struggle to obtain benefits from the data economy).

Some of these laws and policies have already been identified during this study (e.g. existing laws on liability for high-risk products that could be applied to IoT and robotics, (draft) legislation on drones and self-driving vehicles, and guidelines for establishing trial zones for innovative technologies. The latter include regulatory sandboxing, i.e. the temporary suspension of certain legal requirements in relation to a new and innovative product or service, focusing

on a well-defined sphere of operation (e.g. limited to a certain geographical area, user group, or transaction value) under supervision and continuous evaluation, in order to support experimentation in a controlled manner. This policy option would thus entail the continued identification of new initiatives, evaluation of their effectiveness, and promotion of these solutions among Member States, without however imposing any changes on Member State or EU level laws or policies.

In the case of industry, the emphasis would be on identifying and promoting practices (including contractual practices, templates, licence models, standards, R&D strategies and data exploitation/monetisation strategies and guidelines) that are conducive to innovation and economic growth. Within the research domain, there are many examples of general initiatives promoting data sharing and disseminating knowledge on licence models and standards across sectors. For instance, the Research Data Sharing Alliance is an interdisciplinary initiative "providing a neutral space where its members can come together through focused global Working and Interest Groups to develop and adopt infrastructure that promotes data-sharing and data-driven research, and accelerate the growth of a cohesive data community that integrates contributors across domain, research, national, geographical and generational boundaries"[183]. Within the business domain, the ODPi platform "is committed to simplification & standardization of the big data ecosystem with common reference specifications and test suites"[184]. Composed of many companies and especially SMEs, the ODPi provides specifications, reference implementation and test suites to remove complexity and accelerate the take-up of Big Data[185].

Again, it would be important to recognise key principles such as consumer rights, data protection, fair market practices and competition as assessment criteria for identifying best practices.

Establishing appropriate standards, assessment schemes and benchmarks for the data economy

A recurring concern in this emerging market is the lack of appropriate criteria for assessing the ability of a product or service to satisfy legal and policy demands. This relates to issues such as interoperability and data portability (what can/should be done before data can be considered accessible?) but also to the more fundamental issues of safety (how and based on which criteria should a product or service be tested before it can be considered as sufficiently secure?). These are not purely legal questions and require consideration of technical and operational issues as well. A mapping of existing norms (standards, schemes and benchmarks) would be needed, followed by actions to fill any gaps identified, e.g. by establishing standardised criteria and methodologies for conducting risk assessments.

[183] See : https://www.rd-alliance.org/about-rda
[184] See: https://www.odpi.org/about
[185] Ibid

Establishing Member-State specific coordination and cooperation mechanisms to address cross-border challenges

One or more Member State expert groups could be established that would coordinate and cooperate on any issues where cross-border challenges may occur. Examples of some of these challenges were identified at previous stages of the project and include the creation of cross-border transportation mechanisms (including (semi-)autonomous driving), cross-border health care analytics. Currently, Member States address these topics individually, but this is not conducive to the creation of cross-border products and services.

A more basic example of a cross-border challenge is the lack of a common understanding of the concepts of data ownership and data access/use rights. Since there is no common understanding, the rights applicable (and the validity of rights claimed) may differ from Member State to Member State. However, this is an issue that may require legislative intervention and in that case would be more appropriately covered by Option 2.

The distinguishing element between this action and the first action in this list (encouraging the identification and dissemination of best practices) is that the latter focuses on any best practices that might be of interest, whereas this action focuses specifically on cross-border cooperation.

Increased funding for innovation and research

Finally, this last option would ensure that additional funding would be made available at the EU level (including by encouraging Member States to provide their own funds) for innovation and experimentation in the data market, including IoT, robotics, and M2M. This is of course not new, since this action is currently already undertaken, particularly in the context of H2020 funding. This specific action would however entail an increase in the funding available in order to provide a further stimulus to European innovation and research in the data economy.

Policy option 1B: Sector-specific non-regulatory measures

Option 1B would imply that specific sectors, industries or contexts are selected on the basis of the evidence available and their unique characteristics, and that specific expert/working/coordination groups with representatives from the relevant stakeholder groups would be set up at the EU level to identify, assess and promote suitable guidance and best practices.

The operational measures used in implementing option 1B would be similar to those identified under option 1A, but would target specific sectors. They would, therefore, still comprise:

- Encouraging the identification and dissemination of best practices;
- Establishing appropriate standards, assessment schemes and benchmarks;
- Establishing specific coordination and cooperation mechanisms with Member States to address cross-border challenges; and
- Increased funding for innovation and research.

Policy option 2: The regulatory option

Beyond the non-regulatory option, legislative action could also be considered to address some of the problems identified. As for Option 1, sub-options could be considered.

The options below are not mutually exclusive and could be applied cumulatively. However, a cumulative approach is arguably harder to apply than for the non-regulatory option, due to the risk of conflicts between legal frameworks (e.g. a horizontal legal instrument should ideally not counteract the effectiveness or credibility of sector-specific initiatives).

The regulatory option will typically target one or more distinct barriers, such as data ownership/access/use, liability, and data portability; each may require a separate legal instrument.

Policy option 2A: Legislative horizontal measures targeting the data economy as a whole

Option 2A would consist of one or more legislative horizontal measures targeting the data economy as a whole, without focusing on any specific industry, data type or subject.

This could contain both the **adoption of new legislation**, as well as **amendment of existing legislation** to the extent necessary.

In relation to the **adoption of new legislation**, a Directive or Regulation could e.g. target data ownership, access and/or usage rights (including mandatory data sharing, either generically or under fair, reasonable, and non-discriminatory terms - FRAND), data portability, liability, and/or M2M contracting.

Key implementation measures[186] could be:

- A legal instrument that would homogeneously define data ownership, access or use rights, possibly in combination with a data portability right for non-personal data. This could deal with specific types of data or be restricted to specific use contexts (e.g. for personal use and for public interest, scientific or historical research purposes or statistical purposes, or insofar as required to enable maintenance and repair of products, including by third parties); and
- A legal instrument that would address liability in the data economy, e.g. by recasting the Product Liability Directive in order to ensure a more comprehensive scope of application (i.e. by unambiguously including data and software within the scope of the definition of a product), and/or to provide an alternative liability regime for products with an elevated risk profile (which would include but not specifically target certain robots or IoT devices), based on a risk-opening approach or a risk management approach.

Amending existing legislation could focus on revising and updating existing legal instruments in order to better consider the objectives of the data economy. This action focuses

[186] In principle data location is out of scope of this study. However, a legal instrument that would remove unjustified national legal data location restrictions – or more broadly: legal requirements that affect the flows of data which are not proportional and justified by an overriding reason relating to the public interest –could be a 'supporting' measure to the ones addressing the 'emerging' issues.

more on the perspective that existing legal instruments are fundamentally appropriate, but require a re-scoping or modernisation to take account of the new challenges encountered in the data economy. Thus, this action would not envisage the creation of a single horizontal legal instrument, but rather aim to identify existing legal instruments that contain certain inadequacies, and revise those to ensure that the issues identified in the problem statement can be addressed.

Key examples would be the revision of the **Product Liability Directive and the eCommerce Directive** – both of which are already under review – to account for some of the current challenges. A reworking of the Product Liability Directive could e.g. comprise a relatively simple extension of its scope to unambiguously ensure that data and software as such (separate from any carrier) would be qualified as a product, or to ensure that IoT devices and robots would be considered as products to which the Directive applies.

Alternatively or cumulatively, the Product Liability Directive could be modified to include separate liability regimes for (semi-)autonomous or self-modifying devices (including learning robots), or more generically for products with an elevated risk profile (which would include but not specifically target certain robots or IoT devices), based on a risk-opening approach or a risk-management approach.

A risk-opening approach implies an ex-ante legislative allocation of liability to the entity that decides to create a risk by taking a product with an elevated risk profile into use. The risk-management solution also implies an ex-ante legislative allocation of liability, but to the actor best placed to minimise or avoid the realisation of the risk by strengthening product safety; this will typically be the manufacturer of the product. In both approaches, claims can be addressed through a common fund or mandatory insurance scheme.

An even greater revision could be to recast the Directive into a Product and Services Liability Directive, ensuring that data economy services would fall under rules comparable to their counterparts that rely on tangible movable goods.

Policy option 2B: Legislative measures focusing only on specific sectors

Option 2B would take a similar approach, but focusing only on specific sectors, industries or contexts (comparable to Option 1B above). These sector-specific legislative measures would build on the observation that the challenges encountered in each sector are different, due to the different business models, public interest and economic sensitivities, and that therefore a diversified approach is also needed. This approach is not entirely new: this study has highlighted initiatives aimed at improving access and usage rights to data in specific industries, such as public sector information, vehicle repair and maintenance information, and payment services. In each of these cases, targeted legal intervention has been appreciably successful in improving the functioning of the data market. Similar initiatives might be undertaken in relation to research data (where open science policies already exist) or health data (where open access is less prevalent), in each case making data sharing mandatory (conditionally or unconditionally).

Similarly, a distinction could be made between data services and tangible movable goods (IoT and robotics) by, for example, considering the creation of a specific IoT/robotics legal instrument that could extend the scope of existing frameworks (such as the Product Liability Directive) to the IoT or robotics, possibly with relevant additions (e.g. access and usage rights to data generated by the relevant products) or modifications (e.g. modification of the liability regime to a more risk-oriented approach where liability is allocated to the producer of the device, or where liability is borne through a common fund).

Alternatively or additionally, this new legal instrument could build on existing product standardisation regulations such as the Mutual Recognition Regulation (EC) No 764/2008[187]. This would allow e.g. safety requirements and assessment methodologies to be harmonised, allowing ex-ante safety assessments to be conducted that result in declarations of conformity for approved IoT/robotics devices, while reducing the scope for national derogations. The applicability of the Mutual Recognition Regulation would not fundamentally change the liability rules for such products as such, but this issue could be addressed by also extending the scope of application of the Product Liability Directive as described above.

[187] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008R0764

5 Assessment of the impacts of the options

This chapter presents the assessment of the policy options identified to address the problems related to the emerging barriers to the data economy and provides some insights into the order of preference.

Introduction

This chapter presents our draft assessment of the impacts of all the options, including the baseline scenario.

The following assessment criteria were agreed on for the assessment of the impacts of the options:

- Effectiveness in achieving the policy objectives:
  - Achievement of specific objectives;
  - Achievement of general objectives;
- Efficiency:
  - Costs of the option[188];
  - Benefits of the option, including reductions in some of the costs as well as other positive effects on (some of) the stakeholders;
- Coherence of the option.

To the extent possible, the assessment is built on **quantitative and qualitative information, including costs and benefits**. For this purpose, we took various data sources into account for the assessment of the impacts, including:

- Desk research, including a legal analysis;
- Written consultations of stakeholders:
  - EU Commission public consultation;
  - Deloitte survey;
- Stakeholder interviews, including in the context of sector-based case studies; and
- Several workshops with different groups of stakeholders, including Member States and businesses of various sectors and sizes.

[188] The types of costs that are particularly relevant in the context of this assignment include: Costs related to the legislative framework, e.g. changes to national legislation and the development of guidance for public administrations and businesses; Transaction costs, e.g. communication with stakeholders, training, monitoring and enforcement of legislation; Compliance costs, e.g. administrative burden and opportunity costs; Costs related to the legal aspects, e.g. lawyers' fees; and Costs related to the technical implementation, e.g. procurement and/or development of hard- and software.

Overall, while we aimed to collect an as comprehensive set of quantitative data as possible, **stakeholders were not able to provide us with the *ideal* set of information in relation to *all* types of costs and benefits**. Thus, while we used quantification as far as possible based on the data available, **illustrative examples** (both in quantitative and qualitative fashion) of the effects that the policy options would have are used to complement the analysis.

The assessment of the options in relation to the different assessment criteria are expressed in **scores**. Each option received scores between -5 (very strong negative impact) and +5 (very strong positive impact) on each of the five assessment criteria.

Summaries of the assessments, including the scores, are presented at the beginning of each section below.

Based on the assessment of the options, we later determine a ranking of the different options. For this purpose, we will use **Multi Criteria Analysis (MCA)**. The MCA is a largely qualitative analysis of the policy options, based on ratings and rankings with quantitative data supporting the assessment. Based on the ratings attributed to each policy option as explained above, it is then possible to calculate the ranking of the policy options, i.e. which scores best, second best etc. It is also possible to score different combinations of policy options against each other. For this purpose, it is possible to attribute different weights to the different assessment criteria. For example, it is possible to attribute a higher weight to the assessment criterion "Achievement of the specific objectives" than to the criterion "Costs of the option" or vice versa. The weight of each assessment criterion will be devised at a later stage in discussion with the European Commission.

Further details on our approach are presented in Annex 4 – Approach to the Impact Assessment.

Limitations relating to the findings of this study

As mentioned in chapter 1, the data collection was hampered by the fact that the markets considered are still in the "emergence" stage. This made it particularly challenging to quantify the evidence relating to the barriers identified. Thus, the findings of this section are based on the analysis of mainly qualitative data and should be seen as a first attempt at examining this topic and as providing only a preliminary (mainly qualitative) overview of the potential impacts of these preliminary policy options.

Policy Option 0: No intervention

Under this policy option, no changes to the current policy would be introduced.

Key findings of the assessment

The table below provides an overview of our assessment of the baseline scenario. The detailed assessment in accordance with the individual assessment criteria can be found in the subsequent sub-sections.

Table 14: Key findings of the assessment of the baseline scenario

Assessment criteria	Rating (-5 to + 5)
Effectiveness	
Achievement of specific objectives	0
Achievement of general objectives	0
Efficiency	
Costs	0
Benefits	0
Coherence	
Coherence with existing initiatives	0
Sum	**0**
Average	**0**

Source: Deloitte

Effectiveness in achieving the policy objectives

Achievement of specific objectives

Without policy action, the problems identified for **businesses** would be likely to remain in place and be addressed bilaterally or multilaterally by businesses in the next few years.

As mentioned in Chapter 3, the European Data market overall is in its *infancy* or in the 'emergence phase'. However, the level of maturity differs according to the type of business and sector. Some businesses and sectors have in fact already moved to the '*breakthrough phase'*, in which some of the emerging barriers have already been addressed or are in the process of being tackled. This is the case of sectors in which, for instance, interoperability standards are being developed at the industry level (e.g. energy sector, telecommunications, automotive) and in which legal measures have been adopted regulating the use of data in a certain situation (e.g. financial sector). This means of course that the legal, technical and other barriers identified in Chapter 3 will evolve differently in different sectors. Without policy intervention, the **development of the data economy** in Europe would proceed at a different speed depending on the different sectors and their market phase. Although **all industries would most likely transition to the 'breakthrough phase' over the next few years (possibly with delays)**, the result would be an **uneven situation** in which there would be some players (from SMEs and from certain sectors) starting from a disadvantaged position and unable to immediately reap all the benefits of the data economy. This is described in more detail in the following paragraphs.

In terms of evolution of the **legal barriers**, a distinction must be made between different types of contractual and non-contractual issues. On the one hand, given the current strong reliance on contractual tools for sharing and accessing data[189], it is very likely that with no EU intervention contractual relationships would remain the key vehicle for organising and structuring structure commitments within the data market. This would mean that data ownership, access and (re-)use would be defined on a case-by-case basis and through bilateral relations. This would raise some challenges for SMEs. They are not necessarily equipped to bear the costs of such a legalistic approach and they might lack the negotiation and bargaining power to get access to the data they need.[190] In the case of non-intervention, the power of deciding who gets access to the data and under which conditions, would remain in the hands of the *de facto data owner.,* That is likely to be the entity with the most significant commercial power. This might hamper the experimentation and development of new business models and thus slow the transition of the market into the 'breakthrough phase'.

Liability is also currently addressed through contractual measures. Here again, if there were no EU intervention, liability clauses in contracts would remain the main tool at the disposal of businesses when negotiating access to and (re-)use of third party data. This might have consequences from a consumer perspective (as discussed below) but also from a business perspective. Indeed, businesses would continue to work out individual liability regimes through their contractual arrangements within the boundaries of the 1985 Product Liability Directive (PLD) and this legal basis might prove inadequate to cope with further development of IoT, robots and autonomous systems technologies. Furthermore, the EU acquis presently contains no consistent answer to the applicability of these rules to pure data services and to the related extra-contractual liability. As a result, national law governs these issues, resulting in market fragmentation and uncertainty.

In terms of the way in which the **technical barriers** might evolve without EU intervention, interoperability and portability standards and practices would probably continue to be slowly developed by industry on a case-by-case basis. If some sectors are already at a stage in which the different stakeholders in the value chain are sitting together to develop such standards (e.g. automotive, energy), this is not yet happening for most of the others (e.g. aerospace). This means that, in the next few years, there would be a multi-speed situation leading to differences between industries. Moreover, if the standards are developed at industry and sectoral level, there would be a lack of cross-industry standard development if the EU did not intervene. This would be particularly challenging, as new applications and

[189] As demonstrated in the section on contractual and legal barriers in Chapter 3, companies rely on contracts to regulate and govern their exchanges of data.

[190] The discussions held at the High Level Conference on Building a Data Economy on 17 October 2016 and during later workshops showed that the stakeholders are split in terms of satisfaction with this widespread contractual approach to the sharing of data. However, some SMEs complained about one-sided contract clauses and the burden that legal advice represents for them. As also suggested by the web-based survey, smaller players might also be more concerned than incumbents with the unequal bargaining power with the data holder. However, there is no unanimity amongst smaller companies on this topic as, overall, most agree that the contractual freedom provided by this modus operandi is positive due to the early stage of the market. Bigger players on the other hand in general argue that the contractual framework is well suited for the current situation and the current level of development of the market.

new products and services are more and more often based on the merging of datasets coming from different domains. This would, therefore, increase the interoperability challenge in the future and, if no action were taken, the innovative process would be slower because of the technical barriers.

Finally, with respect to the **other barriers**, the issues of valuing data, finding the right skills and innovative procurement procedures, also have an impact on the market development and take-up of new data services and product. The impact of these barriers without policy intervention would, however, be more limited than in the case of the legal and technical barriers. The question of valuing data for instance tends to be intrinsic to the early stage of development of the market and would most likely be solved through market-based mechanisms, adjusting demand and supply once the businesses are ready for the 'breakthrough phase'.

Similarly, the question of procurement could be resolved in the next few years by the market without policy intervention except in the case of highly regulated markets (e.g. finance) in which it is the regulatory framework which poses a problem[191]. Finally, with respect to the question of accessing the right skills for fostering the sharing and access to data, if there were no policy intervention, the skills gap and the lack of suitable profiles for data-related jobs is likely to increase. As recent studies show, "there may be a lack of up to 500,000 Information and Communication Technologies (ICT) professionals in 2020[192]" and this will of course have an impact on the ability of firms to share and (re-)use data.

Thus, there might be small improvements relating to the sharing of data, but several barriers would remain in place (or be solved only slowly) without policy intervention. On this basis, **businesses would continue to face costs** relating to these barriers. As demonstrated in Chapter 3, legal barriers as a whole are considered as one of the most expensive elements to tackle when dealing with sharing and accessing data.[193] For example, the uncertainty surrounding liability contributes to the legal costs for businesses. The technical barriers are normally also very expensive to address at the individual firm level. This is especially true of SMEs.

On this basis, **consumers** would continue to face the costs and obstacles they face now as the businesses would continue passing on the costs they incur from these barriers. At the same time, specifically linked to liability and due to the fact that this issue is tackled at the contractual level by companies exchanging data, consumers would continue to face an unclear situation every time their specific case was not explicitly foreseen by these contracts. Therefore, if no policy intervention is foreseen, these problems would persist in the years ahead and would continue having a concrete effect on consumers and citizens.

[191] See Annex 2 – Sectoral Case Studies

[192] See: https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition

[193] Indeed, around 49% of data user respondents to our general survey identified costs of legal advice as the most important cost category for them, by far.

Achievement of general objectives

Without policy intervention, there would be limits to the extent to which the objective of fostering the development of innovative business models, products, and services would be achieved.

A non-interventionist approach essentially relies entirely on the market to drive innovation where possible, and ensures that the data economy is neither specifically favoured nor specifically limited by new initiatives. On the flipside, the problems identified – such as the legal uncertainties around data ownership, access and usage, or the allocation of liabilities in relation to (semi-)autonomous and self-adapting products and services including robotics, would be likely to go unaddressed under this policy option. This would hamper the development of the European data economy.[194] As explained earlier, the market would still develop at a moderate pace, thus some innovation would still occur. However, the fact that certain sectors and certain types of business (notably SMEs) would face disadvantages would hamper innovation by these players. This might also have negative effects on the European economy as a whole.

There would be no significant impacts on the objective of safeguarding fundamental rights and fostering digital inclusion. Consumers would continue facing uncertainty in relation to the compensation for damage, potentially impacting on the right to an effective remedy. Consumers would probably continue to face unduly high prices and this would be an impediment to digital inclusion.

Efficiency: Costs and benefits of the option

Costs of the option

As demonstrated in the section on effectiveness, **businesses** would continue to face costs in relation to the exchange of data, including e.g. based on different technical standards and unclear legislation. In addition, they could be expected to face opportunity costs, as data would be shared only to a limited extent.

Consumers would face higher prices, as businesses passed on their own costs on to consumers.

Public administrations would not face any costs.

Benefits of the option

Without policy intervention, the market could develop further without restraints. This would be beneficial according to some stakeholders consulted as part of this study, who argued that the market is still in the 'emergence phase'. However, overall, the expected benefits

[194] It was, for example, pointed out by the Max Planck Institute for Innovation and Competition that "access to data will be key for the building of the European data economy." *Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public consultation on Building the European Data Economy"*, http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf

would be limited. As explained above, some sectors and types of businesses could be expected to be disadvantaged and consumers could be expected to face higher prices.

Coherence of the option

As there would be no intervention, coherence with existing legislation can largely be confirmed. However, there is a case for arguing that the barriers identified as part of the problem assessment would hinder the achievement of the Digital Single Market Strategy.

Policy Option 1A: Non-regulatory measures across different sectors

Policy Option 1A includes horizontal non-regulatory measures, notably:

- Encouraging the identification and dissemination of best practices;
- Establishing appropriate standards, assessment schemes and benchmarks for the data economy;
- Establishing specific coordination and cooperation mechanisms with the Member States to address cross-border challenges; and
- Funding innovation and research.

Key findings of the assessment

The table below provides an overview of our assessment of the Policy Option 1A. The detailed assessment in accordance with the individual assessment criteria can be found in the subsequent sub-sections.

Table 15: Key findings of the assessment of Policy Option 1A

Assessment criteria	Rating (-5 to + 5)
Effectiveness	
Achievement of specific objectives	2
Achievement of general objectives	1
Efficiency	
Costs	-1
Benefits	3
Coherence	
Coherence with existing initiatives	2
Sum	**7**
Average	**1.4**

Source: Deloitte

Effectiveness in achieving the policy objectives

Achievement of specific objectives

Overall, this option would have a positive impact on the achievement of the specific objectives.

It can be expected that **data sharing would be supported** and could increase to a moderate extent. This is because it could be expected that the barriers businesses currently face would be lower, as described in the following paragraphs.

Horizontal soft measures would help to reduce the **legal barriers** identified as part of this study. Uncertainty in relation to existing legislation could potentially be reduced by means of the awareness-raising measures targeting policy makers[195] as well as cross-border cooperation mechanisms. The promotion of contractual practices or templates could help businesses in ensuring access to and (re-)use of data.

As demonstrated in the section on contractual and legal barriers in Chapter 3, companies rely on contracts to regulate and govern their exchanges of data. To give an example, (re-)use of third party data is normally defined by contracts and restricted as far as possible.[196] Awareness-raising, the exchange of good practices and potentially the development of model contracts, might encourage businesses to be more open about the (re-)use of their data.

Difficulties relating to liability would also be improved by horizontal soft measures. As the data suggest, companies tend to decide on a case-by-case basis and through contractual means which liability assurance they need and wish for. This can also be a result of the legal uncertainty of the overall liability regime. As mentioned in Chapter 3, liability seems to be a transversal concern touching upon businesses situated at different stages of the value chain and in different sectors.[197] Thus, horizontal measures would be adequate to address these concerns. In particular, awareness-raising, the exchange of good practices and potentially the development of model contracts could help to reduce uncertainty and the need for legal advice.

The **establishment of standards** would help address technical barriers that are not sector-specific but rather horizontal. For example, horizontal measures relating to interoperability could be particularly useful, as data could then also be shared across sectors, thus generating wider access. Depending on the specificities of each industry sector and the type of busi-

[195] These measures may entail legal research to identify national laws which may support innovation. Such an analytical approach was, for example, advocated by several stakeholders during the workshops carried out by Deloitte as part of this study. An analytical approach, first looking into available solutions in competition law, is also favoured in: *Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public consultation on Building the European Data Economy"*, http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf

[196] This was demonstrated by the stakeholder consultations and case studies carried out by Deloitte as part of this study, see e.g. the case study on Chemicals, Annex 2

[197] This said, the exact concerns of stakeholders depend on the role in the data value chain.

ness in the data value chain, the case studies and the general survey[198] revealed that interoperability is a crucial prerequisite for data exchange to take place effectively and at low cost.[199] Thus, addressing these barriers through the adoption of common standards (across sectors) and the development of guidelines could help reduce costs and potentially increase data sharing and the development of new business models.

In addition, this option could be effective in addressing the other barriers (e.g. how to value data, skills etc.). Through the **identification and dissemination of best practices**, more businesses are expected to become aware of the potential of the data economy. For instance, platforms such as ODPi[200] facilitate learning and increase awareness on the standards and practices available, thus fostering knowledge and making it possible for less resourced companies to reap the benefits of Big Data. Moreover, the open community created around this platform also provides relevant expertise and insights into specific needs and questions coming from stakeholders.

As a side-effect, the increased cooperation between businesses that would be needed to implement this option could help create a climate of increased trust. This could contribute further to increased data sharing.[201]

However, it is possible that the solutions would not be useful to all businesses and sectors, as they might not match their specific concerns. For instance, companies situated in the data access segment of the supply chain (e.g. same-sector downstream providers) might have needs in terms of access to data (e.g. real-time access to specific data, technical issues) which are not addressed through these soft and general measures. Moreover, where there are significant obstacles due to unequal bargaining power and fierce competition between stakeholders in the market (e.g. car repairers and car manufacturers in the automotive sector), these measures might not be sufficient to protect those players with a vital need to access data. In addition, it is likely that smaller businesses would be at a disadvantage, as they have less bargaining power in industry-led standard-setting initiatives and when it comes to negotiating access rights.

New standards that would help lower the technical barriers and guidance on contract practices and legislation **could lower costs** for **business**. For example, if common standards were developed and more widely used, the degree of interoperability would increase.[202]

---

[198] 51% of the data users and (re-)users who responded to the general survey identified lack of interoperability and technical standards as a blocking factor, very important or considerable barrier preventing them from deploying new business models. This percentage increases significantly if one considers the data of the targeted survey to start-ups and data analytics companies. In fact, amongst these more innovative businesses, 86% of respondents identified technical barrier as a major obstacle.

[199] This is particularly true if one looks at the future of smart industries as standardisation is one of the precondition for the emergence of a strong Industry 4.0 in Europe. Industry 4.0, Study for the ITRE committee, European Parliament, 2016, see: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf

[200] See: https://www.odpi.org/

[201] The general survey showed that uncertainty about usage of the data and what others will do with it is a major issue for 35% of respondents (blocking factor – 12%, very important barrier - 25%). Thus, increased trust might help to reduce such uncertainties.

In addition, businesses may be able to secure benefits from new data-sharing activities. This could also result in **lower consumer prices**. Moreover, best practices and information sharing on consumer rights could to some extent help ensure **better enforcement of rules on consumer protection and safety**, including rules on liability and compensation for damage.

As the option includes soft measures, the magnitude of the expected effects described above depends on the willingness of businesses to take up new practices and standards.

The option is supported by a large number of stakeholders. For example, during the workshop with SMEs carried out in the context of this study, 37% favoured a horizontal over a sector-specific approach.

Achievement of general objectives

Through the reduction of barriers and problems faced by businesses, this option would also have a positive impact on the achievement of the general objectives.

As this option entails soft measures, it would not harm the current effort of business model experimentation in this early phase of the market. In addition, an increase in awareness among business and an increased level of data sharing would support the development of innovative business models in Europe.[203] It is possible that the exchange of practices would lead to new ideas. In addition, innovation would be supported via increased funding of research activities. Thus, the measures could have a positive effect on the stage of market development and accelerate the take-up of the data economy. The positive effects might not be fully realised as there would still be disadvantages for smaller businesses.

The effects on the protection of fundamental rights and digital inclusion would be rather small. While there could be positive effects in relation to consumer safety and consumer rights, this would depend heavily on the willingness of businesses to become active in this area.

Efficiency: Costs and benefits of the option

Costs of the option

This option would entail moderate costs.

Businesses could incur some costs relating to the participation in events aimed at the exchange of good practices and standard-setting. The magnitude of these costs depends on the number and type of events businesses choose to participate in. Overall, the costs should be affordable for businesses. As this is a voluntary activity, every business will be able,

[202] It was shown in the stakeholder consultations carried out by Deloitte, including the web-based surveys, interviews and workshops that technical barriers are an important cost factor. Cf. e.g. Case study on the Financial Sector.

[203] The potential of data-driven business models for innovation has been analysed in recent OECD publications, notably OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, p. 132, http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en; OECD (2016), Maximising the Economic and Social Value of Data – Understanding the Benefits and Challenges of Enhanced Data Access.

moreover, to decide on the extent to which they want to contribute to such activities based on their resources.

In addition, businesses would incur costs for implementing new standards. Depending on the standard, this could for example entail the implementation of new IT systems. Again, the costs would be voluntary. Thus every business would only do what is affordable (which could be different for bigger players and SMEs, supposing that the latter have less resources available to invest in this area).

At the EU level, moderate costs would be incurred if additional funding were made available. It is expected that these costs would be moderate, as a number of relevant programmes already exist (e.g. H2020 for the research part, ISA2 etc.) In addition, some costs would arise in coordinating the different initiatives, e.g. organising and facilitating events aimed at the exchange of good practices.

National public administrations would also incur moderate costs in relation to the participation in the exchange of good practices, and in specific coordination and cooperation activities. Additional costs might be incurred in relation to legal research on the application of legislation to the data economy or developing guidance documents on existing legislation.

Benefits of the option

This option would have multiple benefits.

As mentioned under effectiveness, the effects of this option would be positive overall, as it could lead to more data sharing, including better access to and (re-)use of data. This would lead to lower costs for businesses and eventually to lower consumer prices. In addition, innovation would be supported, with positive effects for the performance of the European economy.

As the option entails soft measures, the exact benefits depend on the participation and take-up by the stakeholders. The fact that the option leaves freedom of choice to businesses and Member States can be seen as a benefit in itself.

Coherence of the option

This option is coherent with existing initiatives at the international, EU and national level.

At the international level, it is for example in line with the position and activities of the OECD in this domain. No evidence was found of interference with other existing initiatives.

The option is in line with many other initiatives at the EU level in multiple domains, including the DSM, H2020, ISA2, the eGovernment Action Plan, the Big Data Value PPP etc.

In the Member States, there are several on-going initiatives aimed at supporting the data economy and/or at addressing the barriers identified as part of this study (e.g. development of model contracts[204]). Based on the soft nature of this option, no interference is expected.

Policy Option 1B: Sector-specific non-regulatory measures

Policy Option 1B includes sector-specific non-regulatory measures. The operational measures used to implement option 1B would be similar to those identified under option 1A, but target specific sectors. They would, therefore, still comprise:

- Encouraging the identification and dissemination of best practices;
- Establishing appropriate standards, assessment schemes and benchmarks for the data economy;
- Establishing specific coordination and cooperation mechanisms with Member States to address cross-border challenges; and
- Funding innovation and research.

Key findings of the assessment

The table below provides an overview of our assessment of Policy Option 1B. The detailed assessment in accordance with the individual assessment criteria can be found in the subsequent sub-sections.

Table 16: Key findings of the assessment of Policy Option 1B

Assessment criteria	Rating (-5 to + 5)
Effectiveness	
Achievement of specific objectives	2
Achievement of general objectives	1
Efficiency	
Costs	-2
Benefits	3
Coherence	
Coherence with existing initiatives	2
Sum	**6**
Average	**1.2**

Source: Deloitte

[204] For example, the Netherlands started an initiative aimed at developing standard contracts that can be (re-)used by the various stakeholders willing to access and share data. The standard contracts were developed in a collaborative way.

Effectiveness in achieving the policy objectives

Achievement of specific objectives

This option is expected to have very positive effects on the achievement of the specific objectives.

As in the case of Option 1A, **data sharing would be supported** and would be likely to increase to a moderate extent. This is because it is expected that the barriers businesses currently face will be reduced. This is described in the following paragraphs.

Sector-specific soft measures would help reduce the **legal barriers** identified as part of this study. Uncertainty in relation to existing legislation could potentially be reduced based on the awareness-raising measures targeting policy makers[205] and cross-border cooperation mechanisms. The promotion of contractual practices or templates could help businesses in ensuring access to and (re-)use of data.[206] Based on awareness-raising, the exchange of good practices and potentially the development of model contracts, businesses could be encouraged to be more open about the (re-)use of their data. This is supported by feedback received during the workshops with industry representatives, especially from SMEs. In the Netherlands, for instance, ministries have implemented the national initiative 'Dare to Share' that targets corporations and SMEs alike, and encourages the businesses to share information, as well as to establish good practices or common rules. This initiative is, however, still in its early testing stages.

Difficulties relating to liability would also be improved by sector-specific soft measures. The data collected for this study suggests that companies tend to decide on a case-by-case basis and through contractual means which liability assurance they need and want. This can result also from the legal uncertainty about the overall liability regime. However, the sector-specific approach could lead to fragmented approaches to a topic that is relevant for the whole data economy.[207]

Option 1B would be particularly relevant to more effectively recognise and address the distinct characteristics of submarkets of the data economy. By way of example: access and use

[205] These measures may entail legal research to identify national laws which may support innovation. Such an analytical approach was, for example, advocated by several stakeholders during the workshops carried out by Deloitte as part of this study. An analytical approach, first looking into available solutions in competition law, is also favoured in: *Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public consultation on Building the European Data Economy"*, http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf

[206] As demonstrated in the section on contractual and legal barriers in Chapter 3, companies rely on contracts to regulate and govern their exchanges of data. To give an example, (re-)use of third party data is normally defined by contracts and restricted as far as possible. This has been demonstrated by the stakeholder consultations and case studies carried out by Deloitte as part of this study, see e.g. the case study on Chemicals, Annex 2

[207] As mentioned in Chapter 3, liability seems to be a transversal concern affecting businesses' situation at different stages of the value chain and in different sectors. This said, the exact concerns of stakeholders depend on the role in the data value chain.

rights to specific types of electronic data have already been created in the public sector (via the PSI Directive as amended), to certain payments data (via the PSD 2 Directive), to vehicle repair and maintenance data (via the Repair and Maintenance Information (RMI) Regulations)[208], and to some extent for personal data (via data access and portability rights in the GDPR).

Option 1B would also allow a clearer distinction to be drawn between purely digital content (such as the data processed through online services) and tangible movable goods that collect, generate or otherwise process digital data (such as the IoT or robotics). The complexities for these two categories are slightly different, since tangible movable goods can interact more directly with the physical world, thus arguably creating different liability concerns and fewer data access, use and portability difficulties. Non-regulatory intervention might therefore also differ: whereas digital content would be likely to benefit from model contractual terms, the IoT/robotics arguably require a stronger emphasis on safety standards and safety assessment methodologies, since they can operate (and create damage) outside a purely contractual framework. Option 1B would be more conducive to reflecting these distinctions in comparison with horizontal measures.

The **establishment of standards** would help to address technical barriers. A sector-specific approach may be positive, as specific challenges could be addressed in a targeted manner. Addressing these barriers could help reduce costs and potentially increase data sharing and the development of new business models.[209]

In addition, this option could be effective in addressing the other barriers (e.g. how to value data, skills etc.) Through the **identification and dissemination of best practices**, more businesses are expected to become aware of the potential of the data economy.

As a side-effect, the increased cooperation between businesses that would be needed to implement this option could help create a climate of increased trust. This could contribute further to increased data sharing.[210]

On this basis, **costs** for businesses relating to legal and technical barriers could be reduced and businesses might be able to secure benefits from new data sharing activities, as also explained in relation to Option 1A. This could also result in **lower consumer prices** as busi-

[208] https://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/vehicle-repair-maintenance_en

[209] Depending on the specificities of each industry sector and the type of business in the data value chain, the case studies and the general survey have revealed that interoperability is a crucial prerequisite for data exchange to take place effectively and at low costs. 51% of the data users and (re-)users who responded to the general survey identified lack of interoperability and technical standards as a blocking factor, very important or considerable barrier preventing them from deploying new business models. This percentage increases significantly if one considers the data of the targeted survey to start-ups and data analytics companies. In fact, amongst these more innovative businesses, 86% of respondents identify technical barrier as a major obstacle. See also: Industry 4.0, Study for the ITRE committee, European Parliament, 2016, see: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf

[210] The general survey showed that uncertainty about usage of the data and what others will do with it is a major issue for 35% of respondents (blocking factor – 12%, very important barrier - 25%). Thus, increased trust may help to reduce such uncertainties.

nesses operating in competitive landscapes have incentives to forward (internal) cost reductions through increased efficiency to their customers (especially to end-consumers) in order to obtain a competitive advantage vis-à-vis other relevant market participants. Such 'discounts' can, on the one hand, create awareness of specific products or services among new customers while it can also strengthen existing client relationships. Moreover, best practices and information sharing on consumers' rights could help ensure better enforcement of rules on consumer protection and safety to some degree, including rules on liability and compensation for damage.

As the option includes soft measures, the magnitude of the expected effects described above depends on the willingness of businesses to adopt new practices and standards.

This option received strong support from stakeholders. For example, during the workshop with SMEs carried out in the context of this study, the majority of participants favoured a sector-specific over a horizontal approach.

Achievement of general objectives

By reducing the barriers and problems faced by businesses, this option would have a positive impact on the achievement of the general objectives.

As is the case of Option 1A, this option would not harm the current efforts to experiment with business models in this early phase of the market based on its soft nature. In addition, an increase in awareness among business and an increased level of data sharing would support the development of innovative business models in Europe.[211] It is possible that the exchange of practices could lead to new ideas. In addition, innovation would be supported via increased funding of research activities. Thus, the measures could have a positive effect on the stage of the market development and accelerate the take-up of the data economy. The positive effects could be slightly hampered because smaller businesses continue to be at a disadvantage.

As explained under Option 1A, the effects on the protection of fundamental rights and digital inclusion would be rather small. There could be positive effects in relation to consumer safety and consumer rights. However, this depends heavily on the willingness of businesses to become active in this area.

Efficiency: Costs and benefits of the option

Costs of the option

This option would entail moderate-costs.

Option 1B would entail the same types of cost as Option 1A, that is to say:

[211] The potential of data-driven business models for innovation has been analysed in recent OECD publications, notably OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, p. 132, http://www.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en; OECD (2016), Maximising the Economic and Social Value of Data – Understanding the Benefits and Challenges of Enhanced Data Access.

- Costs **for businesses** related to:
  - The participation in events aimed at the exchange of good practices and standard-setting;
  - The implementation of new standards;
- Costs at **the EU level** related to:
  - The increase in funding;
  - The coordination of the activities;
- Costs for **national public administrations** related to:
  - The participation in the exchange of good practices, and in specific coordination and cooperation activities;
  - Legal research into the application of legislation to the data economy or preparing guidance documents on existing legislation.

As explained for Option 1A, the costs are expected to be moderate/affordable, in part because some activities are already on-going. Overall, the magnitude of costs might be slightly higher for all stakeholders involved than for Option 1A, as a sector-specific approach might mean that there would be a higher number of initiatives. For example, there might be different working groups or events covering different sectors, but all the same topic.

Benefits of the option

This option would have multiple benefits.

As mentioned under effectiveness, the overall effects of this option would be positive, as it could lead to more data sharing, including better access to and (re-)use of data. This would lead to lower costs for businesses and eventually in lower consumer prices. In addition, innovation would be supported, with positive effects for the performance of the European economy.

As the option entails soft measures, the exact benefits depend on the participation and take-up by the stakeholders. The fact that the option leaves freedom of choice to businesses and Member States can be seen as a benefit in itself.

Coherence of the option

This option is coherent with existing initiatives at the international, EU and national level.

At the international level, it is for example in line with the position and activities of the OECD in this domain. No evidence was found of interference with other existing initiatives.

Similarly, the option is in line with many other initiatives at the EU level in multiple domains, including the DSM, H2020, ISA2, the eGovernment action plan, the Big Data Value PPP etc. Moreover, as mentioned above, some sector-specific legislation already exists at the EU level. Sector-specific non-regulatory intervention (as contemplated by Option 1B) could build on these existing measures and would not override them.

In the Member States, there are several on-going initiatives aimed at supporting the data economy and/or at addressing the barriers identified as part of this study (e.g. development of model contracts). Based on the soft nature of this option, no interference is expected. On

the contrary, as Member States tend to follow sector-based approaches, this option may suit their activities very well.

Policy Option 2A: Legislative horizontal measures targeting the data economy as a whole

Key findings of the assessment

The table below provides an overview of our assessment of the Policy Option 2A.

We have provided a separate analysis concerning:

- The adoption of new legislation; and
- Amendments of already existing legislation.

The two options should not be seen as separate sub-options under the overall horizontal legislative approach of this policy option, but rather as complementary sides of the same medal. This is why we have provided one rating for both together instead of separate ratings for each of the approaches.

The detailed assessment in accordance with the individual assessment criteria can be found in the following sub-sections.

Table 17: Key findings of the assessment of Policy Option 2A

Assessment criteria	Rating (-5 to + 5)
Effectiveness	
Achievement of specific objectives	*+2*
Achievement of general objectives	*+1*
Efficiency	
Costs	*-4*
Benefits	*+3*
Coherence	
Coherence with existing initiatives	*-3*
Sum	***-1***
Average	***-0.2***

Source: Deloitte

Effectiveness in achieving the policy objectives

Achievement of specific objectives

Overall, this policy option is expected to contribute positively to the achievement of the specific objectives.

Analysis of the adoption of new legislation

First and foremost, a legal instrument that would homogeneously define data access and ownership would contribute to ensuring the effective implementation of standards on the access to data by businesses and citizens across different industries. This would give all stakeholders involved a level playing field and equal opportunities both in initiating, as well as developing their business model further. Naturally, this is of particular relevance for SMEs and start-ups that might otherwise face difficulties in the baseline scenario in developing their business as they might be tied to the willingness to share data of larger corporations.

Particular positive impacts could be expected in industries that are currently governed by large incumbents that hold a lot of data and are not able or willing to share these with smaller players, e.g. for the sake of keeping their competitive advantage.

The definition of data ownership and respective usage rights for up- and downstream businesses, as well as in the relationship between businesses and users of a product or service is expected to clarify the legal framework for stakeholders and similarly provide a level playing field for businesses (SMEs and large enterprises) to develop their business model and find their niche in the data economy.

Issues around data ownership and access – such as those currently faced in the automotive after sales market – could be overcome and essentially contribute to reducing costs for businesses in the long run.

It is important to keep in mind that the baseline scenario is also expected to lead to a reduction in the costs of data sharing in the long term in line with the typical s-curve development of the data economy and respective products and services. The main benefit of one or more legislative horizontal measures targeting the data economy as a whole would be that an equal playing field would be achieved sooner, so businesses' opportunity costs decrease faster (as discussed under efficiency).

This would also have a positive effect on prices paid by consumers. It could be expected that businesses would not only pass on their savings to their customers but also eventual *gains* through a level playing field in data access and ownership, e.g. in the form of lower prices or increased freedom of choice.

The definition of a data portability right within this policy option would have particularly positive effects on the extent to which consumers are able to choose freely and seamlessly between different product manufacturers and service providers. Ensuring freedom of choice for consumers in that way is also expected to have a positive impact on the prices paid by consumers compared to the baseline scenario.

Similar positive impacts can be expected if a horizontal legal instrument addressed liability in the data economy, e.g. by recasting the Product Liability Directive, or by providing an alternative liability regime for products with an elevated risk profile. Improving consumers' certainty and the effectiveness of compensation for damage is viewed as a positive impact and contribution to a level playing field not only between businesses but also the B2C aspect of the data economy.

The extent to which a legislative horizontal measure targeting the data economy as a whole could ensure such positive impacts for businesses and citizens depends on the specific form of the legal instrument. A Directive setting minimum standards in all Member States would be likely to have a more limited positive impact than a Regulation that provides for an equal legislative framework in all Member States. While it would probably be more difficult initially to get a Regulation adopted, a Directive could serve as a viable solution in the medium term and a basis for further discussion and development in the long term. The advantage of a Regulation would be that it would be expected to ensure increased compliance and behavioural change on the part of companies compared to a Directive.

A legislative horizontal measure targeting the data economy as a whole would be positive for industries that are currently already comparatively advanced in their data-related development. However, sectors that are less mature today could be expected to suffer from issues arising from legislation based on today's problems in specific industries that may not be relevant in other industries tomorrow. This could have the adverse effect of increasing costs for businesses that are affected by legislation but are not fully within its scope and/or part of the data economy. This could be a particular challenge for SMEs. Moreover, a horizontal legislative instrument could be seen as a barrier to self-regulating sectoral initiatives and competitive developments between companies (e.g. in the area of platforms), in particular it could reduce the potential for industry to experiment with data, as well as for SMEs and start-ups to take advantage of the current unclear situation.

Finally, it is not clear what the "data economy" is today and will be in the future, and who exactly is in scope of the policy option. This leaves considerable leeway for legislators and enforcement bodies to interpret any EU initiative, as well as for industries to position themselves in and out of scope of legislation.

Thus, the extent to which policy option 2A would have positive impacts largely depends on its careful and balanced design without using abstract concepts to solve only specific problematic, industry-specific situations today.

Analysis of amendments to existing legislation

Data sharing can be expected to be fostered through the horizontal revision and update of existing legal instruments such as the Product Liability Directive (PLD) and the eCommerce Directive. However, the magnitude of the impact is expected to be small due to the absence of a specific instrument targeting data access.

However, as both of these instruments are currently under review and exactly how these the legal instruments will be updated is not known, so that a clear assessment is not possible at this stage.

An extension of the PLD's scope to ensure that data as such would qualify as a product – or to ensure that IoT devices and robots would be considered as products to which the Directive applies – could, however, result in an improvement of the situation for businesses and citizens compared to the baseline scenario. This would clarify the existing legal framework compared to the baseline scenario. Businesses would face less uncertainty compared

to the baseline scenario which, in turn, could translate into cost savings and improved efficiency in product and service development processes.

Moreover, citizens could benefit from lower prices as businesses can be expected to pass on any cost savings to consumers.

The revision of the PLD could, in particular, improve the position of consumers' with regard to the effective compensation for damage.

Achievement of general objectives

In line with the achievement of the specific objectives, this policy option is expected to have a positive impact on the achievement of the general policy objectives.

Analysis of the adoption of new legislation

As a horizontal EU policy measure by definition deals with cross-border issues, positive impacts are expected in to cross-border cooperation and trade between businesses, as well as between businesses and consumers.

The extent to which innovation and competition would be fostered depends, however, on the exact scope of the legislative instrument (i.e. a careful and balanced design) and its enforcement. It is crucial in this regard to recognise that the concrete, sector-related examples of specific cases (opportunities, threats, good practices etc.) driving the discussion today might not necessarily be the most suitable basis for the definition of abstract, cross-sectoral solutions for the future.

Conversely, legislative horizontal measures targeting the data economy as a whole could have a positive impact on competition and innovation in sectors that are currently more mature than others in terms of data sharing. The downside is that less mature sectors could suffer from missing an experimental phase during which SMES and start-ups could use an uncertain situation to their advantage. Thus, horizontal legislation could in the short run contribute to fostering innovation and competitiveness in some sectors, but could also hinder innovation and prevent disruptive business models emerging in others.

Thus, again, the direction and magnitude of the impacts largely depend on the careful and balanced design of the policy option, as well as its enforcement.

The same is true of the discussion around freedom of choice and digital inclusion as a fundamental right of citizens.

Analysis of amendments to existing legislation

Revising and updating existing instruments could contribute to improving achievement of the general objectives.

Under this policy option, however, the achievement of the general objectives is not expected to differ broadly from the baseline scenario due to the narrow scope of the recommended changes.

Liability risks might be better addressed than under the baseline scenario.

Efficiency: Costs and benefits of the option

Costs of the option

Analysis of the adoption of new legislation

The costs of this policy option are expected to be high. The order of magnitude cannot be determined at this stage as it is not clear what exactly the legislation would entail.

The policy option is expected to have an impact on different types of costs:

- *Costs related to the legislative framework/budgetary costs*, e.g. changes to national legislation and the development of guidance for public administrations and businesses;
- *Transaction costs*, e.g. communication with stakeholders, training, monitoring and enforcement of legislation;
- *Compliance costs*, e.g. administrative burden and opportunity costs; and
- Costs related to the *legal aspects*, e.g. lawyers' fees, which are particularly relevant for citizens.

Budgetary costs would be significant as a horizontal legislative measure targeting the data economy as a whole would naturally have to be all-encompassing and thus trigger changes to different types and parts of national legislation. In a similar vein, extensive costs could be expected for public authorities providing guidance.

This is also valid for transaction costs as – depending on the form, scope, and content of the horizontal measure– public authorities and businesses alike would have to interpret, understand and implement legislation within their own organisations, as well as develop relevant internal procedures.

Depending on the form, scope, and content of the horizontal measure, compliance costs are expected to be significant as well – in particular for SMEs and start-ups in sectors that are less mature than others today. Market entrants could also be expected to face higher costs than established incumbents, as they already have the opportunity to shape and adapt to legislation. Thus, a horizontal measure could be seen as a means of ensuring a level playing field among established market actors but make it harder for other businesses to enter existing markets. Depending on their current business model, however, incumbents could also face costs stemming from the re-organisation of their business models and its adaptation to the data economy.

While opportunity costs would be expected to decrease for businesses as horizontal legislation would ensure a level playing field, it could also be argued that less mature data economies or industries would suffer from increased opportunity costs as businesses – especially SMEs and start-ups – would not have the possibility of experimenting experiment with business models and using a degree of uncertainty to their advantage in order to carve out a niche for themselves in the data economy.

In the short term, costs related to the legal aspects are expected to be significant for businesses as new legislation must be interpreted, understood, and implemented by each organ-

isation. Lessons learnt from the implementation of the GDPR could be applicable here. In the long run, however, this could lead to a significant reduction in legal costs.

Legal costs for citizens are not expected to be significant under this policy option, given that this option would address liability in the data economy, e.g. by recasting the Product Liability Directive or by providing an alternative liability regime for products with an elevated risk profile.

Analysis of amendments to existing legislation

The budgetary costs of this option are expected to be limited at both the EU and Member State levels as the legal instruments *only* need to be adapted/updated and not developed from scratch. The magnitude of compliance costs would depend on the extent to which the different legal acts are modified and new obligations are imposed on businesses.

Depending on the exact changes, however, the magnitude of the policy option could also represent an unreasonable burden on innovative companies – especially SMEs and start-ups – before they are even able establish a new service or product.

Benefits of the option

Analysis of the adoption of new legislation

The main benefits of this policy option are grounded in the improvement of the effectiveness of the policy measures compared to the baseline scenario, as well as an increase of the efficiency of internal processes, as well as the development of new products and services based on data sharing.

The order of magnitude of costs, however, cannot be determined at this stage as it is not clear what exactly the legislation could entail apart from the potential cost-saving measures the Commission provided in its Commission Staff Working Document on the free flow of data[212]:

- Default contractual rules for data licences in B2B relationships to govern cases in which parties have not foreseen contractual clauses on these specific points;
- Access for public interest purposes, more specifically by public sector bodies, e.g. based on the (revised) Public Sector Directive;
- Data producer's right to non-personal or anonymised data in order to enhance the tradability of non-personal or anonymised machine-generated data as an economic good; and
- Access against remuneration to non-personal or anonymised data held by other economic players.

[212] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the document *Communication: Building a European data economy.* SWD(2017) 2 final. See: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy

Overall, the costs – or the extent to which these could be reduced – depend on the extent to which different industries are connected and actually sharing data, i.e. it is expected to be more of an individual, micro-level decision by businesses than an overall macro-economic effect of legislation.

Such efficiency gains, however, are expected to lead to cost reductions for businesses and thus for consumers.

Depending on the exact scope and content of the horizontal policy measure the option would have overall positive effects, as it could lead to more data sharing, including better access and (re-)use of data. This could result in lower prices for consumers.

Again, this depends largely on the careful and balanced design of the option as there is a risk that a horizontal measure would have a positive impact in some industries while simultaneously creating negative externalities in other industries or even policy areas. The benefits of such a horizontal policy measure could accrue to only a limited range of types of players in specific industries only, i.e. those currently suffering the most from limited access to data or unclear liability provisions, while not compensating for the costs that would be imposed on other firms – or even harming their current business models – that are facing less severe issues today.

Analysis of amendments to existing legislation

The benefits of the policy option are expected to be similar to the costs, albeit positive.

Coherence of the option

Analysis of the adoption of new legislation

The option would imply complexities due to the need to integrate appropriately with existing instruments (the GDPR, Product Liability Directive, eCommerce Directive, the consumer protection acquis, etc.)

Thus, depending on its exact scope and content, it is expected to be challenging to integrate the horizontal measure into the existing framework without jeopardising its coherence.

This is of particular relevance with regard to any specific legislative measures taken or under way at the Member State level.

In addition, the data economy is by definition international and not restricted to EU boundaries. Therefore, the coherence of any horizontal initiative with international standards (either existing or in development) is imperative for both businesses and consumers.

Analysis of amendments to existing legislation

Depending on the exact changes of the legal instruments, the policy option is expected to contribute to ensuring or to improving the coherence of the existing legal framework.

Policy Option 2B: Legislative measures focusing only on specific sectors

Key findings of the assessment

The table below provides an overview of our assessment of Policy Option 2B. The detailed assessment in accordance with the individual assessment criteria can be found in the subsequent sub-sections.

Table 18: Key findings of the assessment of Policy Option 2B

Assessment criteria	Rating (-5 to + 5)
Effectiveness	
Achievement of specific objectives	*+2*
Achievement of general objectives	*+1*
Efficiency	
Costs	*-3*
Benefits	*+1*
Coherence	
Coherence with existing initiatives	*-3*
Sum	***-2***
Average	***-0.4***

Source: Deloitte

Effectiveness in achieving the policy objectives

Achievement of specific objectives

Overall, this policy option is expected to contribute positively to the achievement of the specific objectives.

A sector-by-sector regulatory initiative could help improve interoperability and guarantee better access to data and more liability certainty in the sectors concerned. This is seen as an enabler of data-sharing in the specific sector.

At the same time, this means, however, that sector specific regulatory intervention has both the benefit and the downside of being highly targeted: while it avoids unintended side-effects, it is also arguably less capable of providing all-encompassing solutions.

For that reason, the direction and magnitude of impact that can be expected from this policy option are proportionately similar to those stemming from the implementation of a horizontal measure targeting the data economy as a whole – but limited to certain sectors in scope of the legislation.

As a consequence, sector-specific legislation could lead to the disintegration of established market structures and fuel the growth of innovative services in that specific sector. This could have a positive effect on costs incurred by businesses and prices paid by citizens.

Thus, the overall impact of sectoral legislation is expected to be positive but relatively less than for a horizontal measure.

This also means, however, that positive spill over effects expected under the horizontal policy measure cannot be expected for a sector-based solution and that the development of the data economy will thus be driven further by sector-specific problems and solutions that may not necessarily be applicable to or relevant for all sectors.

This does not fully contribute to a level playing field between actors across industries and cross-border.

That being said, as the nature of the data economy is not limited by sectoral boundaries (service providers in one sector can use data from another sector to provide relevant new services there), sectoral legislation may solve problems faced today, but give rise to grey areas and problems at the cross-roads of different sectors or between business models in the future.

Liability is a particularly important issue in that regard as products and services of manufactured or provided in one sector may depend heavily on products and services in other sectors. Diverging liability standards could hamper the effective governance of malfunctions and detriment, as well as impose new barriers to effective remediation of damage incurred by any party.

Thus, sectoral legislation is expected to be a short- to medium-term solution to solve the most urgent existing problems. Depending on the future development of the data economy, it is, however, not seen at this stage as the *ultimate* future-proof solution – rather a stepping-stone, module or building block towards a more sustainable solution.

Achievement of general objectives

The reduction in costs for businesses and consumers is expected to have a positive impact on the competitiveness and innovativeness of businesses in the sectors covered by the specific legislation. Positive impacts through the introduction of the PSD2 in the banking and fintech industry could be taken as illustrative examples of such a development. This could also lead to increased freedom of choice for consumers and thus contribute to ensuring their rights.

The magnitude of this positive impact, however, largely depends on the specific industry concerned and the extent to which this industry (and the data shared within the ecosystem) is linked in practical and business terms with other sectors.

To this end, it could also be case that positive impacts in one sector might have negative external effects in other sectors. Industries are heavily interconnected but an imbalance in the legislative playing field could trigger a development in which large, established enterprises in one sector move towards the provision of services that are genuinely located in other sectors but would then fall under new sector-specific legislation. This could have the adverse effect of increasing the market concentration around large incumbents in sectors that would be regulated under this policy option (for instance an automotive OEM (original

equipment manufacturer) providing banking, telecommunication, and insurance services or a large rail transport operator providing services in the area of B2B and B2C energy supply). Discussion around such "cartel-like effects of big-data applications" are only emerging at the moment.[213]

This would then, in turn, hamper the overall impact of the policy option on innovation and competitiveness in the Digital Single Market, as well as citizens' freedom of choice among digitally inclusive products and services.

Efficiency: Costs and benefits of the option

Costs of the option

The costs associated with the implementation are expected to be significant for the sectors in scope of the legislation. The order of magnitude of costs cannot be determined at this stage as it neither clear which sectors would fall under legislation, nor what exactly the legislation would entail.

The types of costs considered are similar to those under a horizontal measure. Budgetary costs, in particular, are expected to be significant as different legislative requirements would have to be developed, negotiated and implemented in several industries.

The same is true of businesses' compliance costs of businesses. As this policy option, however, deals with a sector-specific rather than a horizontal measure, the overall (macro-economic) magnitude of the impact is expected to be comparatively smaller – at least in the short- and medium-term.

This implies that it is crucial to assess the policy option in relation to the (macro-economic) size of the sector in scope. This means that legislation of larger industries is expected to have a larger cost-related impact than legislation of smaller industries.

At the same time, there is a need to acknowledge that, although costs could primarily be incurred within sector-specific silos, the collaborative, cross-sectoral, and disruptive nature of the data economy could trigger negative external effects in other industries (e.g. in the form of "cartel-like effects of big-data applications" as discussed above) that would, in turn, lead to *de facto* compliance costs and opportunity costs in other sectors as well – although it was initially not intended to regulate other sectors.

This could then trigger the need for sector-specific legislation in another industry.

Thus, sector-specific legislation in selected industries is not necessarily an alternative to horizontal legislation but rather horizontal legislation is the necessary consequence of sectoral legislation.

[213] See, for instance: Position Statement of the Max Planck Institute for Innovation and Competition of the 26 of April 2017 on the European Commission consultation on "Building the European Data Economy", Max Planck Institute for Innovation & Competition Research Paper No. 17-08,

From this perspective, the overall costs can be expected to be comparatively small in the short- and medium-term but could exceed those of e.g. horizontal legislation in the long term.

Benefits of the option

Benefits compared to the baseline scenario can be expected for businesses that are active in the sector in scope of legislation, as well as for consumers purchasing products or services from these businesses.

Again, the benefits are expected to relate to the improvement of the effectiveness of the policy measures taken today, as well as an increase in the efficiency of internal processes, as well as the development of new products and services based on data sharing.

The order of magnitude of benefits cannot be determined at this stage as it neither clear which sectors would fall under legislation, nor what exactly the legislation would entail. The overall magnitude of the benefits is, however, expected to be lower than for horizontal measures.

Coherence of the option

The same assessment of the coherence applies to policy option 2B as to policy option 2A. The main issue is increasing complexity in integration with existing instruments at the EU and national level, as well as the international (non-EU) character of the data economy at large.

Comparison of the options: Multi-Criteria-Analysis

In line with the European Commission's *Better Regulation Guidelines*[214] and its toolbox[215], most importantly tool 57[216], we carried out a Multi-Criteria Analysis (MCA) based on the data gathered as part of the sectoral analysis, the online survey and the workshops, as well as the interviews carried out with businesses.

Multi-Criteria-Analysis is a widely-used tool in policy evaluations, impact assessment studies, and feasibility studies that aims at drawing a conclusion on the comparative rating of potential policy solutions.

We have carried out such analysis in previous studies on behalf of various Directorate-Generals of the European Commission. As part of this study, we carried out a fully detailed MCA, as exemplified in the *Better Regulation Guidelines* in order to take full account of the complexity of the subject matter and the level of granularity of the previous analyses carried out.

Thus, the complex MCA approach as presented below is regarded as an added value to the study, much less than it is seen as adding complexity to an already very difficult subject.

[214] http://ec.europa.eu/smart-regulation/guidelines/toc_guide_en.htm
[215] http://ec.europa.eu/smart-regulation/guidelines/toc_tool_en.htm
[216] http://ec.europa.eu/smart-regulation/guidelines/tool_57_en.htm

The MCA was carried out in the following three distinct steps:

- *Step 1:* Establish indicators or assessment criteria against which the policy options are assessed and compared. This includes establishing the performance of a policy option (i.e. the magnitude of its impact), the weight of the criteria in relation to each other, as well as the direction of the impact (negative/positive). The indicators are established in an analytical grid;
- *Step 2:* Build an outranking matrix in which the scores for all policy options and criteria are provided in order to summarise how the policy options compare with each other in relation to established criteria; and
- *Step 3:* Prepare a so-called permutation matrix that enables the selection of a final ranking of all the possible policy options against each other. This means that it is possible not only to select a preferred policy option but also a ranking of all other options against each other.

Step 1: Establishing assessment criteria and indicators

As an illustration for Step 1, we drafted an **analytical grid** in which the scores for all policy options are collected and compared in relation to each criterion towards each other.

Table 19: Analytical grid for the assessment criteria

Main assessment criterion	Weight	Direction (positive /negative)	Performance value (Baseline scenario always 0)				
			BS	1A	1B	2A	2B
Effectiveness of the policy options in reaching the specific and general policy objectives	2	+	0	3	3	3	3
Efficiency	1.5	+	0	2	1	-1	-2
Coherence of the policy options	1	+	0	2	2	-3	-3

Source: Deloitte.

The *performance* of a policy option is multiplied by its *weight* and its *direction,* as well as totalled across all assessment criteria in order to devise a weighted performance.

Step 2: Building an outranking matrix to compare policy options

In relation to Step 2, the following table provides an **outranking matrix** in which all the weights indicated in the table under step 1 are totalled for the criteria in relation to which a policy option is favoured over another policy option (abbreviated e.g. as "AB") as indicated by the weighted performance of each criterion.

This means that the outranking matrix provides an overview of the overall scores of the policy options compared to each other (i.e. the differences between them).

Table 20: Outranking matrix

	BS	PO 1A	PO 1B	PO 2A	PO 2B
BS	0	0	0	2.5	2.5

	BS	PO 1A	PO 1B	PO 2A	PO 2B
1A	4.5	0	1.5	2.5	2.5
1B	4.5	0	0	2.5	2.5
2A	2	0	0	0	1.5
2B	2	0	0	0	0

Source: Deloitte.

Naturally, the grey combinations received a score of 0 as it does not make sense to compare these. In essence, the table shows that the impacts of the policy options outrank those of the baseline scenario and that policy options with a higher score outrank those with a lower score.

The differences between the overall rankings of each policy option between each other as presented above are derived from the sum of the individual scores per policy option and assessment criterion in the analytical grid.

Step 3: Preparing a permutation matrix to identify the order of preference

In the present assignment, i.e. with six policy options, 120 permutations are possible.[217]

Thus, an overview of all 120 policy ranking **permutations**, as well as respective policy pairings, and coefficients of policy pairings with final scores, are provided in Annex 5 – Supporting tables for the Multi-Criteria Analysis.

As can be seen from the tables in Annex 5, the permutation with the highest coefficient based on the outranking scores of its policy pairings is #31, i.e. **1A-1B-BS-2A-2B**.

This means the following:

- **Policy option 1A is the preferred policy option** as it provides the most favourable combination of effectiveness, efficiency, and coherence;
- If 1A cannot be implemented, **1B would be the second most favourable**;
- The baseline scenario is more favourable than 2A and 2B; and
- The **least favourable option is 2B**.

Moreover, the coefficients table shows that permutations #33 and #34 are only 0.5 to 1 points behind the preferred permutation. This means that it does not have a substantial impact on the choice of preferred policy option how the baseline scenario, policy option 2A, and 2B are ranked, as 1A and 1B seem to contain a much more favourable combination of effectiveness, efficiency and coherence.

[217] As a general rule, there are N! (factorial) different ways to rank the policy options which must be "scored".

6 Conclusions

The emergence and consolidation of data driven business models and the increasing reliance on IoT, robots and autonomous systems are not completely new phenomena in Europe. On the contrary, they have been around for long enough to start showing certain features, shortcoming and risks which policy makers want to monitor and assess.

For the legislator, the aim of this monitoring exercise is twofold: on the one hand, there is a need to facilitate the establishment of these technologies so as to strengthen the competitiveness of the Digital Single Market, and promote growth and jobs. This means, for instance, acting to remove the barriers to the sharing and access of data in order to support the EU data economy and unlock its full potential. On the other hand, it is crucial to protect consumers and citizens from the possible downsides of these emerging technologies. This could entail, for instance, setting up a solid and appropriate liability regime for IoT, robots and autonomous systems.

Although the interests at stake for the legislators are clear, recent data show that the markets related to these technologies in the European Union are only in the 'emergence phase' which results in a difficulty in producing accurate analysis of future barriers and challenges and in serious obstacles when it comes to quantifying them. The objective of this study was therefore to formulate a number of 'early' hypotheses about the emerging barriers to the data economy and the challenges brought by IoT, robots and autonomous systems in terms of liability, and to collect what evidence is available in order to validate/falsify them.

Given the infancy of the markets considered, this report should be considered as a first attempt at examining this topic and gathering the existing data on these subjects. This analysis is therefore based on the limited data available and provides a preliminary (mainly qualitative) overview of the main trends, barriers and risks which should be the object of the policy makers' attention for the future with respect to the data economy as well as the IoT, robots and autonomous systems technologies.

In considering the European data economy and the B2B sharing and access of data, it in fact emerged quickly from the analysis that the EU data market is still in the 'emergence phase' as only 6.3% of European companies are already intensive data users. This means the experience of most European businesses with data access, sharing and re-use is so far limited, and that they have thus not yet encountered to any extent the barriers which are the object of this assessment.

Notwithstanding this context of 'emergence' of the market, it was assumed that a number of barriers existed which were hampering the development of further data-based business models and slowing down the market take-up. A number of barriers were originally considered:

- ‘Ownership’ of data;
- Interoperability;
- Access and re-use of data;
- Liability;
- Intellectual property rights;
- Portability of data.

The empirical evidence as well as legal analysis showed that while some of them (such as interoperability, liability and access and re-use of data) are indeed primary obstacles to the full deployment of the data economy, others are more secondary (e.g. ‘data ownership’, portability and IPR). Moreover, it emerged that ‘other barriers’ not originally considered, such as the lack of skills or the unequal bargaining power between stakeholders, need to be included among the primary barriers as they constitute considerable obstacles to all companies in general (e.g. skills) or to specific categories of companies (e.g. unequal bargaining power). Indeed, this analysis also illustrated that the type of barriers a company is more likely to face depends on three main characteristics:

- Its sector
- Its position in the data value chain
- Its size.

The combination of these aspects determines whether one of the barriers identified will be a blocking factor or not for a certain company which is willing to share, access or re-use data. This also explains why no agreement could be reached among stakeholders when discussing the magnitude and relevance of these barriers overall. The analysis also showed that, if policy-makers do not intervene, the development of the EU data market will be slower and uneven depending on the sectors and types of company.

Similar considerations emerged from the analysis of the issues related to the liability of IoT, robots and autonomous systems. It was originally assumed that the development and uptake of the IoT, robotics, and autonomous systems in the EU was being hampered by deficiencies in liability legislation. Once more, the difficulties in the data collection showed that the market of IoT, robots and autonomous systems in Europe is not fully mature yet, which makes the identification of concrete issues and cases at this stage very complex. Nonetheless, the analysis of the existing legal frameworks (at the EU and the national level) and their shortcomings with respect to IoT, robots and autonomous systems and of the characteristics of these new technologies (autonomy and complexity) led to the conclusions that:

- It is undue costs borne by stakeholders that are the impediment to the take-up of IoT, robotics, and autonomous systems;
- Divergences in national liability regimes create market barriers for producers and service providers; and
- Injured parties cannot count on the availability of redress.

It was also found that there are currently three determinants of the degree and types of liability issues that IoT, robots and autonomous systems can bring. These are the diversity of

the market and existing technologies (in terms of autonomy, determinism, dependence, operating environment and risk context), the diversity in the stakeholder ecosystem and the novelty of the market. If no action is taken by the legislators to clarify the regulatory environment, the liability challenges identified will have a direct effect on the innovation potential and performance of the Digital Single Market. Moreover, by affecting the most innovative businesses in Europe, in particular, these liability challenges will slow the innovation path of the IoT and robotics market in Europe.

Given this context and the outcomes of the two problem assessments, the following policy options (both soft/non-regulatory and hard/regulatory as well as horizontal or sector specific) were put forward:

- **Option 0 – No intervention:** No particular policy measure is taken to address these emerging barriers. This option constitutes the baseline scenario against which all other options are assessed.
- **Option 1A – Horizontal non-legislative measures:** These could include awareness raising measures, sharing of best practices, funding research etc. All these measures would not target one sector specifically but rather be cross-sectoral and cross-domain.
- **Option 1B – Sector- specific non-legislative measures:** This policy option mirrors option 1A but takes a sectoral approach, meaning that the measures should target one or more specific sectors (e.g. sharing of best practices in the aviation sector, funding research for the automotive sector, awareness-raising in the chemicals sector etc.)
- **Option 2A – Horizontal legislative measures:** These could include one or two regulatory measures targeting the barriers in liability, access and (re-)use of data or interoperability in a horizontal way and covering all sectors at the same time. The regulatory measures could take the form of Regulations or Directives.
- **Option 2B – Sector-specific legislative measures:** This option mirrors option 2A but would entail the adoption of sector-specific Regulations or Directives (e.g. Regulation concerning access to data in the automotive industry).

The assessment of each of these policy options against the effectiveness, efficiency and coherence criteria showed that options **1A (horizontal non-legislative measures) and 1B (sector specific non-legislative measures) were respectively the first and second best** in the final multivariate ranking. The baseline scenario (policy option 0) then ranked third while options 2A and 2B came at the bottom. This means that, at the present stage, soft measures such as awareness-raising, sharing of best practices and funding research and innovation from a horizontal perspective are more effective, efficient and coherent (thus desirable) than any other option. The same measures could also be pursued from a sector-specific perspective, but this would be considered as sub-optimal also knowing that borders between sectors and topics are increasingly challenged by the digital economy.

This outcome is consistent with the overall analysis as well as with the principle underlying evidence-based policy making. Indeed, in the absence of well-defined market failures and precise problems, regulatory measures should be considered carefully in order to avoid missing the desired target. This does not mean that regulation might not be needed in the future or that soft measures will be sufficient to address these emerging barriers and issues. On the

contrary, continued monitoring of the situation and further study of these questions is strongly recommended so as to obtain a more refined problem assessment when new/more data become available.

To conclude, European businesses are currently examining and integrating new technologies such as data, IoT, robots and autonomous systems in their ways of working. They do not yet have a final and consolidated perception of how these will work for them and which particular challenges they will bring in future. The impact of these issues and barriers also depends on the company's characteristics in terms of sector, size and position in the value chain. However, data, IoT and autonomous systems technologies are also transforming sectors and value chains as such, which adds a layer of complexity to the identification of future barriers and challenges. Therefore, at the current stage, the role of the European policy maker is to accompany businesses in the journey by further investigating these complex topics in a horizontal way, sharing knowledge and best practices and being prepared and reactive when (or if) well defined and particular issues do emerge.

Annex 1 – Outcome of the legal mapping

This Annex contains the outcome of the legal mapping carried out in the Member States with respect to data ownership, M2M contracting and liability of IoT, robots and autonomous systems.

Ownership

Member State	State of play
Austria	Austrian law basically distinguishes between two categories of exclusive rights: property of things ("Sacheigentum") according to § 308 in conjunction with § 354 of the Austrian General Civil Code (Allgemein Bürgerliches Gesetzbuch, "ABGB") and so-called "intellectual property" (Geistige Eigentum), including patent, trademark, copyright, utility model and design rights (Immaterialgüterrecht). With regard to the property of things, the ABGB provides as follows: (i)§ 285 ABGB defines "things" (Sachen) as "everything that is different from a person and serves the use of humans is called a thing in the legal sense" whereas (ii)§ 285 ABGB merely excludes animals from this legal definition of "things" and (iii)§ 353 ABGB provides that "Everything that belongs to somebody, all his/her tangible and intangible things, is called his/her property". Therefore, Austrian legal commentators **generally argue that data/information falls within the legal definition of "intangible things"** (see, e.g., Koziol – Welser/Kletečka, Bürgerliches Recht I14 (2014), mn 766, referring also to Andreewitch/Steiner, Outsourcing – Herausgabe der Daten bei Vertragsbeendigung?, ecolex 2005, 358 and Thiele, Nochmals: Übertragungsanspruch bei Domainstreitigkeiten, RdW 2006, 80 fn 80 et sequ). However, it is also clear that the ABGB's **regulations on the property of things are not applicable to intangible things such as data** (see, e.g., Koziol – Welser/Kletečka, Bürgerliches Recht I14 (2014), mn 913; Helmich in Kletečka/Schauer, ABGB-ON1.02, §285 mn 2). Data as such also are not protected by any intellectual property rights currently existing in Austria. **In February 2015, The Austrian Green Party proposed a respective approach (see, e.g., http://derstandard.at/2000011407350/Datenschutz-Gruene-wollen-Daten-als-geistiges-Eigentum-etablieren) and several Austrian legal commentators are continuously discussing whether an intellectual property and/or a property of things approach towards data might make sense in general (see, e.g., Wiebe, IP Day2016 Hand-Out, p. 54-63).** However, all of these approaches came to nothing at present stage. With regard to a possible application of intellectual property protection to data, Austrian legal commentators usually refer to the fact that intellectual property protection specifically is only granted to efforts created by individuals, but not to mere data/information that is "just there". Also, the Austrian Supreme Court explicitly held in a copyright case that resizing images to thumbnails does not amount to any act relevant under the Austrian Copyright Act (Urheberrechtsgesetz, "UrhG"), particularly in case such resizing happens automatically without any human interaction being involved; in the same decision, the Austrian Supreme Court also explicitly held that computer-generated results are not to be qualified as "intellectual creations" in general (see Austrian Supreme Court, 4 Ob 105/11m – 123people.at/Vorschaubilder). Consequently, automatically generated data generally seem to be **barred at least from copyright protection**. If created by a human and reaching the required "originality" threshold, however, data may enjoy copyright-protection. Furthermore, and from a copyright-related point of view, mere data, respec-

Member State	State of play
	tively a collection thereof, may be protected under the sui-generis legal protection for databases laid down in § 76c to § 76e UrhG even if the "originality" requirement applicable to copyright-protected works is not met. However, even if data cannot be owned under Austrian law, this does not mean that there are no legal means to defend against any unlawful use of data: Firstly, and with a view to personal data, there is the Austrian Data Protection Act (Datenschutzgesetz, "DSG"), which is the lex specialis to the ABGB. Whilst the DSG equally does not speak of any "property" or "ownership" with regard to personal data, it provides data subjects (i.e., in contrast to other EU jurisdictions, individuals and entities, see § 4 fig 3 DSG) with claims that are quite similar (but not identical) to those granted by the ABGB to the owners of things. Most notably, the DSG does not provide data subjects with a claim for surrender of personal data (as laid down in § ABGB for owners of things), but instead with a claim for having personal data deleted/destroyed (§§ 26 to 29 DSG). Furthermore, data in general (i.e. not only personal data) enjoy protection under the Austrian Criminal Code (Strafgesetzbuch, "StGB") as § 126a StGB sanctions wilful damage to data that were created/transferred with EDP-support. Also, data in general may enjoy protection under the Austrian Unfair Competition Act (Gesetz gegen den unlauteren Wettbewerb, "UWG"): using third-party data without permission can be qualified as "unlawfully exploiting some else's accomplishment" (Ausbeuten fremder Leistung) or "passing off" (unmittelbare Leistungsübernahme) under § 1 UWG if committed consciously (see, e.g., Wiebe in Wiebe/G. Kodek, UWG I² (2012), mn 650 et sequ ad § 1 UWG). Finally, the Austrian Data Protection Authority is often pointing out that more and more technical data, for example data related to smart power meters, connected cars, wearables or, more generally speaking, in the Internet of Things ("IoT") context, have to be qualified as personal data because they often reveal information which may be used for identifying the individual who owns and/or operates such "connected"/IoT products by legal means (e.g. if such a smart and/or IoT product is linked to a user account which contains the user's entire name and/or other data which may be used for identification purposes, such as the user's address; see, e.g., also Schnider, Echte Rechtsgrenzen in der virtuellen Realität, DiePresse Online, 7.9.2016 = http://diepresse.com/home/recht/rechtallgemein/5081550/Echte-Rechtsgrenzen-in-der-virtuellen-Realitaet).
Belgium	Belgian legislation has **no specific provisions in relation to the ownership of data**. The Civil Code distinguishes between physical and non-physical goods ("biens corporels" versus "biens incorporels"). Physical goods are tangible, sense perceptible goods, such as objects, plants or animals. The provisions of the "law of goods" (droit des biens, zakenrecht) are applicable to these goods. Non-physical goods, on the contrary, are immaterial. These goods include, between others, ideas or creations of the mind, on which intellectual rights are applicable (copyright, patents, etc.) but also abstract collections of all kinds of goods, such as a commerce or a heritage, or even rights (usufruct, debt claim, etc.). The Belgian Civil Code further distinguishes between "rights in rem" (droits réels, zakelijke rechten) and claims (droits d'action, vorderingsrechten). "Rights in rem" create a legal relationship between a person and a physical good. Claims create rights between two or more persons. "Rights in rem" can be characterised as "absolute rights", in the sense that they are valid against anyone, while a claim, at least in principle, is only valid against a debtor. Another major difference between these two categories of rights consists in the fact that the Civil Code contains an exhaustive list of the rights in rem (the so-called "numerus clausus"), while the list of possible claims is endless and can continuously be extended through contracts. The "ownership right", as one of the "rights in rem" next to "possession", "usufruct", 'tenancy", "emphyteusis, "easement", etc. is defined by Art. 544 of the Civil Code as follows: "**the right to benefit and to dispose of a good in the most absolute manner, as long as the use of this right doesn't violate the laws and regulations**". The traditional view in Belgium is that the right defined in Art. 544 of the Civil Code exclusively refers to physical goods. It can, however, not be denied that this traditional view becomes progressively under pressure. This is partly due to the fact that legal terminology in Belgium is influenced more and more by European Union Law. In an interesting contribution published in the European Law Review (2014, n. 4, p.447-469), Eveline Ramaekers explains how EU law treats all types of objects (in EU second-

Member State	State of play
	ary law usually called assets) in the same way, as long as they represent an economic value, regardless of whether they are movable or immovable, tangible or intangible. Examples of things that fall within the definition of goods are electricity, natural gas, and even waste. Union law itself introduces a number of new, intangible, objects of property rights, such as the Community trade mark, the Community design and emission trading rights. As far as the Community trade mark and the Community design are concerned, the Regulations that introduce them both stipulate that they "may be given as security or be the subject of rights in rem" (read, for example, art. 19 of Council Regulation (EC) No 207/2009 of 26 February 2009 on the Community trade mark, Official Journal L 78, 24/03/2009 p. 1). Ramaekers also explains that, with the emission trading rights, the situation is a bit more complicated. Directive 2003/87 establishing a Scheme for Greenhouse Gas Emission does not of itself stipulate that emission trading rights can be objects of rights in rem as the Regulations on the Community Trade Mark and Design do. Of course, the Emissions Directive 2010/75/EU is a Directive, meaning that it is left to the Member States to choose the form and methods of implementation. The Trade Mark and Design Regulations, by contrast, became directly applicable in the Member States' legal orders, 24 leaving them no choice regarding the form of implementation. Because the Emissions Directive allows Member States to decide how to implement it, some Member States have decided to treat the emission trading rights as objects of property rights, whereas other Member States treat them as public law licences. In Belgium emission trading rights are sometimes qualified as public law authorisations (see M. Pâques, La nature juridique du quota d'émissions de gaz à effet de serre, in: X., Verhandelbare emissierechten als klimaatbeleidsinstrument, 2005, p, 43-69) but some other authors qualify them as rights in rem "sui generis" (see T. Martens, Een nieuw klimaat in het goederenrecht: groenestroomcertificaten, KU Leuven, Faculty of Law, Masters Thesis 2016). Notwithstanding the progressive evolution of the legal notion of property in Belgium, **the notion has not yet been applied to "data", neither in court decisions nor in legal doctrine**. It can however be expected that in the near future a discussion on this topic will be inevitable given the increase of economic transactions related to data. As in other Member States, Belgian companies, for example in the direct marketing sector, "sell" or "rent" data (for example postal addresses). The contracts used in this sector differentiate between "data sale" (the data can be (re-) used by the client without restrictions) and "data renting" (the data can be used by the client only once). In the case of "data sale" these contracts often state that the data become the "propriety" of the buyer. A thorough discussion on the legal qualification of the rights of buyer and seller in this context has, unfortunately, not yet been undertaken in Belgian legal doctrine. **The majority doctrine holds that ownership rights do not apply to digital data** (except of course in the context of materialised data on a data carrier, or in the context where the rights to data are being held, such as IP rights). Applying ownership doctrine to data could also raise other problems, since the Civil Code also holds that the "property of a movable or immovable entitles the owner to anything that the good produces and to anything that is united with it, either naturally or artificially" (Article 546). Application of this rule to digital data could significantly impact the possibility of modifying or enriching data for third parties. There is no civil case law making an explicit and definitive statement on the point. However, one of the earliest hacking cases under Belgian law[218], involving digital data (specifically mail messages) being unlawfully accessed and retained, was prosecuted under a claim of 'theft of computer energy', in the absence of any specific cybercrime legislation at the time. While such case law has not repeated since then and it is presently considered as an outlier, it is worth noting that apparently a claim of simple theft of data was seen as legally less obvious than theft of electricity. In another and older case[219] the copying of computer software was however qualified as theft; supported by the consideration that copyright certainly is a form of property. Globally, **there is no clear resolution** to the question whether data can be owned or not.
Bulgaria	Under Bulgarian law, **"data" as such (**information as it is) **cannot not be considered the object of ownership or to other proprietary rights**.

[218] Bistel ruling, Correctional Court of Brussels, 8 november 1990.
[219] Court of Appeal of Antwerp, 13 September 1984; discussed by SPRIET, https://www.law.kuleuven.be/jura/art/34n2/helsen.htm

Member State	State of play
	The Bulgarian law regulates exclusively, on the one hand, the property of "tangible objects", such as moveable properties and real estates and, on the other hand, the intellectual property, such as copyrights and related rights, trade marks, patents, etc. Both fields of law do not include data as such. As data are not tangible object, data cannot be owned as moveable property or real estate within the meaning of the Bulgarian Property Act („Закон за собствеността"). Bulgarian Property Act does not explicitly provide for a legal definition of movable property, but **the commonly accepted meaning of the used term „вещ/и" ('thing/s'/ or 'good/s') refers exclusively to 'tangible objects'**. Data as such are not protected by any of the existing intellectual property rights under Bulgarian law as well. Bulgarian Copyright and Related Rights Act („Закон за авторското право и сродните му права") in its Art. 4 'Exceptions' explicitly specifies that the data are not object to copyrights. Only in cases where the data meet specific additional conditions, one of these rights could become applicable (for example, if a collection of data fulfils the originality requirements). The intellectual property right that is closest to a protection of data is the sui generis legal protection of databases under Chapter 11A of the Bulgarian Copyright and Related Rights Act. However, it is again not the very data that are protected by this right by its specific collection, organization, structure, etc. With respect to the above, data as such cannot be owned under Bulgarian law, but the law provides for various legal instruments for its protection. These instruments, however, ensue not from an ownership, but are an expression or a part of another type of rights which are explicitly legally protected by the law. For example, personal data, as well as specific types of personal data as medical data are protected in the context of the right of inviolability of the personal life protected by the Constitution of Republic Bulgaria („Конституция на Република България") and more recently the right to protection of personal data under the EU Charter of Fundamental Rights; correspondence and traffic data are protected in the context of the constitutional right of inviolability of the correspondence and again as part the personal data protection right; trade and industrial secrets as information are considered expressions the commercial interests of a company and protected by the Commercial Act („Търговски закон"), the Protection of Competition Act („Закон за защита на конкуренцията") and other legal acts, etc.
Czech Republic	In order to determine whether data can be "owned" under Czech law, it is necessary to clarify the meaning of "ownership" and "data". There is no legal definition of "data" as such, however, in a general sense, by data we understand any information used to describe a certain phenomenon or attributes of an observed object. Pursuant to Czech law, **everything that is different from a person and serves the needs of people, is a thing (in a legal sense)**. A corporeal thing is a controllable part of the external world having the character of an independent object, whereas incorporeal things are either i) all rights which by their nature may be considered incorporeal, or ii) other things without corporeal substance (s. 489 and 496 of the Czech Civil Code (Act No. 89/2012 Coll., the Civil Code, hereinafter the "Civil Code"). It follows from the definition above, that **data are not a corporeal thing** (as opposed to the tangible object in which the data may be incorporated in), **but an incorporeal thing, if they fulfil the condition that they serve to the human needs**. Under s. 1011 of the Civil Code, „**everything that belongs to someone, all his corporeal and incorporeal things constitute the person's ownership**". A special form of the ownership rights are the exclusive proprietary intellectual property rights. **Data, as incorporeal things, may be subject to ownership** in the sense described above. According to legal jurisprudence, this applies in particular to the proprietary intellectual property rights, such as patent rights (s. 11 et seq. of Act No. 527/1990 Coll., the Patent Act), trademarks (s. 8 et seq. of Act No. 441/2003 Coll., on Trademarks), or rights to registered designs and utility models (s. 19 et seq. of the Patent Act). However, not all incorporeal things are subject to exclusive ownership rights within the meaning of s. 1012 of the Civil Code: "An owner has the right to freely dispose of his property within the limits of the legal order and exclude other persons from such disposal (..)". **Vast categories of incorporeal things (including some data) are not subject to ownership rights but they may be only subject to the right of possession** (i.e. a right which may be transferred to another by legal action and which permits permanent or repeated performance according to s. 988 (1) of the Civil Code). This concerns certain "residual" assets, to which the state (for various politi-

Member State	State of play
	co-economic reasons) does not grant exclusive proprietary rights. This applies for example to certain know-how, calculations, scientific knowledge, statistics, non-patented inventions, game rules, diagnostic methods, treatment/business/work procedures non-registered (trade) marks and labels, or other types of "mere" information. It is legally permissible that more than one person, independently on the others, possesses the same thing (such as the identical outcomes (i.e. the data) of several independent scientific researches) and thus it cannot be owned by any of them. This does not mean that such incorporeal things (such data) cannot be protected. The possessor has the right not to be disturbed in their possession by anyone and if someone infringes this right, the possessor may claim that the infringer refrain from such activity. Further, the possessor has the right to be protected against unfair competition.
Estonia	There is **no general data ownership regulation** under Estonian law. The topic has currently not been subject to case law or widely discussed in the legal literature either. The evaluation should be based on specific types of data which have been regulated with legal acts, e.g. personal data, databases, also genetic data. However, in general we consider that in the context of data, **ownership in rem is likely not applicable** and wider interpretation of ownership should be considered. Ownership (omand) under the Law of Property Act is full legal control by a person over a thing. "**Things" under civil law are physical objects** which can be objects of a right. Therefore, it could be argued that there is no ownership over data, since data is not physical and therefore not a thing. However, the General Part of the Civil Code Act prescribes that in the cases provided by law, provisions concerning things also apply to rights (i.e. non-physical objects). Such are, for example, pledge of rights. Rights relating to data can be attributed to a person, as it is the case, for example, for the legal protection of personal data, databases or the protection of trade secrets. Ownership is a collection of rights that belong to a certain person (e.g. right to possess, use and dispose of a thing). The rights of an owner may only be restricted by law or the rights of other persons. Ownership is created only in the cases provided by law. For example, with regards to data, Human Genes Research Act prescribes that the chief processor's right of ownership of a tissue sample, description of state of health, other personal data and genealogy is created from the moment the tissue sample or personal data is provided or the moment the state of health or genealogy is prepared. In some cases the law explicitly prescribes that certain data is not subject to transfer. For example, the tissue samples and uncoded information in the ownership of the chief processor and written consent of gene donors are not transferable. Upon termination of activity of the chief processor, the right of ownership of data will transfer to the Republic of Estonia. The clauses of the Human Genes Research Act referred to therefore confirm that data can be owned by a person and transferred to another person, but transfer of certain sensitive data may be restricted by law. Nevertheless, the Constitution of the Republic of Estonia uses the term "omand" in a different meaning ("property"). "Property" under civil law means a set of monetarily appraisable rights and obligations belonging to a person. According to the commentaries of the Constitution, the interpretation of the term "property" in the context of the Constitution is wider than the definition of "property" in civil law. There are at least 6 different interpretations of "property" in the Constitution: for example, property can mean physical objects belonging to a person, ownership as a real right, right of acquisition as a real right, economic rights related to the intellectual property, certain rights to claim under law of obligations, person's property as a whole and certain type of economic positions in public law. In the future **it is therefore not excluded that "property" can also refer to data, since the notion is evolving in practice and the list is not exhaustive**. According to the Constitution, property of every person is inviolable and equally protected. However, this is not an unlimited right, as the property may be taken from the owner without his or her consent, but only in limited occasions (e.g. the public interest, in the cases and pursuant to a procedure provided by law, and for fair and immediate compensation). Everyone has the right to freedom from interference in possessing or using his or her property or making dispositions regarding the same. Limitations of this right are provided by law. Therefore, if data is considered "property", the rights related to data would not be absolute. All in all, as legal literature and practice have **currently not resolved the matter**, there is no clarity as to how ownership in the context of data is or should be understood.
Germany	German law distinguishes between two categories of exclusive rights: property of things (Sacheigentum) according to § 903, S.1 of the German Civil Code (BGB) and so-called "intellectual proper-

Member State	State of play
	ty" (Geistige Eigentum), including patent, trademark, copyright law etc. (Immaterialgüterrecht). **None of these two categories is well fitted for data**. Property of goods only applies to tangible objects as defined by § 90 BGB that explicitly states: "Sachen im Sinne des Gesetzes sind **nur körperliche Gegenstände**". Since data aren't tangible objects, **the provisions of Book 3, Section 1 of the German Civil Code regulating "property" ("Eigentum") aren't applicable**. Data as such are by default not protected by one of the existing intellectual property rights either in Germany. Only if data meet specific additional conditions, could one of these rights become applicable. The intellectual property right which comes closest to a protection of mere data is the sui generis legal protection of databases under §§ 87 and following of the German Copyright Law (Urhebergesetz, UrhG). **Some German legal authors** have proposed to accept the concept of "data property" (Dateneigentum) by an **analogy to "property of things" (Sacheigentum)**[220]. This opinion is, however, **not shared by the majority** of German legal doctrine.
Finland	In Finland, data is **not per se treated as a subject of ownership**. The Finnish law does, however, provide various concepts and instruments to protect data, such as for example: -Objects of intellectual property rights, such as for example patents, utility models, designs, copyrights, databases and catalogues, are protected by different intellectual property laws. -Trade secrets gain protection in Finland under the Employment Contracts Act, the Unfair Business Practices Act and the Criminal Code. -The Criminal Code includes provisions on certain data and communications offences (Ch. 38), for example computer break-in regarding hacking into an information system (Ch. 38 Sec. 8), and identity theft regarding unlawful use of a third party's personal information, access codes or other corresponding identifying information (Ch. 38 Sec. 9(a)). -Personal data is protected by the Personal Data Act. -The Information Society Code, which came into force in 2015, includes (among other things) provisions on confidentiality of communications and protection of privacy (part VI). For example, whoever receives an electronic message (etc.) not intended for him/her shall not disclose or make use of the content of such a message, or the knowledge of its existence (Sec. 136).
France	Under French law **data (données informatiques) are considered as "goods" (des biens) for the application of the criminal code**. For example, Art. 314-1 of the Criminal Code sanctions breach of confidence, consisting in diverting "goods". In a case against an employee of a bank the Cour de Cassation decided that the term "**goods" can include not only movable goods but also data** (Cass. crim., 22 octobre 2014, pourvoi n°13-82.630). **Ownership** (propriété) as a legal concept established by article 544 of the French Civil Code **doesn't traditionally apply to data**. It applies to « things » (des choses) that can be the object of appropriation. Originally « a thing » exclusively referred to material – movable or immovable – items but this restrictive interpretation is undeniably evolving. The accent of « propriety » as a legal concept progressively shifts from « things » to « rights ». A farmer can, for example, be the owner of "milk quota" or a company can buy or sell "emission quota". Goods are more and more perceived and legally defined by the relationships triggered by these goods. This is accentuated by the fact that the term "goods" in the French Civil Code refers sometimes to the "things" themselves and, in other provisions, to the "rights related to these things" (Cours de Droit Civil, http://www.cours-de-droit.net/) . In the future it is therefore not excluded that the term "propriété" will also refer to data. The essential point is that the term "propriété" under French law refers to "the most complete right someone can have with regard to something". Therefore, **it is difficult to imagine how the concept could be applied to "data"**. Data are items of information, belonging to the public

[220] This opinion has, for example, be expressed by Thomas Hoeren, who estimates that the reasoning applied in German criminal law (where the simple fact of creating certain data can be qualified as a crime) should also apply to data; see http://www.uni-muenster.de/Jura.itm/hoeren/veroeffentlichungen/hoeren_veroeffentlichungen/Dateneigentum_MMR_2013_486-491.pdf

Member State	State of play
	domain. Rights relating to data can be attributed to a person, as it is the case, for example, for the legal protection of databases or the protection of trade secrets. However, these rights, even if combined, never can reach the stage of "propriety", at least according the laws of France. A new discussion related to "data ownership" has been conducted in the context of the proposed legislation on "the digital Republic" (la République numérique). The discussion was, however, restricted to personal data and the proposed owner of the personal data is the data subject. A provision proposed during the public consultation stated that health data, collected or produced by anyone or by any automated or other means, is, from its creation, the property of the person to which these data are applicable. For obvious reasons this provision didn't pass the filter of the scrutiny by the legal professionals and doesn't appear any longer in the final text adopted by the French government. (http://www.republique-numerique.fr/project/projet-de-loi-numerique/step/projet-de-loi-adopte-par-le-conseil-des-ministres)
Italy	Several authors in the Italian literature assessed data ownership issues, mainly as far as domain names are concerned. According to Cassano[221], property rights on domain names shall be excluded. To the contrary, according to Palazzolo[222], domain names can be owned, i.e. property rights apply to domain names, otherwise the contracts regarding the transfer of domain names would be void. Article 810 of the Civil Code applies ("**Goods are the things that can be the object of rights**"), and in this sense there is little doubt that this provision is **applicable to immaterial goods such as data** and information since they have a financial value and can be (and are) the object of agreements. One of the very few court decisions about this point has been issued by the court of Bologna[223] that pointed out that domain names are not property rights or credits and therefore they cannot be seized. Resta[224] said that ownership on immaterial goods, the so-called 'virtual property', implies that the immaterial goods such as domain names are part of the assets (in Italian 'patrimonio') of the owner. The same author highlights that **in the Italian legal literature appeared so far three different opinions** regarding the applicability of ownership rights to immaterial goods: • According to the traditional approach, ownership **does not apply to immaterial goods** (see Pugliatti, La proprietà nel nuovo diritto, Milano, 1964; Santoro Passarelli, Dottrine generali del diritto civile, Napoli, 1986). More recently, some contemporary authors made clear that, although there is a redefinition of the concept of copyright, due to the expansion of the use of licenses, and an extension of the ownership rights, there are little or no grounds to apply property law to both material goods, such as land, and immaterial goods, such as ideas and information[225]. • A **sui generis property right** is applicable to immaterial goods, provided that the owner has the exclusive right to use them [226]; • **Property right applies to immaterial goods**[227].
Latvia	**Data can be "owned" under the Latvian law**. According to the general principle of civil law embodied in Section 929 of Latvian Civil Code (CL), **the subject-matter of ownership may be anything that is not specifically withdrawn from general circulation by law**. Section 841 of CL states that things are tangible or intangible; intangible things consist of various personal rights, property rights and rights regarding obligations, insofar as such rights are constituent parts of property. Accordingly, intangible things are to be understood as rights. For example, intangible things are intellectual property, rights to undivided shares of a property, rights to claim. An owner of a thing is given a full exclusive right of control over the thing, insofar as this right is not subject to specific restrictions laid down by law.

[221] See Diritto dell'Internet. Il sistema di tutela della persona, Milano, 2005 and Monti, I veri problemi giuridici del nome a dominio, published on www.interlex.it

[222] Alcuni spunti in tema di regolamentazione di nomi a dominio: la pignorabilità, il potere di disposizione del titolare registrante e la disciplina pubblicistica, nota a T. Bologna, 22/3/2000, NGCC, 2002, 43

[223] Decision of 22/3/2000, available at http://www.interlex.it/testi/bo000320.htm

[224] Diritti esclusivi e nuovi beni immateriali, Torino, 2011

[225] See Gambaro, Dai beni immobili ai beni virtuali, http://www.treccani.it/enciclopedia/dai-beni-immobili-ai-beni-virtuali_(XXI-Secolo)

[226] See Greco, I diritti sui beni immateriali, Torino, 1948

[227] See Mattei, Qualche riflessione su struttura proprietaria e mercato, Riv. critica. dir. priv., 1997, 19

Member State	State of play
	Data can also in certain circumstances be regarded as intangible thing that belongs to a person as long as the law does not provide otherwise. For example, personal data of a natural person cannot be regarded as an intangible property because under the Latvian law it is a natural person who has rights over his personal data, even if the data has been transferred to another person. For example, the data subject may request to rectify or delete data in certain situations. This is contrary to the concept ownership of things. Data can also be a part of trade secrets that belong to a person. According to Section 19 of the Commercial Law of Latvia, the status of a commercial secrets may be assigned to things of economic, technical or scientific nature which satisfy all of the following characteristics: 1) they part of the undertaking of the merchant or is directly associated with it;2) they are not generally available to third parties; 3) they are of an actual or potential financial or non-financial value; 4) if disclosed to third parties, they may cause losses to the merchant; 5) in relation to which the merchant has taken reasonable measures to preserve secrecy. It is evident that in the information society data can qualify as trade secrets, as often being one of the main assets of a company. Under the Commercial law, the trade secret owner has exclusive rights to trade secrets. As discussed above, one cannot "own" intangible property but rather have exclusive rights over the data.
Lithuania	According to the Civil Code of the Republic of Lithuania the objects of ownership rights may be things and other property (Article 4.38), i.e. tangible and intangible. According to Article 1.97 of the Civil Code of the Republic of Lithuania objects of civil rights are things, money and securities, other property and property rights, results of intellectual activities, information, actions and results thereof, as well as any other tangible and intangible values. Although there is **no specific reference in the Civil Code to "data" as a category of an object of civil rights, the list of such objects is not exhaustive, so the data would qualify as an intangible asset and may be the object of civil rights (can be owned, used and transferred)**. Certain data (information) may also qualify as a commercial or industrial secret, which would have additional legal protection, specified in the Civil Code. The Civil Code of the Republic of Lithuania provides that the information is considered to be a commercial (industrial) secret if a real or potential commercial value thereof manifests itself in what is not known to third persons and cannot be freely accessible because of the reasonable efforts of the owner of such information, or of any other person entrusted with that information by the owner, to preserve its confidentiality. Information is also considered to be a professional secret if, according to the laws or upon an agreement, it must be safeguarded by persons of certain professions (advocators, doctors, auditors, etc.) (Article 1.116).
Luxembourg	As in most other Member States Luxembourg companies, particularly in the direct marketing sector, advertise for "sale of data" (vente de données; see, for example, http://lu.kompass.com/fr/l/general-conditions). A closer look at the terms and conditions ("conditions de vente") leads, however, to the conclusion that this terminology doesn't actually correspond to the content of the particular contract. According to these "sale of data" contracts, **the "owner" of the database provides a service to the other party**. The service consists in making a list of data available to the client, often for a definite period, which is called the duration of "the subscription". The client can download the relevant data from the server of the provider or the provider sends the relevant data to an electronic address of the client. Notwithstanding the fact that these contracts often explicitly mention that the data are "owned" by the provider, this so-called **"ownership" cannot be qualified as "propriety" in the sense of Art. 544 of the Luxembourg Civil Code**. This article defines "propriété" as « the right to benefit and to dispose of things, as long as one doesn't make a use of it that is forbidden by the laws or the regulations or one doesn't cause trouble that exceeds the normal inconvenience of a neighbourhood by breaching the balance between equivalent rights." The term "property" thus refers to a relationship between a person and "a thing" ("une chose"). The latter term is not explicitly defined in the Civil Code Originally it referred exclusively to physical – movable or immovable – things. Today it is generally accepted that it can also refer to non-physical objects, such as immaterial, fungible financial instruments. This is explicitly confirmed in the law of the 1st of August 2001 regarding the circulation of titles and other financial instruments. Financial instruments are no longer exchanged in the form of paper documents but the exchange is expressed by bookings on an account. This is called "dematerialisation" of financial instruments. The law of 1 August 2001 is applicable to "fungible" instruments. "Fungible" ("fungible" in French) means that one instrument can perfectly be

Member State	State of play
	substituted by another equivalent one. One of the innovations of the law of 1 August 2001, commented by legal authors in Luxembourg, has precisely been the inclusion of immaterial financial instruments in the legal category of "ius in re" (droits reels). **Part of the legal doctrine in Luxembourg estimates that the ownership of a fungible financial instrument should be qualified as "property" in the sense of Art. 544 of the Civil Code. This conclusion is, however, not followed by everyone**. In an opinion submitted during the parliamentary discussions on the draft of the law 1 August 2001, the Luxembourg Chamber of Commerce, for example, qualified the ownership of immaterial, fungible financial instruments more as a right "sui generis" (Avis de la Chambre de commerce du 11 janvier 2001 relatif au projet de la loi de 2001, Doc.parl. 4695, cited by Yves Prussen, Le régime des titres et instruments fongibles, available online at http://www.ehp.lu/uploads/media/Titresetinstrumentsfongibles.pdf). Authors, such as Prussen, estimate that, unlike a property right related to a physical object, the right of the owner of a financial instrument doesn't have an absolute resale right that can be exercised against everyone (ibidem, in particular, p. 1307). The discussion illustrates, nevertheless, that also in Luxembourg, the strict distinction of the 19th century Civil Code, between "rights in rem" (droits reels) and "claims" (droits de créance) becomes more and more under pressure.
The Netherlands	While the concept of ownership of data is commonly applied in IT contracts to any generated or collected data, the majority of doctrine holds that **ownership of data is not a legally valid concept**, as data cannot be regarded as an object that is subject to ownership under civil law in the sense of Article 5:1 of the Civil Code. As articulated by ENGELFRIET and RAS, "data should be regarded as a by-product of a service. It is therefore unwise to refer to 'owners' of data."[228] In the Netherlands, Book 5 of the Dutch Civil Code ("Burgerlijk Wetboek", or "BW"), states that property is the most comprehensive right that a person can assert on a thing ("Eigendom is het meest omvattende recht dat een persoon op een zaak kan hebben", art. 5:1 BW). Book 5 of the Dutch Civil Code distinguishes further between ownership of movable property (Title 2) and ownership of immovable property (Title 3). **It does not seem that data as such will be regulated by these titles**, as data as such is intangible (just bits and bytes), while movable and immovable property rights require tangible objects. Ownership rights offer the owner of tangible property protection against unlawful acts of others, while intellectual property rights protect intangible creations of the mind of the owner. In the Netherlands, several types of intellectual property rights are distinguished: such as copyright, trademark law, patent law,…. However, the Dutch Civil Code does not regulate these intellectual property rights. The expressions of ideas, or so-called intellectual property rights, are protected by separate laws in the Netherlands. For example, the "Copyright Law" ("Auteurswet"), the "Patents Act" ("Rijksoctrooiwet") and the "Database Act" ("Databankenwet"). The Dutch Civil Code, nor any separate Dutch law, provides for ownership rights on data as such. The majority of Dutch authors (http://degier-stam.nl/wp-content/uploads/2013/08/Juridische-aspecten-van-The-Internet-of-Things-Automatiseringsgids.pdf M. HEINTGES, J. KUHLMANN, A. ENGELFRIET) stated that **there exists no ownership of data**. For example, a manufacturer of a personal weighing scale cannot claim that he owns the weight data produced by the scale. Nevertheless, the manufacturer can invest in the composition of a database which contains weight data (which may also trigger some privacy issues). This database, and not the data as such, will probably be protected under the Database Act ("Databankenwet"), which is the Dutch transposition of the European Database Directive . Data that are not included in a protected database can be used freely, because nobody "owns" it. Another example, as explained by a Dutch ICT author (http://blog.iusmentis.com/2012/09/19/ik-wil-mijn-data-van-mijn-leverancier/): **the fact that there exists no ownership on data as such would mean that the client cannot oblige the software provider to convert "his" data in a format that is understandable to him** (the client). Dutch lawyer F. MULDERS reiterated, in the context of cloud service providers, that data is not a tangible object. Thus there can be no ownership of data as such. However, one could have the right to use certain data, or some data may be protected by intellectual property legislation, as data is a creation of the mind (http://lexx-it.nl/lexxit-knowledge/internet-risk-management/eigendom-van-

[228] ENGELFRIET, S. RAS, *Handboek ICT-contracten*, Utrecht, Ius Mentis, 2015, 24; see in the same sense DOERGA, https://www.fme.nl/nl/nieuws/wie-eigenlijk-eigenaar-big-data

Member State	State of play
	data-de-cloud/). Consequently, in the hypothesis of a cloud service provider or hosting provider that went bankrupt, the author stated that the curator cannot sell the data as such. However, he could sell the hard disk that contains the data. In addition to that, the curator is not under an obligation to give "your" data to you. Another Dutch lawyer (R. DORGA) reminds that speaking about "ownership of data" is wrong, as it is not explicitly included in the Dutch Civil Code (https://www.fme.nl/nl/nieuws/wie-eigenlijk-eigenaar-big-data). **It is technically better to speak about a right to data ("recht op data") or control over data ("zeggenschap over data").** A criminal case from the Court of Arnhem[229] provides further support for this position, since the Court explicitly held that "the taking away of computer data does not qualify as the taking away of 'any goods' in the sense of Article 350 of the Criminal Code. **A 'good' as intended by the aforementioned provision must have the fundamental quality that the one who has factual power over it loses this if another person assumes such factual power. Computer data lack this quality.**" As a generic principle, this seems valid.
Poland	Under Polish law ownership is **restricted to tangible objects**. According to Art. 140 Polish Civil Code (the provision determining the scope of ownership) "within the limits set by the law and the principles of community life, an owner may, to the exclusion of other persons, use a thing in accordance with the social and economic purpose of his right, and may, in particular, collect the profits and other revenues from the said thing. Within the same limits, he may dispose of the thing", while, pursuant to Art. 45 of the Polish Civil Code "within the meaning of this Code, **things are material objects only**" (emphasis added). As Polish law very explicitly restricts ownership to material objects only, rights of the data originator (or creator) akin to ownership rights (e.g. the right to dispose of the data, use them etc.) are first and foremost determined by legal acts in more specific fields of law. As long, however, as the specific legal acts do not preclude certain prerogatives of the data originator (or creator), he/she will be entitled to make use of the data, make it available to others, or dispose of them according to the general principle of **freedom of contract** (Art. 3531 Civil Code: "Parties executing a contract may arrange their legal relationship at their discretion so long as the content or purpose of the contract is not contrary to the nature of the relationship, the law or the principles of community life").
Romania	There is **no specific provision** under Romanian law referring to the ownership right over the data. The ownership right (*drept de proprietate*) is a legal concept established by Art. 555 of the Romanian Civil Code, which consists of the right to hold, use and dispose of a good in an exclusive, absolute and perpetual manner, according to the limitations determined by law. According to Art. 535 of the Romanian Civil Code, a "good" is considered an asset, tangible or not, which is subject to a patrimonial right. The doctrine notes that the concept of **"good" includes the non-tangible assets**, which do not have a physical existence, being creations of the human mind (for example intellectual property rights, copyrights). However, not all assets are considered goods, just only those which can be valued in money, and therefore can be the subject of a patrimonial right. **The doctrine did not discuss data, in general, as being the object of an ownership right**. Given the lack of (i) specific legal provisions acknowledging that the data are subject to the ownership right, and of (ii) opinions on this issue from the doctrine, **it is difficult to ascertain whether, under the Romanian law, data can be subject to the ownership right.** One of the prerogatives of the ownership right is the right to dispose of the goods. However, for examples in case of personal data, an alleged ownership over the personal data cannot be transferred as the data subjects will continue to keep the said personal data (only a right to use the said data can be transferred). Therefore, **it is difficult to imagine how the concept of ownership could be applied to "data"** (which represents pieces of information). Rights relating to data can be attributed to a person, for example in case of legal protection of copyrights, trade secrets or legal protection of databases. However, as shown above, although certain rights are granted by law, for example in relation to databases, the law does not refer to an ownership right over the database.

[229] See http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHARN:2011:BQ9209

Member State	State of play
Slovenia	In general, the Slovene law distinguishes between two categories of exclusive ownership rights: property rights on things ("lastninska pravica") according to Section IV of the Slovene Law on Property Code (Official Gazette of the Republic of Slovenia no. 87/02, as amended, hereafter "LPC") and intellectual property rights ("pravice intelektualne lastnine") which include (a) copyright and related rights pursuant to the Copyright and Related Rights Act (Official Gazette of the Republic of Slovenia no. 21/95, as amended, hereafter "CRRA") and (b) industrial property rights such as patents, trademarks, models, special security certificates and geographical indications as provided by the Industrial Property Act (Official Gazette of the Republic of Slovenia no. 45/01, as amended, hereafter "IPA"). With respect to both categories of ownership rights, we may observe, that they are **not suitable for establishing ownership of data**. Pursuant to Article 15, LPC property rights on things relate only to tangible objects that can be controlled by humans. Since data cannot be defined as a "tangible object" the cited provision is not applicable. A similar observation can be made also with respect to defining data as a specific form of intellectual property. Although data may be regarded as intellectual property if they meet specific [additional] conditions, as defined by the CRRA and IPA, **"data" as such are not subject of any specific ownership right**. The most similar concept to property rights on data as such (without any additional substantive conditions) can be identified within the concept of the rights of database creators pursuant to Chapter 5, Section 6 of the CRRA, which is described in legal theory as an exclusive right similar to copyright. However, as the legal protection of databases relates to a larger collection of data – the database – we may observe that only the collection but not the individual data is subject to exclusive ownership rights. In this respect we note that also the Slovene Personal Data Protection Act Official Gazette of the Republic of Slovenia no. 86/04, as amended, hereafter "PDPA") does not implement any data ownership provisions. The problem of "data ownership" is not discussed in the available Slovene legal theory, however **the available case-law on personal data protection** (e.g. Administrative Court of the RS ref. no. I U 317/2012, I U 897/2012, IV U 85/2010, and other) **implicitly suggest that the courts accepted the concept of "data property" at least with respect to personal data**. In the rulings cited above the courts on various occasions referred to personal data as "own data" thus implicitly indicating that there is also an owner of such data and consequently there should also be data ownership, which is not conditioned with any other criterion and is in fact very similar to the ownership of things. It is therefore quite likely that the courts could use the same analogy also with respect to other [non-personal] data and that effectively the controller of any data would be regarded as their legitimate owner. On the other side a possible application of an intellectual property right for data seems rather impossible under Slovene law. As any intellectual property right is conditioned with meeting specific criteria provided by law "data as such" cannot be qualified as any exclusive intellectual property right (with the exception of database creator rights, where however the collection and not the data is the factual object of protection). In the context of data ownership data also subject to legal protection and whereby the "owner" of data may defend himself against unlawful use of data by third parties, however, again the available case law is limited to personal data protection issues. It is very likely that due to the relatively small Slovene market several data ownership issues did not arose and are thus not discussed by available case-law and legal theory.
Sweden	There is **no clear right to data** according to Swedish property law. While intangible things are generally considered personal property, the only specific property right granted by law concerns intellectual property rights. In other words, **the law does not stipulate a specific property for data as such**. For copyright protection, as in other countries, a certain level of human creativity is required according to the Swedish Copyright Act (lag (1960:729) om upphovsrätt till litterära och konstnärliga verk), which therefore does not apply to data that is generated automatically in a computer system. Another possibility according to the Copyright Act would be the sui generis protection of databases (corresponding to the EU Database Directive 1996/9/EC). In such cases, the question arises of whether a substantial investment has been made, which might not be the case if the data is generated as a by-product of a computer system or cloud service.

Member State	State of play
	Another potential protection for data originates in the Swedish Trade Secrets Act (lag (1990:409) om skydd för företagshemligheter). Here the challenge is to keep the data secret even within an organisation in order to be awarded legal protection. The last possible statutory protection is the Swedish Personal Data Act (personuppgiftslag (1998:204)) which implemented the EU Data Protection Directive 1995/46/EC, and which through various provisions grants an individual the right to her or his personal data. A common recommendation in Sweden - especially with regards to cloud services - is to include a clause in the contract on the right to data. One of the main standard contracts for cloud services used in Sweden published by IT & Telekomföretagen stipulates in Section 15 the Rights to Customer's Data and entitles the client to all rights to her or his data. In Section 1.1 the customer's data is defined as data or other information that the customer "makes available to the supplier and the result of the supplier's processing of data." Log files are specifically regulated in Section 15.2, which restricts the supplier's access to what is necessary in order to perform the service.
United Kingdom	Under the law of the UK **data or information cannot be "owned"**. Even in the statutory systems of patent and copyright there is no real ownership of information. Instead there are limited monopoly rights over the reproduction and exploitation of certain forms in which information is expressed. The legal protection of databases, implementing the European directive on this subject, is the closest UK law comes to establishing some right of "ownership" of data. In English **criminal law** the rule is even more straightforward: **information cannot be stolen**. This rule did emerge in the 1978 case of Oxford vs Moss ([1978] 68 Cr App R 18). Moss was an engineering student who acquired a copy of the examination questions before the examination. He was charged but acquitted. It was agreed that he did not intend to deprive the university of the paper, and the question was whether the information was property which could be stolen. The answer was that it was not property, and an appeal by the prosecutor was dismissed. However, beyond the strict legal rights available, the importance of physical possession and control of the data cannot be overstated. If valuable data has been obtained, can be kept secure and cannot easily be obtained by others, then the value of the data can often be exploited without the need to rely on any legal rights relating to that data. Even when the existence of legal rights is necessary to exercise full control, the practical steps taken to secure the data will usually be of utmost importance in maintaining "ownership" in practice.

M2M contracting

Member State	State of play
Austria	The basic principle for entering into contract under Austrian law is that a consenting declaration of intent (Willenserklärungen) must be given by the contractual parties. In this context, it is clear that such **declaration has to be given by an individual** (be it on the individual's own behalf or on behalf of another individual or entity, provided that the declaring individual is duly authorized to represent such other individual or entity). However, it is also clear that such declarations of intent **can be given by electronic means** (see, e.g., Koziol – Welser/Kletečka, Bürgerliches Recht I14 (2014), mn 315 et sequ; Koziol – Welser, Bürgerliches Recht I11 (2000), p. 12-13 and p. 370 in the distant selling context; § 3 fig 2 of the Austrian Distant Selling Act, Fern- und Auswärtsgeschäfte-Gesetz, "FAGG"). With a view to Machine-2-Machine ("M2M") contracts, the general question therefore is whether a declaration of intent or other decision expressed by a computer and/or any other smart/IoT product can be associated to the user. **If the user has at least determined the underlying conditions for a decision or declaration made by a computer/smart product/IoT product, the user will be directly** responsible for the actions taken by the computer/smart product/IoT product in the vast majority of the current use cases. As in Germany, the use of software agents may certainly also be regulated by the prior conclusion of a framework contract between the parties under Austrian law, tying specific legal consequences to declarations made by a software agent. In light of the freedom of contract, parties can always agree on such a procedure. Whether and to what extent the above also may apply to self-learning artificial intelligences, e.g.

Member State	State of play
	software/firmware which is capable of learning and rewriting its own code based upon its learnings, however, entirely is uncharted territory in Austria. A prominent recent example for a software going haywire is Microsoft's chat-bot "Tay" which began tweeting racist comments due to third-party inputs (see, e.g., http://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist and http://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160).
Belgium	There is in principle **no barrier to the use of M2M contracting**, given the principles of freedom of contracting, consensualism (allowing parties to use any valid means to express their intent), and autonomy of will. Parties are furthermore free to conclude agreements on how they shall express their will and express their consent, including through digital means such as M2M agents; this is commonly done in M2M contexts, where participants in e.g. a trading platform first agree to the terms under which a software routine shall be able to create binding obligations on their behalf. In that sense, the 'machine' in M2M transactions is an automated form of communication between parties. This implies also that the **behaviour of a machine in M2M contracts must always be ascribed to a person** (human or legal entity), since a contract can only be formed between persons. If this is not the case, no contract exists, and any legal disputes fall within the area of extra-contractual liability or product liability. Complexities may in particular arise when a software agent acts outside the boundaries of the user's intended behaviour (e.g. a software agent is allowed to bid up to amount X, but bids a higher amount). This is a very factual question, and would need to be assessed on a case by cases basis; no particular legislation or case law exists on this topic. Presumably the seller (who faces a claim for the excessive bid amount) would need to demonstrate that the software agent malfunctioned, and that the fault and liability therefore lie with the provider of the software agent.
Bulgaria	**Contract** within the meaning of the Bulgarian Obligations and Contracts Act („Закон за задълженията и договорите") **is an agreement between "persons"**. The systematic interpretation of the current Bulgarian legislation and specifically of the Bulgarian Persons and Family Act („Закон за лицата и семейството") shows that as a "person" capable to perform legally valid actions and respectively, to conclude contracts are recognized **the "natural persons" and "legal entities"** where the "legal entities" can do so only though their representative bodies. In certain cases Bulgarian law provides limited legal capability for some non-personified organizations and structures, but again such **legal capability can be exercised only though their representatives/ representative bodies or their members**. At the end, for the recognition of a legally valid will and for the performance of a valid legal statement, the involvement of a legally capable natural person is always required (on his/her own behalf, on behalf of another natural person, on behalf of a legal entity or on behalf of a group of natural persons and/or legal entities). **The autonomous software agents and robots on their own are not persons and cannot be recognized as independent legally capable subjects under Bulgarian law**. However, under Art. 15, Para 1, item of Bulgarian Electronic Document and Electronic Signature Act („Закон за електронния документ и електронния подпис") the person indicated as a titular or author of an electronic statement cannot challenge the authorship of the statement toward the addressee, if the statement is signed with an electronic signature when the statement is sent through an information system designated to function in automated regime. Based on this presumption established by law the person indicated as titular of the electronic signature would be engaged with the legal consequences of electronic statements which are signed automatically with this electronic signature. The above presumption does not apply in case the addressee did not take the due care. Taking into account the above legal provision, **it is possible a valid contract to be concluded completely automatically by means of two information systems which function in an automated regime**. Of course, **the legal effects from such a contract would arise for the respective titulars** of the used electronic signatures, **not for the machines**. The quoted presumption is based on the concept that for such an electronic signing in automated regime the data for the creation of the signature should be accessible for the information system which is designated to function in automated regime and only the titular and/or the author of the electronic signature can make these data accessible for the respective automated information system. Thus, the electronic statements sent by the information system are considered to be electronic statements of the titular of the electronic signature used for their signing. As a result of this presumption, the risk from malfunc-

Member State	State of play
	tion of the automated information system, including from potential deviation of the automatically signed and sent statements by the automated information system from the titular's actual will, is for the titular, since it is supposed that the system should be under the titular's control.
Czech Republic	In general, **contracts may be concluded only between persons, therefore it is not possible to conclude machine-to-machine (hereinafter "M2M") contracts**. Pursuant to s. 1724 (1) of the Civil Code, by a contract, parties express their will to create a mutual obligation between them and adhere to the contents of the contract. According to s. 17 of the Civil Code, "**only persons may have and exercise their rights**. Duties may only be imposed upon and their performance enforced in relation to persons. If anyone creates a right or imposes a duty upon something other than a person, such a right or duty is attributed to the person to whom it belongs according to the legal nature of the case" (s. 17 of the Civil Code). There are either natural or legal persons under Czech law (s. 18 of the Civil Code). With respect to the explanation above, it can be inferred, that **every contractual arrangement must eventually be attributed to a certain individual or legal person**. Under applicable legislation, machines do not have a legal personality, and unless their actions may be attributed to a certain person, their actions cannot have legal consequences. On the other hand, it is not difficult to imagine circumstances under which a M2M "contractual" system is **based on a prior contractual arrangement** between the legal persons tying the M2M actions to these legal persons. Under such scenario, the M2M actions would de facto constitute a contract, even though the rights and obligations under the contract could not be attributable to the machines. An example of this is M2M securities trading and other types of exchanges allowing for automated trading.
Estonia	Under Estonian law it is implied that contracts can be concluded by software agents or robots. Even though there is **no explicit regulation or specific case law** on the matter and the topic has not been widely discussed in the legal literature, **in practice M2M solutions are used for the conclusion of agreements**. These contracts are **binding for the natural or legal person who makes use of the autonomous agen**t in accordance to a prior agreement which recognises and regulates the "acts" of the autonomous agent. The software agent is deemed to act on behalf and in the name of the natural of legal person in this case. Under General Part of the Civil Code Act, a declaration of intention may be expressed in any manner (i.e. directly, indirectly, with silence and inactivity if so prescribed by law, an agreement between the parties or the practices established between them), unless otherwise prescribed by law. In practice, the parties have usually concluded a framework agreement under which they agree that contracts or orders can be concluded as a result of M2M transaction (i.e. that the declaration of intention can be expressed this way). The agreement concluded is considered to be in a format enabling written reproduction. Transaction in a format enabling written reproduction must contain the names of the persons entering into the transaction, but need not contain hand-written signatures. However, this format cannot be applied for transactions have a stricter format requirement prescribed by law (e.g. notarial format or written format).
Germany	German legal literature has dealt regularly with the legal status of contracts concluded by autonomous software agents or by robots (see e.g. Cornelius, Vertragsabschluss durch autonome elektronische Agenten, Multimedia und Recht 2002, 353). The legal discussion essentially relates to the question whether a decision or declaration expressed by a computer, can be associated to the user. **Many argue that since the user at least determined the underlying conditions for a decision or declaration made by a computer, the user is directly responsible for the actions taken by the computer**. The use of software agents may of course also be regulated by the prior conclusion of a framework contract between the parties, tying specific legal consequences to declarations made by a software agent. Due to the freedom of contract parties can always agree on such a procedure. **Some authors have expressed concerns about the fact that a software agent could be capable of changing the framework conditions by itself**. Any accountability for declarations made by such adaptive software would be an unpredictable risk. A suggested solution is to associate the declaration as one of the software agent itself and apply the rules relating to representatives. This solution is, however, criticised since software agents or robots are no legal entities capable of performing legal acts by themselves.
Finland	There is no specific guidance on this issue. We assume, however, that **if the machine is acting on behalf of a natural person or a legal person, then the rule of thumb likely is that the contract can**

Member State	State of play
	be binding on the natural persons/legal persons in question. There may be a number of situations or types of contracts regarding which the aforementioned rule of thumb is not applicable though. We also mention that the Finnish Information Society Code recognises electronic contracts.[230]
France	Under French law **it is evident that contract can be concluded by software agents or by robots**. Legal literature refers for instance to the stock market where large numbers of transactions are make via trading robots. These contracts are **binding for the natural or legal person who makes use of the autonomous agent** in accordance to a prior interchange agreement which recognizes and regulates the "acts" of the autonomous agent. **The agent is deemed to act on behalf and in the name of the natural of legal person**. For example, block chain protocols allow the formation of smart, autonomous contracts, concluded without human intervention, which can be triggered under certain conditions. Likewise, platforms such as Ethereum (http://www.ethereum.org), allow building smart contracts intended to manage decentralised exchanges.
Italy	TBA
Latvia	The law does not address explicitly the issue on machine-to-machine contracts. However, since the matter concerns private law, **the principle that everything is allowed unless prohibited should be taken into account**. This corresponds also with the **principle of party autonomy** according to which **parties may agree on means (e.g. autonomous software agents) how to enter into agreements**. According to Section 1511 of CL, a contract is a mutual expression of intent made by two or more persons based on an agreement, with the purpose of establishing obligations. Thus, it is clear that **legally it is a natural or a legal person that concludes the contract irrespective of a method or technical means that are employed to reach an agreement**. Therefore, the answer is that machine-to-machine contracts can be concluded as long as one can determine who are the persons possessing the machines and whether one can establish the intent of these persons to conclude the transaction in question and bind themselves. If intention to bind by natural or legal persons can be established, a contract can be concluded by any technical means. According to Section 391 of the Commercial Law**, in interpreting the intent expressed by a merchant, the practices existing in the scope of commercial rights in the relevant sector shall be taken into account in the mutual legal relations of merchants**. This means that interpretation of the parties' intent (expressed by autonomous software agents) **depends on development of a relevant business sector**. For example, in a financial sector there are certain transactions that are exclusively concluded by autonomous software agents.
Lithuania	One of the main principles of the Lithuanian civil law is the principle of **freedom of contracts**. Machine to machine contracts are not specifically regulated by the law, however there is **no restriction to conclude such kind of the contracts**. According Article 6.162 of the Civil Code of the Republic of Lithuania which says that a contract is concluded either by the proposal (offer) and the assent (acceptance) or by any other actions of the parties that are sufficient to show their agreement, it is possible to conclude the machine to machine contract. In order to determine if the contract was concluded it is necessary to establish the party's consent to the terms of contract, which can be expressed clearly or implied from the behaviour of the party (Article 1.64 of the Civil Code of the Republic of Lithuania). Machine to machine contracts have to comply with the requirements of the law. Article 6.159 of the Civil Code of the Republic of Lithuania provides the mandatory elements of the contract. The following elements shall be sufficient to render a contract valid: an agreement of legally capable

[230] If a contract must be concluded in writing according to the law, this requirement is also met by an electronic contract with contents that cannot be unilaterally altered, and which remain accessible to the parties. If a contract must be signed according to the law, the separate provisions on electronic signatures shall be applied. The provisions of this subsection shall correspondingly apply to notifications and other measures by the parties relating to the contractual relation which according to the law must be in writing or signed. If a notification relating to a contract must be supplied verifiably according to the law, this requirement may also be met by such an electronic method with which it can be demonstrated that the recipient has received the notification. The provisions of subsections 1 and 2 [i.e. provisions above] shall not apply to a contract concerning a property deal or any other transfer of a property or a contract relating to family or estate law. (Sec. 181)

Member State	State of play
	parties, and, when prescribed by laws, also a form of a contract. Where the transaction is made by employing telecommunication terminal equipment, **in all cases there must be sufficient data for the ascertainment of the parties to the transaction** (Article 1.76. of the Civil Code of the Republic of Lithuania).
Luxembourg	According to the law of Luxembourg a contract is "an agreement through which one or more persons commit themselves vis-à-vis one or more other persons, to give, to do or not to do something" (Art. 1101 Civil Code). Consequently, **a contract can only be concluded by "persons"**. A person can be a physical or a legal person. Legal personality can only be attributed to an entity by law ("legalism" principle). The legislator can attribute legal personality directly and explicitly to an entity or a grouping or enact that the attribution of legal personality will depend on certain conditions to be fulfilled. A legal person can, for example, be created by an agreement between physical persons about the establishment of a commercial company. Until today, the Luxembourg legislator had not yet attributed the status of legal person to robots or other machines or devices. As in other Member States **this doesn't exclude that all kinds of machines and devices can play a role in the execution of contracts**. The typical example is the vending machine. From a legal point of view, at least in Luxembourg, when a person buys a drink from a vending machine, **this person doesn't contract with a machine but with the person who exploits the machine**.
The Netherlands	In the Netherlands, a contract is defined as a multilateral juridical act, formed by offer and acceptance. The contract is formed when the acceptance of the offer reaches the recipient (or on the moment the recipient can be expected (by the sender) to read the message). According to the Dutch Civil Code, **it is determined whether a contract is formed using the doctrine of will and reliance**. Regarding automated systems (or machines), defined as a system that performs acts without human intervention, with preconditions set by a human person, the question arises whether the acts of the system can be grounded on the will of a person (M.B. VOULON, Automatisch contracteren, Leiden, University Press, 2010, 360 p). The Dutch author argued that **the theory of the programmed will and the theory of the general will can be used**. According to the programmed will, **the acts of the system can be regarded as juridical acts of its user, because the acts of the system are based on a pre-existing will of the user**. The theory of the programmed will is **not well suited for automated systems with a high degree of complexity** (such as an EDI-system) **and unpredictability**. Due to that complexity, the user can sometimes not predict the functioning of the automated system. So it would not be excluded that the automated system includes a number of instructions of which the user has no knowledge. The problem associated with automated systems with a high degree of complexity, could be solved by the theory of the general will. In contrast to the theory of the programmed will, the theory of the general will function as follows: **the acts of the system are based on the general will that is aimed at the legal effects of the acts of the system**. However, there can still occur unforeseen situations. This are situations in which the automated system works exactly as expected, but there are certain circumstances on which the user did not anticipate. An example is "program trading". The automated system sells your share when the value of the share drops under a certain value (as anticipated by you). In that case, the unforeseen situation is that the value of all the shares will drop more and more, so finally everyone will sell his shares. Another possibility is the prior **conclusion of a framework agreement** (and the use of software agents), which may be a more practical solution. The traditional example is an EDI-system. More concrete, the interchange agreement can function as framework agreement for the subsequent agreements concluded by the EDI-system, for example by stating that the parties express their mutual intention that contracts formed by EDI will be legally binding upon them.
Poland	As machines have no legal capacity (they cannot be subjects of rights or obligations), **M2M is a shorthand for contracts between those who have the legal capacity (individuals or companies) and use the machines to exercise it**. Polish law is clear that, as a principle, it is entirely possible to use machines for this purpose, due to the freedom of form of the declaration of intent (pursuant to Art. 60 Polish Civil Code "**Subject to the exceptions provided for in the law, the intention of a person performing a legal act may be expressed by any behavior of that person which manifests his intention sufficiently, including the intent being expressed in electronic form**)".

Member State	State of play
	Hence a legal entity can use machines to declare his/her intent, as long at least as it allows for expressing his/her intent sufficiently clear. This has direct implications for contracts, as a contract comprises at least two mutually congruent declarations of intent.
Romania	Under the Romanian law, it is not possible to validly conclude contracts using software agents or robots. This is because **the exchange of consent cannot be expressed by a computer, therefore the condition of validity of the contract provided by the Civil Code is not fulfilled**. The Romanian doctrine has not tackled this issue yet. Thus, the doctrine did not try to adjust the general contract principles in order to validate the use of the electronic agents. Currently, the matter of using smart or intelligent, autonomous contracts, concluded without human intervention is a collateral topic of discussion with regard to the use of the crypto currency.
Slovenia	Although several legal aspects of electronic commerce in Slovene were discussed by various commentators, especially from the year 2000 onward, there are **no indications in the available case law and legal theory in Slovenia that the legal status of contracts concluded by autonomous software agents or by robots was discussed in more detail.** Commentators on general concepts of e-commerce (e.g. Sladič, Jorg, Electronic commerce and electronic signature under European and Slovene Law, Podjetje in delo no. 6-7, GV Založba 2010) suggested that formal requirements of contract conclusion and validity can be sufficiently resolved by the legal concepts of non-discrimination or even equality of the electronic form and by regulating electronic signature as being equal (under certain conditions) with a physical signature, however, especially questions of the validity of the declaration of will may sometimes be problematic in electronic commerce, as it is questionable whether the declaration of will was really made by the lawful representative of a given legal entity (natural or legal person). If this is not the case, this could lead to invalidity of the contract. The latter is even more evident in case of M2M contracts where it is certain that the very declaration of will, leading to contract conclusion was not made by the lawful representative it is therefore questionable whether a declaration expressed by a computer, can be associated to the user as its valid declaration of will. **In order to avoid issues on the validity of M2M agreements the use of automated contract generation schemes should be regulated by the prior conclusion of a framework contract** between the parties, tying specific legal consequences to declarations made by a software agent to a valid expression of will made by the lawful representative of the entity controlling the automated agent.
Sweden	The Swedish Contracts Act (lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område, cit. avtalslag) does not generally require a specific form for a contract to be valid and applies irrespective of the means of transmission. Offers and acceptances communicated via digital technology, such as through email or chat messages, therefore constitute valid contracts. As there are no obstacles for concluding contracts via digital technology, machine-to-machine (M2M) contracts are possible. Sweden has previously made use of EDI (Electronic Data Interchange) technology to conclude contracts. **However, it is assumed that M2M contracts, at least initially, are approved by the contracting parties**. It is unclear to what extent Section 32 Contracts Act dealing with mistakes concerning the content of the contract (förklaringsmisstag) applies to technical errors in a digital system that lead to unexpected or unwanted orders. **Errors as a result of autonomous agents would therefore need to be dealt with on an individual basis**, taking into account the specific circumstances of the case.
United Kingdom	In the UK a legally enforceable contract requires, inter alia, intention to create legal relations and, if the contract is not entered into directly by a party, authority to act on the party's behalf. **Where electronic means and automated devices are used as tools that merely facilitate the conclusion of a contract in accordance with strictly pre-determined requirements established by the parties, there is no doubt that a binding agreement may be formed.** If an autonomous device or agent is able to conclude contract **beyond strictly determined tasks** set out by the parties, **it is unclear whether the requirements to form a legally binding contract will be present**. In this case the device or agent would not be considered as merely a tool to communicate the parties' intentions, but autonomous systems that can take decisions based on the processing of environment parameters without interference from the parties. Since the parties may be unaware of the conclusion and/or the content of the contract, **it is unclear whether the intention to create legal relations will always be present**. At present the current legal framework in the UK does not appropriately address this kind of scenario.

Liability of IoT, robots and autonomous systems

Member State	State of play
Austria	According to § 859 ABGB, Austrian law mainly distinguishes between contractual (vertragliche Haftung) liability, liability in tort (deliktische Haftung) and legal liability (gesetzliche Haftung). The cases of liability in tort and legal liability, however, are regularly seen as one group. Hence, the main two groups are contractual liability and legal liability (see, e.g., Koziol – Welser, Bürgerliches Recht I11 (2000), p. 11). Contractual liability arises from a breach of contract. Legal liability arises from a breach of a statutory provision aimed at preventing damages from arising ("Schutzgesetze", see § 1311 ABGB). Furthermore, any liability also requires the element of causality between the breach and the damage. Moreover, there has to be a certain degree of predictability between the breach and the damage resulting from the breach. The Austrian law further distinguishes between fault-based liability (Verschuldenshaftung) and strict liability (Gefährdungshaftung). The default regime is fault-based liability where negligence or wilful intent is required for founding liability. An individual or entity acts negligently when it fails to exercise the reasonable care (see § 1294 ABGB). The exception to this default regime is the strict liability which does not require any fault such as negligence on the damaging party for triggering its liability. Strict liability is usually stipulated in specific statutory provisions or specific statutory acts. The prime examples for strict liabilities are the Austrian Railroad and Motor Vehicle Liability Act (Eisenbahn- und Kraftfahrzeughaftpflichtgesetz, "EKHG") and the Austrian Product Liability Act (Produkthaftungsgesetz, "PHG"). The rationale behind the EKHG is that operating a train or a motor vehicle per se is a "dangerous" activity. Hence, the EKHG stipulates strict liabilities for the owners of trains and/or motor vehicles who therefore are liable for damages arising out of any accidents irrespective of any fault on their side ("Halterhaftung"). There is no specific provision in the EKHG on self-driving cars, but there is an generic provision on motor vehicles (§ 6 EKHG) stating that if, at the time of the accident, someone used the motor vehicle without the will of the owner, he shall be liable for the replacement of the damage instead of the owner. A user is considered to be "any person who assumes the use of the motor vehicle as such with domination." While this is of course only intended for the more trivial case where a person lends out their car to another person, as such it could apply to autonomous cars, although there is no jurisprudence on that point yet. The rationale behind the PHG is that placing a product onto the market already per se gives rise to risks for which the product's manufacturer (and also its Austrian importer(s)) should be liable. A prominent recent example for such strict product liability would be the Samsung Galaxy Note 7 mobile phones, which are prone to spontaneously burst into flames because of faulty batteries (see, e.g., https://www.cnet.com/news/why-is-samsung-galaxy-note-7-exploding-overheating/). The PHG was adopted into Austrian law in light of the European Product Liability Directive. **With regard to autonomous driving cars, the EKHG applies without any further ado** (see, e.g., Messner, Industrie 4.0: Hoffnungsträger künstliche Intelligenz – Haftungsfragen ungeklärt, chemiereport 5/2015 = http://www.chemiereport.at/sites/default/files/uploads/printausgaben/web_chemiereport_5_15.pdf). Whilst the PHG and thus the manufacturer's/importer's **strict liability basically also applies to autonomous driving cars and all other autonomous objects such as IoT products and robots, the PHG also provides for an exception of its strict liability. Namely, the PHG's strict liability particularly is explicitly excluded if the manufacturer can show that "the characteristics of the product could not be qualified as a defect according to the state of the art and the state of the science existing in the point in time when the product was placed onto the market" (§ 8 fig 2 PHG)**. Hence, the applicability of the PHG basically must be assessed on **a case-by-case basis, especially with a view to any self-learning artificial intelligences** described above with regard to M2M contracts. In this artificial intelligence context, a detailed assessment of the basic programming of such artificial intelligence most likely will be crucial. Therefore, **some Austrian legal commentators believe that the current legal regulations are not entirely sufficient to provide satisfying legal certainty with regard to artificial intelligences** so that new specific laws are required (see, e.g., Messner, ibid).
Belgium	Liability for the use of autonomous device or agents is **not regulated separately** in Belgium. There-

Member State	State of play
	fore, generic liability provisions would have to be applied. As with most Napoleontic regimes, the Belgian Civil Code has extra-contractual liability rules that hold any person liable for damages that they have caused through their actions (Article 1382) or their inactions or carelessness (1383). More relevant in the case of robotics / IoT, the Civil Code also hold persons **liable for actions caused by persons under their care and for objects under their guardianship (Article 1384)**. Thus, the legislation would require for any noncontractual incident involving the IoT or robotics to identify the person (natural person or company) under whose guardianship the relevant device or robot was operating, and to hold them liable for any damages caused by the thing or robot. This is a strict liability. A case judged by the Court of Brussels gives an example thereof: a manager of a playground was responsible for the bodily injuries of child who felt from an unsafe toboggan while using this one out of the opening hours and in violation of the prohibition to come in as indicated on a board affixed on the fence of the playground. The liability could not have been based on the contractual ground as the parents of the child had not paid an entrance fee. It should be noted that the liability was shared between the manager and the parents of the child, the latter having failed to their duty to look after their child (Tribunal de premiere instance of Brussels, 11th section, 2nd March 1999, registration number 96/6839/A). Article 1135 of the Belgian Civil Code provides that "**Agreements obligate not only to what is expressed therein but also for the consequences which equity, usage or the law gives to an obligation according its nature**." Applied to any contract of sale, the case law deducted from this the obligation of the seller to give to the buyer appropriate information, especially on the risks implied the use of the product. This jurisprudential obligation has been consecrated by Art. VI.2 of the Code of Economic Law which provides that at the latest at the time of the signing of the sale, the seller shall provide customers with correct and useful information relating to the product or service features and terms of sale, given the need of information expressed by the consumer and the use stated by the consumer or the reasonably predictable use. With regard to digital products this information has to clarify, inter alia, the functionality, interoperability and required security measures. Article 1604 Civil Code defines the delivery as the "transfer of the thing sold into the power and possession of the buyer". Case law has deducted from this article an obligation for the seller to deliver a product which complies with the contract provisions and especially an obligation to deliver a safe product. However, a product that is not in conformity with the parties' stipulations (express or implied) is not by itself defective and a defective product may perfectly comply with the contract provisions. Under this regime, the buyer may claim for the rescission or the performance of the contract, and can claim compensation if damages arose due to the failure to deliver. The claim must be brought rapidly after the delivery since the claimant could be presumed to have unreservedly accepted the product if the claimant did not raise objection regarding the conformity at the time of the delivery. Article 1641 of the Belgium Civil Code provides that "the seller is held to a guaranty against latent defects in the thing sold which render it unsuitable for the use for which it is intended, or which so diminish such use that the buyer would not have purchase it, or would have given only a lesser price for it, had he known of them". This contractual regime of liability only applies to contracts of sale. The latent defect, as interpreted by judges, can be a "structural" or a "functional" defect. A structural defect can be defined as the one that affects the product intrinsically and a functional defect as the one that renders the product unfit for its expected purpose. The liability of the seller depends on his knowledge of the defect prior to delivery of the product. The burden of the proof of the existence of the defect at the moment of the product delivery bears on the buyer but as the Belgian Supreme Court (Cour de Cassation) considers that professional sellers are deemed to have known the defect, professional sellers have to prove it was totally impossible for them to detect the defect. The European Directive 2001/95/EC on general product safety has been transposed into Belgian law by the Act of 18 December 2002 (which renamed the former Act of 9 February 1994 as the "Product and Safety Act"). It should be noted that this Act does not only deal with the "products" but also with the "services". The Act imposes post marketing duties and entitles the public authorities to take preventive actions. It must be stressed that this Act does not allow a consumer to bring an action before court to obtain compensation for damages caused by an unsafe product or service. The Act of 25 February 1991 on liability for defective products implemented the European Directive

Member State	State of play
	on liability for defective products. Services are excluded from the scope of the Act. Under this Act the injured person must prove the defect, the damage and the causal relationship between defect and damage. It has been held, for example, that the claimant did not have to prove "the exact nature of the defect regarding in particular its technical aspects" but that the defect can be inferred from the "abnormal behaviour of the thing". However, damage is not by itself the proof of the defect as the damage can come from the misuse of the product. In order to prove the defect or to assess the damages, a party may on his own motion have recourse to an expert. The judge may also appoint one or more judicial experts (article 962 Judicial Code). Of course, **specific liability regimes** apply that can overrule these principles. The Belgian **Traffic Code** of 1975 stipulates simply that any **vehicle must have a driver** (article 8.1), and that (s)he must be capable of driving and of executing all necessary driving manoeuvres at all times, keeping full control over their vehicle. Self-driving cars are thus not permitted currently, and drivers remain liable – and must carry insurance – at all times. Similarly, self-flying drones are not permitted: since April 2016, a new Royal Decree **requires an operator for all drones** (whether commercial or not), and requires a specific liability insurance for any professional or commercial use of the drones. Recreational users would not require separate insurance, but would also be liable for incidents as described above.
Bulgaria	Bulgarian civil law distinguishes between contractual and legal (delictual/tort) liability. Both regimes of liability are regulated by the Obligations and Contracts Act. According to this law, **only persons can be held liable for damages**. Contractual liability arises from a breach of a contractual obligation, whereas legal liability arises from a breach of statutory rights. Furthermore, there has to be a chain of causality between the breach and the damage. The law further distinguishes between fault-based liability and strict liability. Fault-based liability is the basic regime. Fault can be based on intention or negligence. In the legal liability the fault is presumed by law and the burden of proof for overcoming this legal presumption is for person who is held liable. **Bulgarian law does not provide for special provisions with regard to liability for damage caused by autonomous objects** (such as autonomous driving cars, internet of things objects, robots, etc.). No relevant case law could be found as well. Therefore the general liability rules will apply. In particular, such damages **could be considered damages caused by goods/things („вещи") and the Obligations and Contracts Act provides for a joint liability for the owner and person under whose control the respective thing is**. Thus, these persons would be held liable for the caused damages due to the fact that they did not use the respective autonomous objects properly or did not undertake the necessary measures to control properly such an object. However, **if the damages actually arise from a production defect or a hidden defect of the respective autonomous object, then the manufacturer, distributor and/or the merchant could be held liable as well**. Their liability could be engaged by owner of the respective autonomous objects. Depending on whether the owner is a consumer or not the liability of manufacturers, distributors and merchants for damages caused by a defective a manufactured or distributed good may be engaged under the Bulgarian Consumers Protection Act, which transposes the Directive 85/374/EEC on product liability which provide for special protection for the consumers or under the general civil rules. In cases of liability for damage caused by an autonomous driving car, the provisions of Bulgarian Road Traffic Act („Закон за движение по пътищата") would also apply. **Pursuant to Art. 20 of the Road Traffic Act the driver is obliged to control uninterruptedly the vehicles which they drive**. Therefore, it could be considered that even in cases of an autonomous driving car, the driver of such a car is obliged to control it, including control over the performance of its autonomous driving. The quoted act imposes various obligations on the all drivers of cars without any distinction whether they are autonomously driving or not as well as on every other participant in the traffic, where both the drivers and the participants in the traffic are always natural persons. In this respect, it could be expected that in case of an accident with an autonomous driving car, the fault of the driver and of all other participants in the accident will be examined. Both for the car drivers and for the other participants in the traffic the liability (administrative or penal) could be only fault-based.
Czech Republic	Under Czech law, distinguished distinction can be made between three types of liabilies: a) contractual liability, as a legal consequence where damage is caused by a breach of a contractual obligation (s. 2913 of the Civil Code), b) statutory liability, as a legal consequence where damage is caused by a breach of statutory rights and duties (s. 2910 of the Civil Code), and c) liability for a breach of good morals, which is a legal consequence where harm is caused to a victim by an inten-

Member State	State of play
	tional breach of good morals (s. 2909 of the Civil Code). In all three cases, there must be a causal nexus between the breach of (statutory or contractual obligation) and the damage. Statutory liability is a liability based on fault (intention or negligence, whereas negligence is presumed), whilst liability for a breach of good morals is linked to intentional behaviour solely. Contractual liability is a "strict liability" where the inflictor cannot be exculpated, but he/she may be solely released from the duty to provide compensation if he/she proves that he/she was temporarily or permanently prevented from fulfilling his contractual duty due to an extraordinary, unforeseeable and insurmountable obstacle created independently of his/her will (s. 2913 (2) of the Civil Code). Apart from this general categorization, the Civil Code sets out specific strict liability regimes for certain circumstances, which (with regards to the assessed question) include: a)Damage resulting from carrying out activities: A person carrying out profitable activities is to provide compensation for damage resulting from such activities. This duty does not apply if it can be demonstrated that all reasonably required care has been taken to prevent damage from occurring (s. 2924 of the Civil Code). b)Damage caused by the operation of a means of transport: A person who operates a means of transport is to provide compensation for damage caused by the specific nature of such an operation. This duty does not apply if it can be demonstrated that there was an external cause of the damage or that all reasonable efforts were made to prevent the damage from occurring (s. 2927 of the Civil Code). c)Damage caused by a thing: A person who uses a defective thing when performing its obligations is liable for the damage caused by such defective thing (s. 2936 of the Civil Code). If the thing causes the damage by itself, the person who should have supervised the thing, or its owner, may be held liable (s. 2937 of the Civil Code). d)Damage caused by a product defect: The damage caused by a product is to be compensated jointly and severally by the persons who manufactured, marketed and imported such product. The product is defective if it is not as safe as it is reasonably expected (s. 2939 (1), (2) and 2940 (1) of the Civil Code).The manufacturer of a component of the product is not required to provide compensation for damages if he/she proves that the defect has been caused by the product's structure into which the component was incorporated, or that it was caused as a result of a fault in the product's manual (s. 2942 (3) of the Civil Code). **Where the damage was actually caused by an autonomous object (such as an autonomous car, internet-of-things object, robot, etc.), the general liability provisions (or a combination of them) described above would apply. There is no specific liability regime** with regards to these machines per se and no relevant case law at present.
Estonia	Under Estonian Law of Obligations Act, a person who unlawfully causes damage to another person must compensate for the damage if the person is culpable of causing the damage or is liable for causing the damage pursuant to law. Section 1056 of the Law of Obligations Act prescribes that if damage is caused resulting from danger characteristic to a thing constituting a major source of danger or from an extremely dangerous activity, **the person who manages the source of danger is liable for causing of damage regardless of the person's culpability**. **A person who manages a major source of danger is liable for causing the death of, bodily injury to or damage to the health of a victim, and also for damaging a thing of the victim, unless otherwise provided by law**. A thing or an activity is deemed to be a major source of danger if, due to its nature or to the substances or means used in connection with the thing or activity, major or frequent damage may arise from it even if it is handled or performed with due diligence by a specialist. **Although there is no specific case law, such major source of hazard could also be an IT system**. Under Section 1057 Estonian Law of Obligations Act, the **direct possessor of a motor vehicle** is liable for any damage caused upon the operation of the motor vehicle, except in certain exception-

Member State	State of play
	al circumstances. This regulation is not based on the definition of motor vehicle from the Traffic Act and its scope is more extensive (Traffic Act applies only to motorised vehicles which have a design speed over 6 km/h). Therefore, all direct possessors of motorised vehicles may fall under the strict liability regulation under the Law of Obligations Act. Estonia has transposed the European Product Liability Directive of 25 July 1985 by Law of Obligations Act. As in other Member States, the regime is based neither on tort nor on contract but it is a purely legal regime. The producer is primarily liable for the damage caused by the defective product that he put into circulation, defined as a product that does not provide the safety which a person is entitled to expect. Under Section 1063 of the Law of Obligations Act, **computer software is also deemed to be a (movable) product**. Therefore, producer of the software can be held liable under the producer liability provisions. This is a strict liability regime under which the producer is liable for causing the death of a person and for causing bodily injury to or damage to the health of a person if this is caused by a defective product.
Germany	German law distinguishes mainly between contractual (vertragliche) and legal (gesetzliche) liability. Sections 280 et seq BGB regulate contractual liability. Legal liability is regulated by Sections 823 et seq. BGB. Contractual liability arises from a breach of a contractual obligation, whereas legal liability arises from a breach of statutory rights. Under both regimes the breach must damage protected rights. Furthermore there has to be a chain of causality between the breach and the damage as well as a certain degree of predictability between the breach of an obligation and the resulting damage. The law further distinguishes between fault-based liability (Verschuldenshaftung) and strict liability (Gefährdungshaftung). Fault-based liability is the basic regime. Fault can be based on intention or negligence. A person acts negligently if failing to exercise reasonable care (Section 276 BGB). A fault-based type of legal liability is "manufacturers liability" (Produzentenhaftung), regulated by Sections 823 et seq. BGB. Strict liability is usually based on specific legal provisions (for example Section 833 BGB for animals or Section 7 StVG (Strassenverkehrsgesetz) for road vehicles). An important type of strict liability is "product liability". The assumption behind this regime is that the placing on the market of a product already causes a risk for which the manufacturer has to be liable. The provisions of the German product liability act (ProdHaftG) are a transposition of the European product liability directive. With regard to the IoT context **some German legal authors have pleaded for an extension of the strict liability regime** (see, e.g. the article of M.C. Gruber, Zumutung und Zumutbarkeit von Verantwortung in Mensch-Maschine-Assoziationen, https://www.jura.uni-frankfurt.de/44269259/Gruber_MMA_121126.pdf) In July 2016 the German media reported about a plan of the German federal minister for traffic Mr. Dobrindt to **propose new legislation on autonomous driving** in Germany. The proposed legislation would aim to authorise autonomous driving vehicles on German roads. According to the proposed text, **the driver should, however, remain stand-by ("wahrnehmungsbereit")** and ready to take over the steering wheel at every moment when the system invites him to do so and in any case each time when a technical incident occurs or a warning message appears on the dashboard. Interesting is also that, according to the proposed legislation, manufacturers are liable if the system fails. In practice it will be crucial, each time an accident occurs, to determine who was driving: the autonomous system or the human driver. Therefore, the proposed text provides an **obligation to document incidents in a secured black box**.
Finland	Autonomous driving cars have been subject to great attention in Finland as well. According to the Finnish Transport Safety Agency (Trafi), **the current road traffic legislation in Finland enables testing of autonomous driving cars, and there has been no need for a separate legal reform**. Trafi will provide practical help to those involved in the development of autonomous driving cars or those interested in the testing of such cars in determining the driver and getting the technical approval and registration for the car. According to Trafi, in an autonomous driving car, the car itself drives the car and observes the surroundings. However, an autonomous driving car always also has a driver which functions as a backup system. The driver may be inside the car or control the car remotely. One driver may have control of several autonomous driving cars at the same time. The Finnish Ministry of Transport and Communications has stated that **according to the current legislation, the driver is always liable for the vehicle**. According to Trafi, **when it comes to deter-**

Member State	State of play
	mining liability, the driver is the one who decides on the movement of the vehicle. In practice, **insurances** likely play a significant role when it comes to the liability in Finland. Motor vehicles registered in Finland must have compulsory car insurance. This covers both physical injury and damage to property caused by using the vehicle in the traffic. A new Traffic Insurance Act enters into force on 1 January 2017. Product liability of autonomous driving cars was taken into account when making the new Act. It was stated that because of autonomous driving cars, the product liability of the car manufacturer may actualise more often than earlier. Accordingly, the right of recourse pursuant to the Product Liability Act was extended to insurance companies so that insurance companies may claim damages from the car manufacturer (which has not been the case so far in Finland). Also transport market regulations are currently under a significant reform in Finland. Transport market regulations will be collected under a unified Transport Code, which is currently considered by the Parliament. The legislative proposal mentions that "discussing cars" are a question of the future, and the proposal mentions various issues that need to be taken into account for the purpose of fully autonomous cars, such as the need of the driving services and road maintenance to get information on traffic signs, road conditions, weather, dangerous situations etc. The legislative proposal states that for the present, regulation which would enable the said activity is not examined. Also **automated financial services** (for example investment advice given by robots and automated trading) have been under discussion in Finland. A representative of Finnish Financial Supervisory Authority has stated that in case of any problems arise – whether caused by a human error or technical error – **a service provider is responsible**.
France	**Liability for damage caused by things** (responsabilité du fait des choses) **is provided for in Art. 1384**, paragraph 1 of the French Civil Code, as construed by the case law of the Court of Cassation. It is a **strict liability** regime. For applying the regime, a "thing" needs to be involved in the occurrence of the damage. "Thing" is an open term and should be interpreted extensively: it can refer to movable or immovable property, whether or not operated by the hand of man, and whether or not inherently dangerous. In some cases, liability for damage caused by things is regulated by **specific regimes**. Provided the case meets all the requirements of the specific regime, it will not be governed by the general rules of the Civil Code. Two relevant examples are the regime with regard to damage caused by **land motor vehicles** (governed by the Law N° 85-677 of 5 July 1985 on compensation for victims of traffic accidents) and the regime with regard to **defective products** (Law N° 98-389 of 19 May 1998). In an IoT context each one of these liability regimes can be applicable depending on the kind of damage or on the context. Under the general regime, the person claiming compensation for damages caused by a thing, will have to prove that the person responsible for compensating the damage sustained should be identified as the **guardian** (le gardien) of the thing. The guardian is the one who had **custody** (la garde) of the thing. **Having custody means having the use, management and control of the thing**. The owner of the thing is presumed to be the guardian but evidence to the contrary is admissible. The guardian can be a minor or even a child. A person acting according to the instructions given by others, such as an employee acting as instructed by his employer, cannot be the guardian of the thing that has been entrusted to him. Custody can be transferred from one person to another, voluntarily or involuntarily, such as in the case of theft or by coincidence. It can also be divided, according to the structure of the thing and its behaviour. France has transposed the European **Product Liability** Directive of 25 July 1985 by law of 19 May 1998, codified in articles 1386-1 to 1386-18 of the French Civil Code, renumbered as articles 1245 to 1245-17 of the Civil Code with effect from 1 October 2016. As in other Member States, the regime is based neither on tort nor on contract but it is a purely legal regime. The producer is primarily liable for the damage caused by the defective product that he put into circulation, defined as a product that does not provide the safety which a person is entitled to expect. It is a strict liability, i.e. without requiring proof of the producer's fault. The law of 19 May 1998 is, similar to the European Directive, only applicable to "products". A product is defined as "a movable thing, even if incorporated into an immovable object". The discussion whether or not the provisions of the law also apply to intangible objects has been discussed with regard to software. Does the law, for example, apply to a **computer programme** which contains a bug or has been infected by a computer virus? Under French law the answer to this question is **not entirely clear**.

Member State	State of play
	However, there seems to be a **consensus that the law applies to a tangible product, such as an autonomous car, even if the defect is purely due to software error**. It is finally clear that, as devices such as cars become more autonomous, identifying who is liable in case of an accident will be more and trickier.
Italy	The Italian literature assessed the issues related to robotics liability in several contributions and articles. According to Sartor, Gli agenti software: nuovi soggetti del ciberdiritto? Contratto e Impresa, 2, 2002, robots may have their own assets, and could be liable within the limits of their assets. Prof. Taddei Elmi proposed to equate robots to 'ambassadors' that simply carry the message of the user of the robot itself to third parties (see Taddei Elmi, Soggettività artificiale e diritto, available at http://www.altalex.com/documents/news/2004/06/25/soggettivita-artificiali-e-diritto). Damages caused by the robot should be attributed to the producer or user of the robot, since robots cannot have legal personality. This would be a case of **extra-contractual liability according to article 2050 of the Civil Code that states that the person who performs dangerous activities must compensate the damage arising from those activities**. In alternative, article 2052 of the Civil Code on the **liability of the guardian of an animal**, who shall be liable for the damages caused by the beast, can also apply analogically. See Scialdone, Il diritto dei robot: la regolamentazione giuridica dei comportamenti non umani, in: La rete e il fattore C: Cultura, Complessità, Colleborazione, Roma, 2016. For an extended analysis of the topic please refer to Santosuosso, Diritto, scienza, nuove tecnologie, Padova, 2011. According to a recent detailed research about robotics liability, such liability can be assessed **based on article 2049 (about liability of masters and patrons) and on article 2051 of the Civil Code (about liability of the guardian for the things under his care)**. However, provided that robots cannot be directly liable since they are not persons, it may appropriate to apply the rules and concepts about strict and quasi-strict liability. The different actors who can be held liable are mainly the producers, programmers and users of the robot. Regarding criminal liability for the damages to persons, the individual in charge of the assembly, functioning and use of the robot shall be held liable for the injuries caused by the robot to human beings. See Artusio, Senar, The Law of Service Robots, available at https://nexa.polito.it/nexacenterfiles/robots-2015.pdf.
Latvia	The Latvian law does **not specifically regulate** the liability for harm caused by autonomous objects or things. However, there is a general obligation to compensate the caused damage. I.e. Section 1635 of CL stipulates that **a person, who has suffered harm caused by any wrongful act or failure to act, has the right to claim satisfaction from the infringer, insofar as they may be held at fault for such act. Section 1779 of CL reiterates that everyone has a duty to compensate for losses they have caused through their acts or failure to act**. The liability **in case of sources of increased risk, e.g., automated cars, is specified in Section 2347** of CL. Namely, it establishes that a person whose activity is associated with **increased risk for other persons (transport, construction, dangerous substances, etc.) shall compensate for losses caused by the source of increased risk, unless he or she proves that the damages have occurred due to force majeure, or through the victim's own intentional act or gross negligence**. In case a third person has unlawfully taken into possession the source of increased risk and there is no fault by the owner (or possessor), the third person is liable for the losses caused. There is also specific regulation regarding situations when a loss is caused by something being thrown or poured out into the street or another place where people walk or stay, or by inadequately fastened objects falling from a house onto the street, etc. According to Sections 2358 to 2360 of CL, a person suffering such loss may claim compensation for the loss from the person living in the building or having possession of that part of the building from which something was poured or thrown. By analogy, in our opinion, a victim could claim compensation, for example, from a drone's owner or possessor, if the drone would have fallen and injured the person. The lack of specific regulation in CL is remedied by the law "**On Liability for Defective Goods and Deficient Services**", which stipulates the liability for harm that has been inflicted upon human life or health, or upon the property of a person, due to defective goods or deficient services, thus it also applies in cases where autonomous objects are sold or are involved in providing a service. Section 5 of this law stipulates that the manufacturer of the goods or the provider of the services has the duty to compensate for the losses caused to the injured person due to defective goods or deficient services. According to Section 8 of the law, the liability is still possible even if the harm is caused by both the product or service and some actions by a third person. In this case, the manufacturer or the provider of the services has a right to bring a third party action against such third

Member State	State of play
	person, insofar as his or her action has caused or increased the loss. We are **not aware of any relevant jurisprudence** in Latvia regarding the liability for harm caused by autonomous objects. This has not been also discussed as a topic in academia and by the legal doctrine yet in Latvia.
Lithuania	Liability for damage caused by autonomous objects (such as autonomous driving cars, internet-of-things objects, robots, etc.) is **not specifically covered** by the law. However, **it would generally fall under the strict liability regime under Article 6.27**0 of the Civil Code. According this article **a person whose activities are connected with potential hazards for surrounding persons (operation of motor vehicles, machinery, electric or atomic energy, use of explosive or poisonous materials, activities in the sphere of construction, etc.) shall be liable to compensation for damage caused by the operation of potentially hazardous objects which constitute a special danger for surrounding persons**, unless he proves that the damage was caused by superior force or it occurred due to the aggrieved person's intentional or grossly negligent actions. Liability falls on the **controller of a potentially hazardous object, who controls the object by the right of ownership or trust or on any other legitimate grounds** (loan for use, lease, or any other contract, by the power of attorney, etc.). The controller of a potentially hazardous object shall not be liable to compensation for damage it has caused if he proves to have lost the operation thereof due to unlawful actions of other persons. In such event, liability arises to the person or persons who gained the operation of a potentially hazardous object by unlawful actions. Where the loss of operation of a potentially hazardous object results also from the fault of the possessor the latter and the person who seized the potentially hazardous object unlawfully shall be jointly and severally liable for the damage. Upon having compensated for the damage, the possessor shall acquire a right of recourse for the recovery of sums paid against the person who unlawfully seized the potentially hazardous object. In the event where damage was inflicted to a third person in the result of reciprocity of several potentially hazardous objects, all the possessors of the objects concerned shall be jointly and severally liable for the damage caused. The Civil Code of the Republic of Lithuania **also provides the liability of a producer which is bound to compensate for damage caused by defective products**. The liability shall be applicable only where the products are obtained for the purposes of consumption but not for commercial purposes. In the event where it is impossible to identify the producer of a product, any person involved in the sale of the product shall be regarded as producer unless he provides the aggrieved person with information about the producer or the supplier of the product. This rule shall also apply in the cases where a product was imported into the Republic of Lithuania without its importer being indicated though the producer of the imported product is known. There is no judicial practice in Lithuania regarding liability for damage caused specifically by autonomous objects.
Luxembourg	Legal discussions with regard to damage caused by "internet of things" objects, without any direct human intervention, have started in Luxembourg in the context of the use of drones. A company - Flash Biologistic – developed a plan to deliver pharmaceutical products and other medical items such as plasma, organs, etc., by drones equipped with an isotherm bag. The company is still waiting to obtain all the required authorisations but hopes to launch the service in 2017. In that context, the **Luxembourg government is currently considering to introduce more flexibility in the current legislation**, in particular in the domain of aviation, in order to make such initiatives possible under specific conditions. At the same time, discussions are ongoing with regard to the complex legal problems that could possibly arise if an accident would occur. To a large extent, the stakeholders hope to be able to solve most of the issues via contractual clauses. Outside the reach of a contract, liability for damage in the IoT context is essentially regulated by the basic rule of Art. 1384 of the Civil Code. Similar to France and Belgium, liability for damage caused by things (responsabilité du fait des choses) is a strict liability regime. For applying the regime, a "thing" needs to be involved in the occurrence of the damage. **To determine who is liable for damage caused by an object, it is essential to determine who the guardian of that object is**. Contrary to the liability based on articles 1382 and 1383 of the LCC, which require proof of a fault, article 1384, first indent establishes a presumption of liability of the holder of the product that caused the damage. Luxembourg case law defines **the "holder" (gardien) as the person having the powers of use, command and direction of the product**. The presumption of liability applies if (i) there was contact

Member State	State of play
	between the object causing the damage and the damaged good and (ii) the object was in motion at the time of contact. In the absence of contact or if the product was inert, the victim must prove that the object was at least in part instrumental to the realisation of the damage. Everyone is aware that, in the context of IoT, this issue could become very complex. Product liability is governed by the Luxembourg law of 21 April 1989 on the civil liability for defective products, implementing the European Directive 85/374/EEC, as amended (http://eli.legilux.public.lu/eli/etat/leg/loi/1989/04/21/n1). Under the provisions of this law, producers are liable for damages caused by defects in their products. The term "product" is defined as "any movable good, even incorporated in another movable or immovable: the term also refers to electricity." A product is defective when it does not provide the safety which the user is entitled to expect. The victim must prove the defect, the damage and the causal link between the defect and the damage. The law does not affect other rights the user may have according to the general principles of contractual or tortious liability.
The Netherlands	The Dutch liability law distinguishes between, at the one hand, contractual liability ("contractuele aansprakelijkheid") and, at the other hand, legal liability ("wettelijke aansprakelijkheid"). Book 7 of the Dutch Civil Code provides for specific agreements. Book 6 of the Dutch Civil Code states general liability provisions. Contractual liability arises from a breach of a contractual obligation, while legal liability arises from a violation of the law. Legal liability then distinguishes further between liability from wrongful act or tort ("onrechtmatige daad", art. 6:162 Dutch Civil Code) or liability from lawful act ("rechtmatige daad"). For tortious liability, five conditions need to be fulfilled: unlawful conduct (act or omission), accountability of the act, damage, causal link between the act and the damage and relativity (art. 6:163 Dutch Civil Code). Relativity means that the offender is only liable for damages, if the norm which he has violated aims to protect the (affected) right of the injured. In other words, there must be a relationship between the damage and the interest protected. Liability from lawful act arises from acts that can result in an indemnification obligation under the Dutch law, but which are not a tortious act. Examples of such lawful acts are benevolent intervention (Negotiorum gestio, art. 6:198 Dutch Civil Code), undue payment (art. 6:203 Dutch Civil Code) or unjustified enrichment (art. 6:212 Dutch Civil Code). With regard to autonomous driving vehicles, the main problem is that the driver himself has still an important role in the current Dutch liability law. Therefore, **some Dutch authors, plead for alternative insurance forms. For example, the so-called direct or first-party insurance. The key feature of that form of insurance is that not the liability risk is insured, but rather the risk of damage**. This means that, in case of a vehicle collision, the party that suffered damages, will claim those damages from the insurance of the vehicle they were in at the time of the collision, instead of claiming damages from the insurance of the party that is liable for the collision. In the Netherlands, this procedure is already applied in case of a multiple-vehicle collision. Note that vehicle insurance is mandatory in the Netherlands. The acts of the driver himself are less important in cases of strict liability ("risicoaansprakelijkheid"), which means that the driver is legally responsible for the damage and loss caused by his acts or omissions, regardless of culpability. An example is art. 185 of the Dutch Road Traffic Act (" Nederlandse Wegenverkeerswet" or "WVW"). This article provides for a form of strict liability for accidents between bicycles and motorised vehicles. This means that, in a collision between a vehicle and a cyclist, that the driver is deemed to be liable to pay damages. The driver's insurance will have to compensate the cyclist, as long as the collision was unintentional. However, the driver's insurance only has to pay half of the damages if the cyclist was in error, unless the cyclist is under the age of 14. Another example of strict liability is product liability (Book 6, Section 6.3.3 Dutch Civil Code, see http://www.ejcl.org/64/art64-6.html). Regarding the context of robots, some Dutch authors (S. DE SCHRIJVER, R. VAN DEN HOVEN VAN GEDEREN) tried to identify the "robot 2.0". They criticized the definition of robot as mentioned in the European project "RoboLaw". They want to do away with the cliché that robots should be human-like. In contrast, they support the definition of a robot proposed by "Robotpark" (http://www.robotpark.com/What-is-a-Robot). Furthermore, some authors (R. VAN HOVEN VAN GENDEREN and E. VAN DUIN) asked the question whether a robot could be identified as a legal subject ("rechtssubject"), instead of a legal object (art. 3:1 Dutch Civil Code). They conclude that, **at this moment, the "robot 2.0" does not fulfil the conditions of a legal subject.**

Member State	State of play
	The Dutch Ministry of Economic Affairs issued in September 2015 a **report dealing with the development and trends regarding the Internet of Things, but the report also deals largely with the spectrum policy to facilitate IoT applications** (https://www.rijksoverheid.nl/documenten/rapporten/2015/10/08/internet-of-things-in-the-netherlands). Some Dutch authors remarked that in an Internet of Things world, a lot of devices are interconnected. This means that a defect in one device, can result in damage with another device. The question then is, which device caused the damage and who will be responsible for that? Producers can limit their liability between each other, such as for indirect damages, but producers cannot limit their liability against consumers.
Poland	There is **no special liability regime for IoT** in Poland. There are some specific liability regimes for **vehicles** (which could apply to autonomous driving cars or other moving robots) and hazardous products (of course, the latter category would not apply to any IoT objects, but only to a very specific category of such objects). The two will be briefly described below. In most of the cases, however, the standard liability regime for damages arising from non-performance or improper performance of an obligation or liability under implied warranty for defects and quality warranty would apply. According to the Civil Code (Arts 436-437) an **owner-like possessor of a vehicle** propelled by natural forces is liable for any personal or property damage caused by the operation of the vehicle (no matter who, if whoever, drives the vehicle), unless the damage is due to force majeure or solely to a fault on the part of the aggrieved party or a third party for whom he is not responsible. However, if the owner-like possessor has given his vehicle over for dependent possession, the liability is borne by the dependent possessor. The liability cannot be excluded or limited in advance. According to the rules governing the liability for damages caused by a hazardous product (art. 4491-11 Polish Civil Code) anyone who, within his business activity, manufactures a hazardous product is liable for damage caused to any person by the product. A product means a movable object even if it is attached to another thing (a product for these purposes also means electricity). A product is hazardous, according to the Civil Code, if it does not guarantee the safety that could be expected based on normal use (circumstances at the time the product is put into circulation, and especially the manner in which the product is presented on the market and the information provided to the consumer regarding product properties, determine whether the product is hazardous; a product cannot be deemed unsafe only because a similar improved product is put into circulation at a later time). A manufacturer is not liable for damage caused by a hazardous product if it did not put the product into circulation or if the product was put into circulation outside the scope of its business activity. Nor is the manufacturer liable if the properties of a hazardous product are revealed after the product is put into circulation unless they are due to an element inherent in the product. Furthermore, the manufacturer is not liable if the hazardous properties of the product could not have been foreseen based on scientific and technological conditions at the time the product was put into circulation (the standard in this respect is objective and restrictive), or if the properties result from requirements established by legal acts. A manufacturer of materials, raw materials or a constituent part of a product bears the same liability as the manufacturer, unless the sole cause of the damage was the defective construction of the product or the manufacturer's instructions. Anyone who, by placing his name, trademark or other distinguishing mark, purports to be the manufacturer, bears the same liability as the manufacturer. The same liability refers to anyone who introduces a product of foreign origin to domestic trade within the scope of its business activity (importer). Compensation for damages caused by a hazardous product is due only if the damage does not exceed the equivalent of EUR 500 (this does not apply to damages to a person). A claim for remedying the damage caused by a hazardous product is barred by the statute of limitations three years after the day on which the aggrieved party learns or, having used due care, could have learned of the damage and of the person obliged to remedy the damage. In every case, however, the claim becomes barred by the statute of limitations ten years after the product is put into circulation.

Member State	State of play
	The liability for a hazardous product cannot be excluded or limited by way of a contract or by choosing a foreign jurisdiction. It is available cumulatively with other liability types.
Romania	Art. 1376, paragraph 1, of the Romanian Civil Code regulates the **liability regime for the damages caused by things** (raspunderea pentru prejudiciile cauzate de lucruri) by providing that anyone has **the obligation to repair, irrespective of any guilt, the damage caused by the thing which was under its guard**. It is a **strict liability** regime. In order to apply this regime, certain conditions have to be met, namely: (i) the existence of the damage; (ii) the existence of a causality relation between the damage and the action of the "thing"; (**iii) the thing must be under the guard of the responsible person**. Under the Romanian Civil Code, the "thing" covers assets, tangible or not, which are subject to a patrimonial right. The doctrine notes that any asset can be considered a "thing" under the Civil Code, it can refer to movable or immovable property, whether or not operated by the hand of man, and whether or not inherently dangerous. In some cases, liability for damages caused by things is regulated by **specific regimes**. Provided the case meets all the requirements of the specific regime, it will not be governed by the general rules of the Civil Code. Two relevant examples are the regime regarding accidents caused by **land motor vehicles** (governed by the Government Emergency Ordinance no. 195 of 2002 regarding Driving on Public Roads) and the regime with regard to **defective products** (Law no. 240 of 2004 regarding the Liability of Producers for the Damages Caused by Defective Products - "Law no. 240 of 2004"). In relation to the IoT and the damages caused by autonomous objects, each one of these liability regimes can be applicable depending on the kind of damage or on the actual situation. Under the general regime provided by the Civil Code, the person claiming compensation for damages caused by a thing will have to prove that the person responsible for compensating the sustained damage should be identified as the guardian (paznic juridic) of the thing. The guardian is the one who has legal custody (paza juridica) of the thing, which means that the guardian has the power to control, use, manage and overview the thing. As a general rule, the owner of the thing is presumed to be also the guardian, however there may be exceptions to this rule (e.g. in case the thing was stolen). The guardian can be even a minor. Custody can be transferred from one person to another, voluntarily or involuntarily, such as in the case of theft or handing over of the thing to someone else for use. Romania has transposed the European Product Liability Directive no. 85/374/CEE of 25 July 1985 through the Law no. 240 of 2004. The producer is liable for the damage caused by the defective product that it put into circulation. It is a strict liability, i.e. without requiring proof of the producer's fault. The Law no. 240 of 2004 is, similar to the European Directive, only applicable to "products". A product is defined as "a movable thing, even if incorporated into an immovable object; energy is also considered product". So far there has been no discussion in the doctrine regarding the extent to which the provisions of the Law no. 240 of 2004 apply with regard to software. However, further to the interpretation of the law, the software is considered a product, and therefore the provisions regarding the liability of the producer should apply. In addition to the Law no. 240, Law no. 449 of 2003 regarding the Sale of Products and the Associated Guarantees provides that the producers are liable to the extent their product does not comply with the specifications. In a similar manner, an autonomous car, for example, will also be considered a product under Law no. 240, consequently triggering the liability of the producers in case of a defective car. However, determining the liability in case of accidents produced by autonomous devices will probably be subject to further discussions in doctrine and maybe subject to new regulations once such autonomous devices will become more frequent.
Slovenia	In general Slovene law distinguishes between civil and criminal liability. Civil liability may be further divided to contractual and legal liability. Contractual liability arises from a breach of a contractual obligation, whereas legal liability arises from a breach of statutory rights. Under both regimes the breach must damage protected rights, in case of contractual liability such rights are provided by the contract itself whereas in case of legal liability the rights are provided by law. Since it is highly likely that IoT services and service providers would be under Slovene law considered as information society services and information society service providers the relevant provisions of the Electronic Commerce Market Act (Official Gazette RS. No. 61/06, as amended, hereafter "ECMA"), should also be observed. Pursuant to general provisions on liability as provided by the Slovene Code of Obligations (Official Gazette RS. No. 83/01, as amended, hereafter "CO"), especially Section 2, together with a breach of legal and/or contractual obligations, the existence of damage and causality between the breach

Member State	State of play
	and the damage shall exist. The same concept was adopted also for any information society services and information society service providers pursuant to the ECMA the Electronic Commerce Market Act which refers to the CO with respect to any liability of information society services providers. **Thus liability with respect to IoT would be adjudicated under the general concepts of civil liability without any specifics.** With respect to liability regimes the Slovene law adopted the concept of the reversed burden of proof, according to which it is sufficient for the creditor to indicate that damage was caused to him by an act or event for which the debtor is liable under either contract or law, the debtor may however exculpate by proving that he cannot be held liable for the caused damages. The law further distinguishes between fault-based liability and objective liability (Article 131, CO). Thereby fault can be based on intention or negligence, whereas in case of objective liability it is sufficient to prove for the creditor to invoke liability that a certain thing or activity under the control of the debtor is objectively dangerous and capable of causing greater damage to the environment. A person acts negligently if failing to exercise due care, whereby the due care is dependent of the subjective status of the concerned debtor. In this respect the CO distinguishes between the due care of a prudent individual, prudent businessman and the expert. **IoT liability was not yet discussed by the available case law and legal theory in Slovenia and also no identifiable legislative measures are in preparation**. However, considering the observations above it is likely that IoT liability under Slovene law could be always interpreted as a fault-based type of legal liability and under certain circumstances also objective liability (e.g. Samsung Galaxy Note 7 battery fire), whereby the due care of the debtor [in this case the application or IoT device controller] would be assessed at least with the standard of a prudent businessman, but even more likely of the expert.
Sweden	Liability for damage to persons or property is governed by the Tort Liability Act (Skadeståndslag (1972:207)). In general, there must exist a subjective element of intention or negligence in order for liability to be found (Chapter 2 section 1). No distinction is made as to whether that causing the damage was a person or an object; the provisions simply provide for an act or an omission resulting in damage to a person or property. As such, **no specific liability provisions exist for damage caused by autonomous objects** under Swedish legislation. The rules of the Tort Liability Act are **not applicable where more specific liability provisions exist**. Injuries caused by traffic is one such area, and is of interest from an autonomous vehicle perspective. The **Motor Traffic Liability Act** (Trafikskadelag (1975:1410)) requires an owner of a motor vehicle to insure the vehicle; any compensation for damage caused in traffic is then paid via the motor vehicle's insurance. Section 10.2 of the Act states that where damage has been caused by another vehicle or was due to another vehicle' defect, that vehicle's insurance is liable to pay for the damage. The Motor Traffic Liability Act contains provisions of a general nature, focusing on the owner of a vehicle and the Swedish insurance system; as such, even though no specific liability provisions exist for autonomous vehicles, it should be possible to apply the existing provisions to these vehicles. In November 2015 the Swedish Government set up an **inquiry focusing on the regulatory changes necessary for the introduction of wholly or partially self-driving vehicles** (Committee Directive 2015:114 of the Ministry of Enterprise and Innovation). An initial part of the inquiry, focusing on the regulation of trials using self-driving vehicles, was presented in March 2016 (Official Government Report 2016:28). The partial report concluded that in such cases the **existing legal framework on damage caused in traffic could be applied to self-driving vehicles**, due to the general nature of the provisions and the fact that the law does not focus on the driver, but rather the vehicle itself and its insurance. The full inquiry is due to be finalised in November 2017 and will include a full analysis of existing Swedish traffic regulations, responsibility for driving self-driving vehicles, and privacy and data security aspects of the storage and use of information from self-driving vehicles. The **Product Liability** Act (Produktansvarslag (1992:18)) is another piece of legislation concerning specific liability provisions, dealing with damage caused due to a product's defect. In such cases the product manufacturer is strictly liable for damage caused by the defective product. The Act is applicable to products, defined in Section 2 as movable objects (lösa saker). **Autonomous objects such as self-driving cars, internet-of-things objects and robots would therefore be considered as products under this definition and treated in the same way as non-autonomous devices**. Where damage has occurred due to a defect in a product that constitutes a component of another product, both products are considered to have caused the damage according to the Product Liabil-

Member State	State of play
	ity Act. The preparatory works, however, state that **software is not considered a product, but rather a series of instructions that make hardware perform certain actions (Government Bill 1990/91:197, p. 93). The legislator left it to the courts to decide where the line should be drawn between damage caused by a defective product (considered within the scope of the Product Liability Act) or damage caused by a software error (considered outside the scope, and therefore reverting to the general principles of the Tort Liability Act where intention or negligence is required). These provisions are clearly of relevance from an IoT perspective**; where smart objects are made up of complex multiple components, it will be more difficult for courts to determine where to draw the line and ultimately determine the component(s) responsible for causing damage and thus where liability should be found. As yet, no case law on this issue is available.
United Kingdom	Since autonomous devices in an IoT context are products, the **product liability** regime in the UK will apply to this context. Claims are likely to arise where defective devices, sensors, etc. are commercialised or where the use of these devices cause damage to their users or third parties. Product liability claims **may arise out of breach of contractual provisions, under the tort of negligence or under the strict liability provided for in the Consumer Protection Act 1987**, which implements the European Product Liability Directive 85/374. Contractual product liability claims may further be brought against a seller of products where there is a breach of expressed or implied terms of the contract under with products were sold. A good overview of the contractual framework for the IoT has been recently published by the European Journal of Law and Technology (Noto La Diega G. & Walden I., "Contracting for the 'Internet of Things': looking into the Nest", in European Journal of Law and Technology, Vol 7, No 2, 201, http://ejlt.org/article/view/450/662). A discussion in the UK which is now solved by the advent of the new Consumer Rights Act of 2015 (http://www.legislation.gov.uk/ukpga/2015/15/contents/enacted), related to the **protection of consumers with regard to digital products**. Professor Robert Bradgate of the University of Sheffield, in a report of 2010 prepared for the UK Department for Business, Innovation and Skills, proposed to regulate the current problems in this domain by new primary legislation (https://www.gov.uk/government/publications/driverless-cars-in-the-uk-a-regulatory-review). Until recently, notwithstanding the growing importance of the digital economy, it was not clear what, if any**, legal rights the purchaser of a digital product had if the product proved defective or failed to live up to expectations**. The rights of the purchaser of a traditional physical product are well-known and familiar. At their core are the "implied terms" contained in the Sale of Goods Act, 1979. Those terms require that the seller has the right to sell the goods, the goods supplied correspond with their description, are of satisfactory quality and reasonable fit for the buyer's purpose, and correspond with any sample by which they are sold. Over time legislation has extended the scope of application of these implied terms so that they now apply not only to contracts of sale but to all forms of contract arrangements by which goods are supplied. In the context before 2015, however, the weakness of the implied terms was that they only applied to transactions for the supply of "goods". There was considerable doubt whether a transaction involving the supply of intangible products in digital form could be said to be a transaction relating to goods, it being argued that goods must be tangible (although this is not an explicit requirement as such stated in the legislation). It is correct that implied terms also exist for the supply of services but for several reasons, this provides a lower level of protection than do the implied terms relating to goods. The uncertainty stemmed also from case law, in particular form the key decision of the Court of Appeal in the St Alban's v. ICL case in which the court gave an opinion that software may be classified as goods so long as it is supplied on some physical medium such as a CD or data key, but that software as such, being an intangible arithmetical algorithm is not and of itself goods (see further: Alison White, Caveat Vendor?, in JILT 1997 (3), https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_3/white/) . As a result, two consumers buying the same product with the same defect have different rights in law. To compound the confusion courts in Scotland adopted a different view on this topic. With the advent of the **Consumer Rights Act 2015** this has all changed. The Act introduces a new category of sales contract, namely **contracts between a trader and consumer in relation to digital content**. The rights and remedies for digital content are found in Part 3 of the Act (see further: Lucy McCormick, http://www.hendersonchambers.co.uk/wp-content/uploads/2015/09/Alerter-Consumer-Rights-Act-and-digital-products-Lucy-McCormick-10-September-2015.pdf)

Member State	State of play
	The UK Department for Transport published a 191 pages report "the Pathway to Driverless Cars" in February 2015 (https://www.gov.uk/government/publications/driverless-cars-in-the-uk-a-regulatory-review). The review concludes that **currently the regulatory framework in the UK is not a barrier to the testing of automated vehicles on public roads provided that a licensed driver is present and responsible for the safe operation of the vehicle, and that road traffic law is observed**. In order to comply with current law in the UK the licensed driver will have to be present. A licensed test driver will be required in case of testing fully automated vehicles. The Government announced that it will **review its national regulations by 2017** in order to address issues related to driverless cars technology. The Government also intends to establish a dialogue with international organisations to amend international regulations by 2018. There is currently no specific legislation on liability related to autonomous cars in the UK. **Criminal and civil liability would be assessed on a case by case basis**. Liability may arise in negligence when a driver breaches his duty of care to other road users and causes damage. According to the Road Traffic Act 1988, third party insurance is required from drivers of vehicles on a road or public places in the UK. Third party insurance covers accident causing damage or injury to third parties, vehicle, animal or property. As the degree of automation increases, continuous human control and thus any liability resulting from the driving activity would be less likely to be attributed to the driver and more likely to lie with the manufacturer.

Annex 2 – Sectoral case studies

This Annex contains the final case studies carried out for this assignment on twelve sectors or domains: agriculture, finance, chemistry, aviation, machinery and industrial platforms, automotive, retail, energy, telecommunication and health.

Agriculture: Precision farming

Context

Global challenges for the agricultural sector

The sufficient provision of food and the efficient use of natural resources is one of the vital tasks for today's society. According to academic estimates, the world needs to nourish an extra billion people within the next twelve years, which poses challenges for the agriculture sector.

In addition, the agriculture sector is facing the following challenges: [231]

- Slow-down in productivity growth;
- Limited availability of new arable land;
- Climate change;
- Price and availability of energy; and
- Impact of urbanisation on rural labour supply.

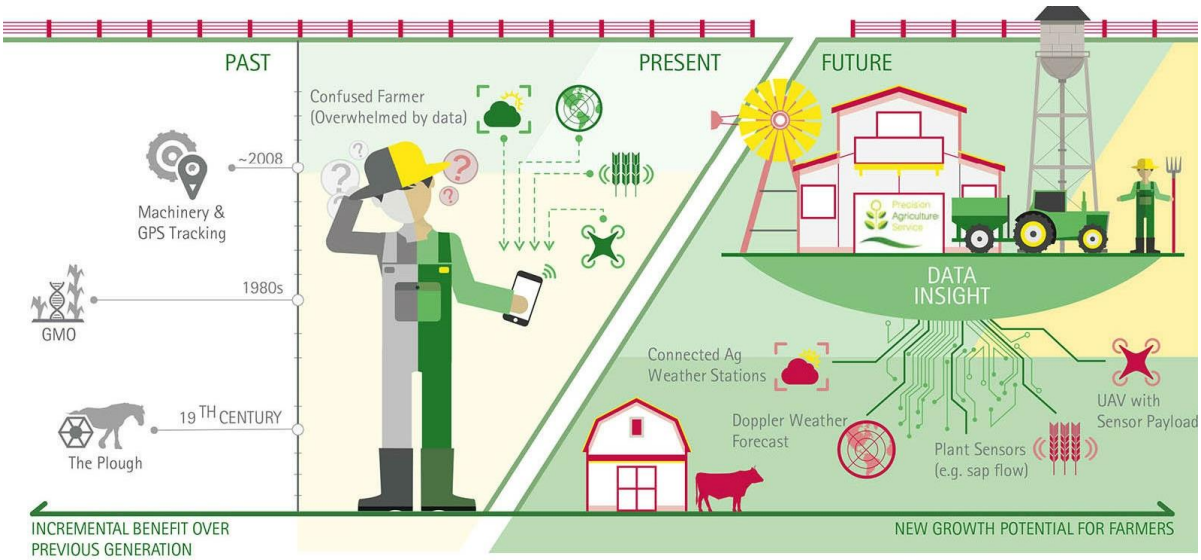
To respond to these challenges, the *Food and Agriculture Organisation of the United Nations* (FAO) calls for increased production from the same area of land while reducing negative environmental impacts - which is also a strong driver for technological innovation.

Precision agriculture: The sector's response to global challenges

As a response to these challenges, modern agriculture could be a data-driven business in which farmers generate data (e.g. through sensors in the fields, their tractors) that is analysed by service providers and fed-back to the farmer or other actors. Data-driven farming is referred to as precision agriculture or smart farming.

[231] CEMA: Farming 4.0: the future of Agriculture? See: http://www.cema-agri.org/page/global-food-challenge

Figure 19: The development of precision agriculture until today and in the future



Source: Accenture.[232]

The above figure depicts key developmental steps of agriculture from the 19th century to the present, as well as the likely future situation.

Until today, agriculture developed from an extremely labour-intensive, resource-heavy industry in which farmers mainly worked in collaborations and networks to share costs and reap collective benefits (e.g. pushing prices through collective action), to an industry that is driven by collaboration via data and networks to increase the efficiency of the production.

The aim of precision agriculture is to enable farmers to meet the demands of today's society, which is to produce more output with less input, in a sustainable manner and at affordable prices.

Thus, precision agriculture enables farmers in the future to make smart use of data produced by themselves (e.g. input data from machinery, sensors in the soil), as well as by other actors along the food chain (e.g. weather forecasts, data on pests and crop diseases). Hence, farmers make use technical tools to constantly monitor the entire farming process in order:

- To make better and more informed decisions;
- To react quicker to external circumstances;
- To react more appropriate to external influences.

The technological advance in the agricultural sector has substantial eco-friendly implications as it allows a more sustainable usage of resources and is less burdensome for the environment According to estimates of the *European Joint Research Centre*, precision agriculture could ensure a huge CO_2-reduction in European agriculture until 2030, by mitigating Greenhouse Gas emission significantly[233].

232 https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Images/Global/Digital_9/Accenture-Evolution-Precision-Agriculture-Background.jpg

233 CEMA: Farming 4.0: the future of Agriculture? See: http://www.cema-agri.org/page/farming-40-future-agriculture

An ideal farmer: Capturing opportunities digitisation offers[234]:

Klaus Münchhoff is a German farmer and owner of the Derenburg estate in Saxony-Anhalt. At a very early stage, he did realise the potential the digitisation holds for his sector and adopted many of the existing technological opportunities, like drones and automated tractors, for his farm. Because of the innovative manner Klaus is conducting his business, he can be seen as a pioneer in the German agricultural sector and therefore, he recently received the German "Farmer of the year award" in 2016.

But how did Klaus Münchhoff became a 'first-mover'?

It started by questioning himself, why the yields on the same field differ so significantly. Motivated by an interest in sustainability and an ambition to harmonise economy and ecology, he decided to change his ways of traditional farming. As a result, he adjusted his farming processes by shifting to subarea specific cultivation. In doing so, he pioneered the use of precision farming techniques already before digitisation or big data gained their present momentum.

Today, he frequently uses the data from satellites, combining it with data collected by his vehicles on the fields. Together with regular soil-analyses, he is able to dispense his resources very accurate and tailored to each occasion. As a result, he was able to reduce the environmental footprint of his work and costs at the same time, due to increased efficiency of production processes enriched by data.

However, one of the main challenges for precision agriculture is that – although relevant data, soft- and hardware, as well as other technology are available – the take-up of relevant technology can still be improved.[235]

Global size of the precision agriculture markets

In 2014, consultancy Roland Berger estimated the **global market volume for precision agriculture** at EUR 2.3 billion, of which EUR 0.4 billion were allotted to Europe.[236] Market volumes are expected to grow until 2020 at a compound annual growth rate of 12% globally and 15% in Europe.[237] Another angle towards estimating market size is measuring the costs for precision agriculture businesses (instead of the sales of manufacturers and service providers). In this vein, the *German Farmers' Association* (DBV) reported that already in 2015, 30% of the costs of agricultural machinery may be attributed to "sensors, software and other ICT devices."[238]

[234] http://www.ceresaward.de/klaus-muenchhoff-679748

[235] A representative of a software provider interviewed for this case study indicated, for instance, that an estimated 99.9% of farmers worldwide do not yet provide data to the cloud.

[236] By far the largest market for precision agriculture is found in the U.S., reaching a total volume of EUR 1.2 billion.

[237] Roland Berger (2015): Business opportunities in precision farming. Will big data feed the world in the future?, p.4; https://www.rolandberger.com/publications/publication_pdf/roland_berger_business_opportunities_in_precision_farming_20150803.pdf

[238] See Poppe, K et al. (2016): *Precision Agriculture and the future of farming in Europe. Briefing paper 4: The economics and governance of digitalisation and precision agriculture*, p. 8

More specific estimates are available for different areas of the precision agriculture market:

- Automated machinery and agricultural robots;
- Wireless sensors and network technologies; and
- Data analysis software.

Wintergreen estimated the global market size for **automated machinery and agricultural robots** at USD 817 million in 2013 and forecasted to grow to up more than USD 16 billion.[239]

Automated machinery and agricultural robots: Use case example

One application increasingly employed by farmers, for instance, are **automated milking systems**, not only collecting milk but also data during the production process. In 2012, around 10,000 farms worldwide already relied on milking robots, about 3,600 of those situated in the Netherlands alone. Significant growths are predicted for the future: For instance, more than half of Northern-European dairy herds are expected to be milked by automated systems by 2025.[240]

Wireless sensors and network technologies are also increasingly common within agricultural machinery and appliances. One of the most obvious use cases for wireless applications in agricultural machinery are tractors.

Wireless sensors and network technologies: Use case example

In Europe, around 129,000 tractors sold in 2013 were equipped with *Global Navigation Satellite Systems* (GNSS). Since then, an additional 240,000 tractors incorporating these systems for guidance and steering have been sold to European farmers.[241] On a global scale, market penetration rates of GNSS-equipped agricultural machinery is estimated to increase from below 10% in 2013 to 50% in 2023. The largest market revenue shares are expected to flow from tractor guidance applications, followed by automated steering solutions. Other growth markets are Variable Rate Technology (VRT) applications, used e.g. used to precisely dispense fertilisers at a given location or track livestock.[242]

The market for **software for data analysis** presents a number of small- to large scale solutions for farmers, operated by a multitude of small app developers[243] as well as large multinational agro-chemical and agro-technical companies (e.g. *Monsanto*, *Dupont*).

Software for data analysis: Use case examples

Evidence on potential market size and number of user is mostly available from reports

[239] Eustis, S. (2014): *Agricultural Robots. Market shares, strategy, and forecasts, worldwide 2014-2020.* Wintergreen Research Inc.

[240] See Poppe, K et al. (2016): *Precision Agriculture and the future of farming in Europe. Briefing paper 4: The economics and governance of digitalisation and precision agriculture*, p. 10

[241] GSA (2017): *Agriculture*; https://www.gsa.europa.eu/segment/agriculture

[242] GSA (2015): *GNSS Market Report*, Issue 4, March 2015, p.60; https://www.gsa.europa.eu/system/files/reports/GNSS-Market-Report-2015-issue4_0.pdf

[243] For small overview of these applications used for scouting and mapping in the U.S. market, see: http://www.precisionag.com/professionals/tools-smart-equipment/16-field-scouting-apps-for-precision-agriculture/

about the U.S. market:

- The farm record software suite *Farmobile* raised more than USD 5 billion in equity financing in the end of 2015.
- *Google Venture*'s *Farmers Business Network* (FBN), one of the largest agricultural cloud-providers, has aggregated data from 7 million acres of land, across 17 states (including performance data on 500 different seeds and 16 different crops).
- *Fieldscripts* by *Monsanto* started its testing period with 150 corn farmers cultivating a combined 400,000 acres in four U.S. states in 2014 and has since then expanded operations to other crops like soybeans, and multi-hybrid plants.[244]

Structure of precision agriculture markets

The US (precision) agriculture market differs from the European. Most importantly, US farms are often larger in size and revenue as their European counterparts which simultaneously can be expected to decrease the magnitude of capital expenditures necessary (e.g. per acre) to invest in precision agriculture machines and appliances.

Consequently, in the EU, precision agriculture machines and appliances are much less purchased by individual farms but much rather by affiliated cooperatives (i.e. larger networks of farms) or neighbouring farms in order to decrease investment costs.

Nevertheless, significant numbers of farmers also already use business management systems to improve their internal business operations or exchange data with other actors. A recent report mentions, for instance, indicates that half of Dutch large and medium-sized arable farmers (with 20 acres and more) already use these software systems.[245]

Still, **precision agriculture technology adoption** in Europe varies by regions: In Northern European countries, farmers have been observed to adopt new technologies faster than their Southern European counterparts. Blackmore et al. attribute these difference to:

- Larger economic farm sizes;
- Higher incomes;
- Ability to financing new investments;
- A role understanding of farmers as entrepreneurs; and
- State policies (depending on the country). [246]

Additional factors that influence the adoption of precision agriculture technology are mobile internet network coverage.

[244] See: http://www.monsanto.com/sitecollectiondocuments/overview-of-integrated-farming-systems.pdf; the development of the trials has so far not been disclosed.

[245] See Capgemini Consulting and Wageningen UR (2016): *Cybersecurity in the agrifood sector. Securing data as crucial asset for agriculture;* https://www.wur.nl/upload_mm/4/6/a/f74a893e-c829-4bf3-9884-e357929ff5d6_Cybersecurity%20in%20the%20agrifood%20sector.pdf

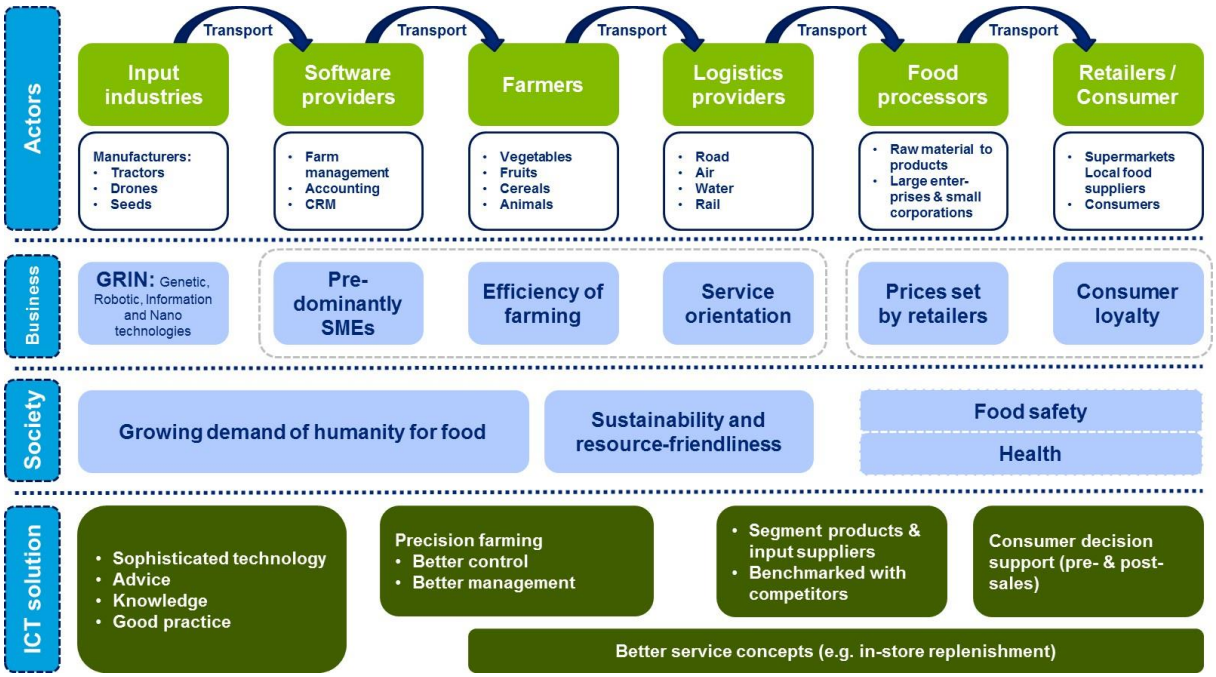
[246] See Blackmore in Poppe, K et al. (2016): *Precision Agriculture and the future of farming in Europe. Briefing paper 4: The economics and governance of digitalisation and precision agriculture*, p. 11

Market participants and technical solutions available

Precision agriculture market participants

The following figure presents an overview of the actors involved within the precision agriculture food chain, as well as the current challenges for businesses and society that precision agriculture aims to overcome by means of technical ICT solutions.

Figure 20: Business and societal challenges and their ICT solution in the food chain



Source: Poppe et al. (2013)[247], adaptation by Deloitte.

As can be seen above, the food chain involves not only farmers but also e.g. input industries (such as equipment manufacturers and producers of seeds and crops), logistics solution providers (e.g. transport companies), and retailers (e.g. supermarkets).

Collaboration and data exchange along this food chain is needed to enable businesses to tackle societal challenges: To make the development and provision of food more efficient, sustainable, and resource-friendly.

As depicted above, within precision agriculture, there are different types of actors active along the data value chain. These actors have different service offerings and are mostly active on the supply side of the data economy.

Technical solutions in the market

Most of the technical solutions relate to the management of crops and animals to achieve better productivity and quality.

[247] Poppe, KJ, Wolfert, S, Verdouw, C Verwaart, T (2013), Information and communication technology as a driver for change in agri-food chains, *Eurochoices*, vol. 12, issue 1.

In this vein, the key technologies and concepts that are offered by the different actors can appear in diverse forms. The most common technical solutions that are currently taking over the market are:

- High precision positioning systems;
- Automated steering systems;
- Geomapping;
- Sensors and remote sensing;
- Integrated electronic communications; and
- Variable rate technology (VRT).

High precision positioning systems (like GPS) ensuring highest levels of accuracy during characteristic farming processes, by providing the unconditional and independent navigation services. To record the position of farm vehicles, geographic coordinates are gathered by satellites or drones.

Automated steering systems are the key to effective site management by delegating specific driving tasks to the machine itself. These systems are available in three different forms: Assisted steering systems (driver's action still needed), automated steering systems (driver can take hands off) and intelligent guidance systems.

Geomapping is used to develop intelligent maps which include information about soil type, nutrients levels et cetera, assigning that to the particular field location.

With the help of Sensors and remote sensing farming relevant data can be collected and evaluated from a distance. The data collecting sensors can thereto be placed on moving machines.

Furthermore, integrated electronic enables the communication between components of the farming process, for instance between the farm office and vehicles or other tools while operating, while variable rate technology (VRT) holds the ability to adapt parameters on machines for precise applications of seed or fertiliser[248].

A few examples of what different actors contribute to the food chain depicted above are provided below:

- Regarding crops, specialised service providers provide improved ways to monitor the status of crops by generating new data and analysing them;
- Manufacturers of drones let their products take photos of fields to improve fertilisation. Such businesses typically own the data and analyse them to provide value added services to farmers;
- Providers of Wi-Fi sensors monitor the status of crops and analyse these data to help farmers increase production and quality[249]; and

[248] CEMA: Farming 4.0: the future of Agriculture? See: http://www.cema-agri.org/page/precision-farming-key-technologies-concepts

[249] For instance, precision agriculture can also serve as a means to reduce the waste of irrigation water by collecting data on soil conditions and plant needs in order to selectively water different plots of land. European pilots for such systems have shown that the waste of irrigation water can be reduced by 40%. See: http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf

- Software companies provide cloud based management platforms to which farmers can upload data generated by them on their calf and crops, such as health, growth and production. The data is analysed and managed by the platform.

Types of data generated and used by different actors

Looking at the types of data provided by and exchanged between businesses, four main types of actors can be distinguished. These actors provide different types of data (see the table below).

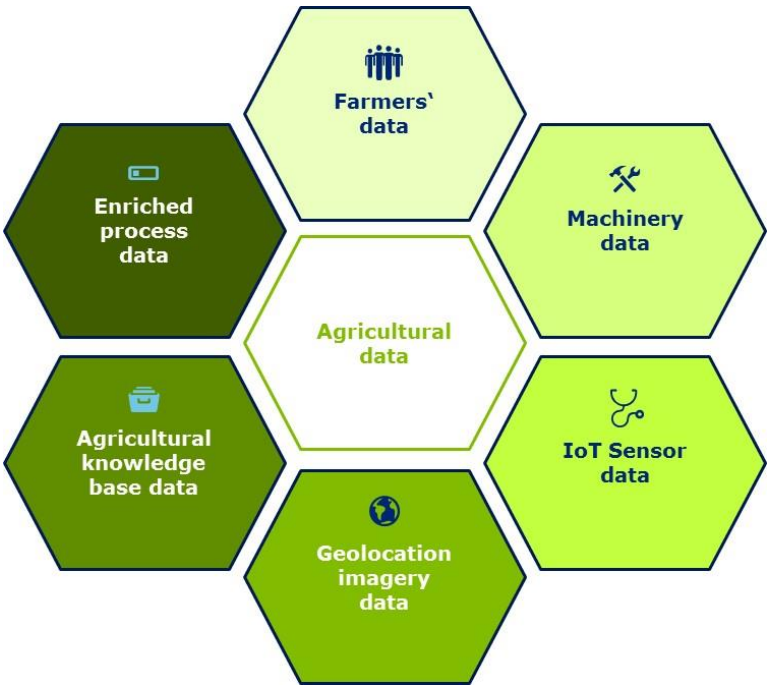
Table 21: Types of actors along the data value chain and their respective contributions to it

Type of actor	Contribution to the data value chain
Farmer	Farmers generate data through their field activities, incl. e.g. tillage, planting / seeding, spraying, fertilising, and harvesting. The data is generated by the machines used for these tasks, as well as from sensors deployed e.g. in the soil.
(Manufacturers of) farming machinery and equipment	In addition to farming data, data is generated by agricultural machines on their operation incl. e.g. maintenance and repair needs. This data is relevant for both the farmers' field activities, as well as for the manufacturers themselves that want to improve the performance of their machines.
Third-party providers of agricultural data	Third-parties provide external data based on the geolocation of the fields incl. e.g. weather forecasts, GPS data concerning geo-locating, tracking of equipment and machinery, satellite imagery, data on pests and crop diseases.
Vendors of agricultural technology	Software firms provide solutions by means of which farmers can collect and analyse the data above and process it through algorithms. These algorithms create the added-value of the data for the farmer who is able to track his assets' performance in a graphical way e.g. by means of dashboards.

Source: Deloitte

These different types of actors along the data value chain, as well as their respective data contributions are closely connected – building on each other with a view to providing added value in relation to farmers' and other involved businesses' needs.

Figure 21: Types of data within precision agriculture



Source: Deloitte

Software providers, for instance, use several data sources to provide added value:

- **Manually generated input data** from farmers, e.g. on types and quantity of seeds, machines, assets which are, in principle, owned by the farmer: This data is used to track and monitor farmers' input and is presented to the customer in a user-friendly format, e.g. via dashboards, as well as data bases for further analysis;
- **Automatically generated data** regarding weather forecasts purchased by the software provider from a third-party company. The software provider owns the data through its purchase. The data are used – together with location data relating farmers' field – to provide micro weather forecasts for the fields themselves instead of for larger areas;
- **Information based on aggregated data** provided by farmers, as well as purchased data from third parties, e.g. early warning systems regarding pests and crop diseases. Such information based on analytics is owned by the software provider; and
- **Information on agricultural good practices** ("knowledge-base") derived from analytics of farmers' aggregated data. Agronomists employed by the software provider develop this database. The information contained in this database can be consulted by the farmers and is owned by the software providers.

Hence, precision agriculture is based on data purchased and received from different types of actors along the food chain. The immense potential variety of data generated for one single task performed is illustrated by the case of dairy robots: Robotic milking generates data in

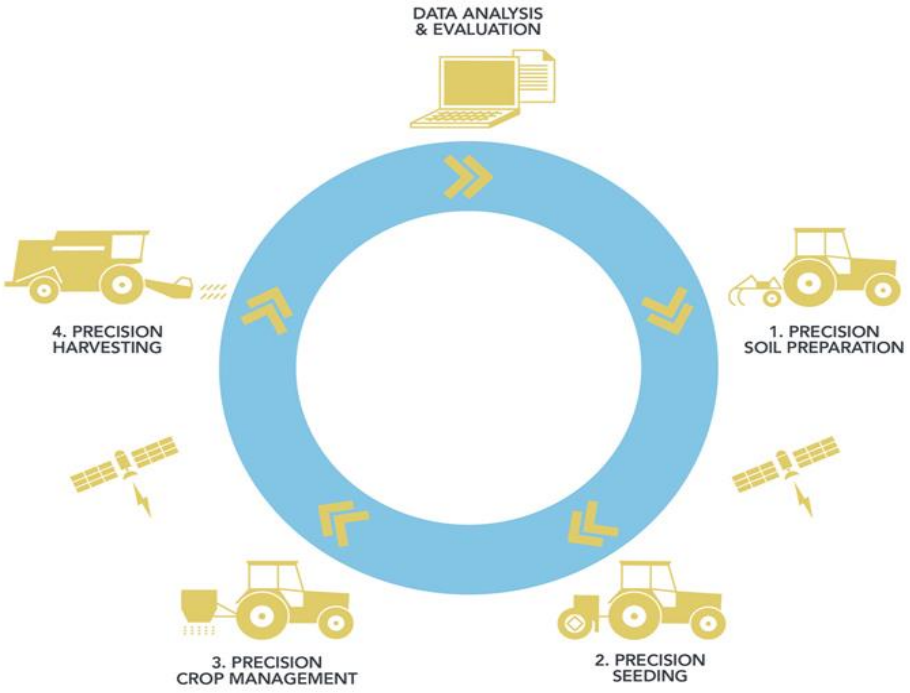
relation to roughly 120 variables per cow and day. These range from frequency of milking to milk components and quality, or cow health and reproductive activity.[250]

Business model and actors: A typical service offering

The types of business models

Precision agriculture generally involves a multitude of business models that relate to the different stages of the farming process (see figure below)

Figure 22: Precision farming innovations in the four steps of the crop growth cycle



Source: CEMA.

At each stage of the farming process (soil preparation, seeding, crop management, harvesting and data analysis/evaluation), technical tools are incorporated that generate and use data.

Precision agriculture is enabled by the collaboration of different types of actors and the integration of their services. There are, for instance:

- Manufacturers as the providers of the of the technical tools like drones and sensors;
- The farmer itself, who needs to buy and use the tools and technology; and
- The data analytics company which handles the collected data and provides the farmer with a substantial feedback.

There are several business models[251] that illustrate how precision agriculture actors collaborate and how they can earn money.

[250] Lee, K. (2015). *Management decisions enhanced with robotic milking data*. March 31th 2015. See: http://www.progressivedairy.com/topics/management/management-decisions-enhanced-with-robotic-milking-data

- Innovative services based on open data;
- Basic data sales as a commercial alternative to open data (e.g. *FarmMobile*, *MySmartFarm*);
- Product innovation, mostly by the agricultural machinery industry to connect their products and make them *smart* (*John Deere*, *Claas* etc.);
- Commodity swap of data (i.e. the exchange of data for data) between farmers and between farmers and the supply chain (up- and downstream), e.g. (food) manufacturers;
- Value chain integration (such as *Monsanto*'s *Fieldscript*); and
- Value net creation (i.e. a pool data from the same consumer, see *AgriPlace* for instance).

The sales strategy of farm management software providers

In terms of sales strategy, providers of **farm management software**, for instance, offer their software as a service to farmers via monthly subscriptions.[252]

The reason for this decision is that providers of farm management software, on the one hand, play an intermediary role between the different types of actors in terms of data exchange. In that sense, providers of farm management software can also be seen as a data hub that collects and analyses data of different actors in order to make them usable for other actors. On the other hand, farm management software is an example of a service that all actors along the value chain use: Visualisation of data in order to understand it and to be able to draw conclusions based on the data collected and analysed.

There are clear boundaries with regard to the access to and (re-) use of farmers' data within the EU. The **privacy of the data must be ensured** by service providers, i.e. data must not be used for aggregation nor by third parties without prior consent of the farmer.

Therefore, software providers may, for instance, provide **different types of service offerings** to its clients. This could, for example, take the following form[253]:

- *"Small" solution:* Affordable for all customers, basic functionality of the software, farmers give their consent that all data may be aggregated and used for other services provided to third parties;
- *"Medium" solution:* Medium pricing, increased functionality of the software compared to the "small" solution, farmers give their consent that certain data may be aggregated and used for certain other services provided to certain third parties; and

---

[251] OECD: Big opportunities for big data in food and agriculture, see: https://www.oecd.org/tad/events/Session%202_Krijn%20Poppe%20OECD%20Big%20Data.pdf For further information, see: Arent van 't Spijker: "The New Oil - using innovative business models to turn data into profit", 2014

[252] This business model (i.e. offering subscriptions to software) is a very common sales approach within the precision agriculture market. While larger market players tend to apply different business models (e.g. selling proprietary software to large clients), smaller firms tend to offer monthly subscriptions as a means of maintaining customers' freedom of choice regarding the types of services and the service providers.

[253] The three pricing solutions below are only illustrative based on desk research and interviews with businesses. It seems that such pricing solutions are fairly common. However, businesses were not willing to disclose their typical contractual clauses in for such models so far. It can, however, be assumed that one general rule applies: The less you pay, the more data can the service provider access and (re-) use for its own business purpose (i.e. not only improvement of provided software and maintenance etc.).

- *"Comprehensive" solution:* High pricing, full functionality of the software, farmers keep complete ownership of their data (e.g. in a private cloud solution) with no aggregation and use for services to third parties.

In practice, giving consent to data aggregation and use for services offered to third parties is done by the farmers through accepting the software providers' Terms & Conditions as part of the subscription process. In this respect, transparency of the subscription process, as well as farmers' interest in what the software provider does with the data is crucial.

A typical client for software providers in precision agriculture:

Typical clients of such software providers are, for instance, medium-sized farms run as family-businesses with the help from seasonal workers. Such a farm could, e.g. grow organic crops such as lemons, citrons, and oranges sold to local supermarkets, as well as to international retailers across different Member States.

Obviously, farmers have to concentrate on their **"primary" tasks**, i.e.:

- Soil preparation;
- Seeding;
- Fertilisation;
- Crop management;
- Harvesting; and
- Supplying to other actors along the food chain.

This is done by using technical equipment such as tractors, sensor systems, soil scanners, drones and similar equipment making use of e.g. geo-location data provided by satellites.[254] However, this involves not only the physical *growing* and *harvesting,* but also dealing with weather forecasts, as well as combating pests and diseases.

Moreover, typical challenges for such farmers also include the **"secondary" management** of their farm, including, amongst other things, paper work regarding administrative obligations, accounting and financial planning of input and output, as well as dealing with contractual issues.

Farm management software helps farmers **carry out these "primary" and "secondary" tasks more efficiently** by enabling farmers to monitor input and output in an efficient and easy to use manner, as well as to make use of information (e.g. good practices) for business decisions that is developed based on (real time) data of other farmers. Farmers who want to use such farm management software could, for instance, register on the software providers' website and can instantly use their existing platform. This platform provides the possibility to input and analyse different types of data, as well as to make use of third-party data for farmers' operations.

[254] See e.g. data provided by the European Space Agency a spart of ist SENTINEL program: http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Overview4

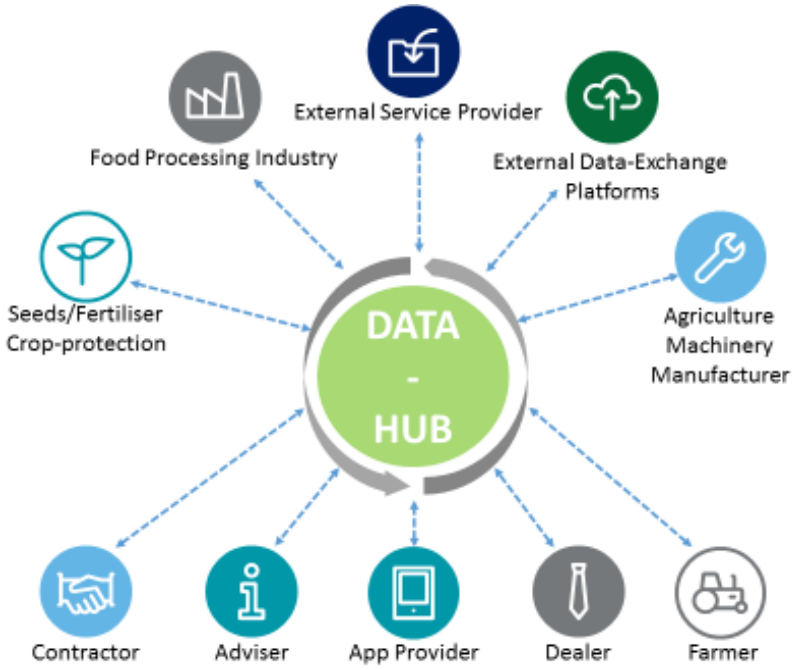
Example of shared data management infrastructure: Data-Hub

Fluent and unrestricted data exchange has so far been a complicated issue to the stakeholders in the agricultural sector. Because of different standards the various products and software have, compatibility was rarely given.

The German company *DKE Data* developed a data hub in order to facilitate the communication and exchange of data between actors along the value chain. The programme is going to be introduced at the *Agritechnica* in March 2017. Data-Hub aims to enable interoperability among the different actors within the agricultural sector by delivering a comprehensive and standardised tool which ensures safe and compatible ways of data transport.

The use of this new tools is free of charge for farmers and other agricultural operators as it is funded through the contributions of manufacturers, app-developer and other service providers.

Figure 23: Communication between actors with Data-Hub



Source: DKE Data, graphical representation by Deloitte.[255]

Potential contractual barriers

This section provides a brief analysis of potential contractual barriers, businesses in the precision agriculture sector may face. So far, this analysis is, however, not based on actual contracts used in the area of precision agriculture, as these are not yet available, apart from the contractual terms of the company John Deere.[256] The section first discusses contractual bar-

[255] See: http://www.dke-data.com/whatwedo/innovation_datahub/

[256] See: https://www.deere.es/privacy_and_data/policies_statements/en_US/data_principles/data_principles.page and https://www.deere.es/privacy_and_data/privacy_and_data_services_subscriptions_data_policy_cis_int.page

riers related to data ownership, access to, and (re-) use of data. Then, risk and liability are discussed briefly. Finally, the section includes a high-level assessment of the potential economic impact of such barriers.

Data ownership

As can be derived from the bullet point list above, **ownership of data is spread across different types of actors** within the precision agriculture value chain, with service providers generally omitting the issue of data ownership in their Terms & Conditions.

From a **legal perspective**, rules on data ownership have emerged only recently but so far focus on the context of individual privacy. In general, no (intellectual) property rights are attributed to farmers' data. Instead, as all non-public data, agricultural data may be either protected:

- By *privacy rules* (e.g. when the data contains personal information)
- As *confidential information* (e.g. business information, trade secrets); or
- By *database rights* in the EU (under Directive 91/250/EEC)

Only some agricultural companies offering hard- and software solutions for precision agriculture treat collected data as personal data of the respective farmer.[257] In practice, protection is lost if data is disclosed or reported to public bodies (like ministries and government agencies), which is often required by law. Thus, contract law between farmers and businesses presently determines for each service or product, whether the farmer owns the data. This may prevent the parallel use of (additional) services by farmers, thereby impeding the future development of new services. **In practice**, automatically generated data is generally owned by the party that purchases the data, e.g. in case of data on weather forecasts, the data is purchased by a software provider and transformed into an easy-to-use application for farmers.

Input data is generally owned by those who create the data (e.g. by farmers) – unless they alienate their ownership as part of the use of services based on data. This position has also been supported by manufacturers of agricultural machinery: For example, the *German Agricultural Machinery Association* (VDMA) demands that the end customers (as the producers of data) remains free to choose:

- Which data is submitted;
- How long it is stored; and
- With whom they wish to exchange their data.

At the same time, they stress the importance of exchanging data through platforms and interoperable systems.[258] Hence, the contractual agreements with a provider of soil sensors might foresee that the data collected from farmers may also be used in an aggregated, anonymised way to provide data services to other clients than farmers, e.g. manufacturers of tractors or seed producers. One farmer interviewed by Deloitte pointed to a possible need to reconsider who has to give consent to this type of data generation and (re-) use, when it is

[257] See Poppe, K et al. (2016): *Precision Agriculture and the future of farming in Europe. Briefing paper 4: The economics and governance of digitalisation and precision agriculture*, p. 33

[258] Agricultural Machinery Association Germany (2016): *Agriculture 4.0 - Understanding, Goals and Need for Action, from the Perspective of the Agricultural Machinery Industry*, Position 15/2016.

conducted on leased land. In addition, he identified a need for further clarification concerning datasets that merge data across several fields (possibly owned by different farmers or landlords). Therefore, data **ownership is not a problem *per se*** but it always depends on the recipient of the information and the products or services the data are (re-) used for, as well as on the remuneration of data generators.

Hence, the **access to, the benefit generated from analytics and the use of the data** is key, much rather than data ownership.

Access to and (re-) use of data

As part of the interviews carried out in relation to this case study, stakeholders have emphasised that data ownership is a problem in case the information generated by farmers is used by third parties to provide services to other actors along the value chain (e.g. equipment manufacturers) that use this information to develop products detrimental to the farmers' interests. Detrimental use can, for instance, lead to adverse pricing effects of data exchange between actors.

Farmers produce large amounts of data on soil preparation, seeding, fertilisation, crop management, and harvesting. This data is transferred to the software provider who analyses the data and transfers it back – e.g. in the form of visual tools such as dashboards – for farmers' own use. Such information for farmers is often paired with third-party data on weather forecasts, pests, and crop diseases, and aims at enabling farmers to take better decisions concerning the operation of their farm.

However, software providers often include – as part of their general terms and conditions – clauses that indicate that the data provided can also be used for other purposes than feeding it back to farmers for their operational purposes. This means that data can, for example, be anonymised and aggregated in order to provide third parties – for instance large providers of seeds – with information on farmers' yields and crop efficiency.

On the one hand, this may lead to farmers having more effective and efficient seeds that can be used to maximise yields. On the other hand, however, seed providers may also use the transparency of the market, created through the information provided by farmers, to predict yields in different geographical areas that, in the end, can influence global market prices for crops.

By analogy, insurances and commodity markets might also be radically changed using inferences from aggregated past observations. While price mechanisms in these markets might benefit, it could also be to the disadvantage of small farms especially prone certain business risks. Taken together, this may put prices for crops under additional pressure, endangering farmers' economic wealth of farmers and food supply to societies.

Practical example for the access to and (re-) use of data:

A German farmer reported that local conditions (e.g. micro-climate, soil-characteristics, etc.) vary in a multitude of parameters. This requires specialised knowledge on the side of the individual farmer about the unique conditions at hand – statistical information based on partially similar conditions would be of little help. Thus, the farmer indicated in con-

trast that farm software providers' business model (especially the data behind) is – from his perspective – much less attractive for farmers than it is for third parties that are trying to provide new, added services to farmers. The farmer exemplified this by the farm management software 365FarmNet that is partially owned by the Allianz Insurance Group. Within this software, farmers are asked to upload their insurance contracts in order to be able to manage them *in one spot*. Such data is, of course, of value for an insurance company. Thus, the farmer is put in a situation in which he also provides his data to a company that is only remotely related to the core of agriculture – mostly without even knowing.

Moreover, a situation in which farmers' data are used against their own interest could arise in case farmers do not receive a remuneration for the provision of their data to service providers – which is generally the case today.

This is a **problem of collective action**:

- It is rational for the individual farmer to make use of data based services e.g. to improve their own farm's yield and make the farm's operations more efficient.
- From a collective action perspective, however, it may be irrational to provide firms with the data, as the aggregated data of many individual farmers may be used against the interests of the collective.

In that sense, individual rationality can turn into collective sub-optimal outcomes in case a regulatory regime governing the exchange of data is missing. Such a regulatory regime could focus, for instance, on minimum requirements of terms and conditions, and contracts regarding the remuneration of farmers that transfer their data to service providers who can then use the data to sell services to third parties.

It has also been emphasised as part of the interviews conducted for this case study that there is a general **lack of awareness amongst farmers** that they are – in the absence of a regime governing the exchange of data – giving away their assets (i.e. their data) free of charge. This is partially due to remaining dominance of traditional farming today and the focus of farmers on their daily operations, as well as due to the **lack of experience in *valuing* data in terms of money**.

In relation to the (re-) use of data, there is an increasing **interest from public bodies** in the data generated manually by farmers. Public bodies may use the information, for instance, to keep track of production and consumption, as well as to develop mechanisms to predict pests and crop diseases.

Practical example: Business Data Principles applied by John Deere

John Deere differentiates business data between machine, production and other data.

- Machine Data generally relates to how your equipment is functioning. Examples include fuel consumption, implementation, basic crop category, bale counts, machine health indicators, vehicle diagnostic codes, and engine performance.
- Production Data generally relates to the work you do with the equipment and the land on which the work is performed. Examples include field task details, crop variety, trees or crop harvested (yield), and agronomic inputs applied.
- Other Data are data that we identify for special handling. Examples include variable rate prescriptions, user-entered notes, and user-formatted reports.

The company also uses these types of data to improve their "products, services, and business", e.g. by means of sharing it with data service providers based on the consent by users (e.g. farmers). For this purpose, machine data is used in both original and anonymised forms while production data is only used anonymised. Other data is not used "beyond what is necessary to provide a service and administer an account."

Machine and production data may be disclosed to affiliates, suppliers and service providers in order to perform business operations. In addition, John Deere may offer or sell information services derived from anonymised Machine or Production Data to non-affiliates and other parties.

The table below provides a brief overview of the types of data John Deere collects based on their Customer Business Data Type Inventory. [259]

Machine data (used original and anonymised)	Production data (used anonymised only)	Other data (used for account management)
• Vehicle/implement controller diagnostic readings & recordings • Vehicle location, altitude • Vehicle performance, settings and diagnostic trouble code event data for the following vehicle systems: Engine, Powertrain, Electrical, Hydraulic, Hitch/PTO, Operator station • Working tool/attachment performance, settings and diagnostic trouble code event data • Production system performance, settings and diagnostic trouble code event data • Self-propelled vehicle production system payload weight data • Vehicle usage states and cycles • Maintenance event logs	• Production system crop and product identifiers (seed variety, product formulation) • Production system target rates/depths (seeding, applications, tillage, etc.) • Field/worksite boundaries • GPS Guidance lines • Production system as-seeded/planted rates, as applied rates, as-tilled depths and as-harvested moisture/yield/constituents • Detailed production system settings levels, tank levels and performance data (combine harvester header/separator/ grain tank, forage harvester header/processor, sprayer tank/boom, planter/seeder tank/row unit, tillage gang) • Detailed environmental readings (temperature, humidity, wind speed, soil moisture, etc.) • Task plan/job plan/work plan/work order referenced setup and output data inclusive of data above • Machine productivity and performance data – measures how well machines perform compared to a baseline – includes vehicle usage states, cycles, and fuel efficiency	• Variable production system target rates/depths (variable rate prescriptions) for seeding and applications • Operator-entered notes • Forestry production data files as defined by the industry standard "Standard for Forest machine Data and Communication"- includes species identifiers, volumes harvested, and other information • Forestry production target settings and bucking or cutting instructions • Construction grade control design and as-built files

[259] See: https://www.deere.es/privacy_and_data/docs/DataTypeInventory.pdf

Risk and liability

With regard to **risk and liability in the B2C context**, it has been argued as part of the interviews that the purpose of data exchange is to improve the performance of the actors along the data value chain. As concerns farmers, this means that business decisions around soil preparation, seeding, fertilisation, crop management, harvesting, and supplying to other actors along the food chain can be based on increased knowledge through real-life evidence. Most importantly, however, farmers can still take deliberate choices, i.e. they can base themselves on data e.g. visualised through a software provider, but **the sheer existence of such a software solution does not relieve farmers from the responsibility for their own decisions**.

In the **B2B context**, precision agriculture businesses themselves are able to work out individual liability regimes through their contractual arrangements under the 1985 Product Liability Directive (PLD).[260] In liability cases, also in precision agriculture, the general principles of liability allocation[261] apply:

- Joint and several liability of all operators in the production chain in favour of the injured party; and
- Burden of proof that a damage was caused by a certain defective product is on the consumer / the farmer.

This means that a liability regime governing B2C situations is already in place while B2B relationships are governed by individual contracts between suppliers along the value chain.[262]

On this basis, consumers and manufacturers can resolve their liability case, either bilaterally through compensation or in court. Such cases, however, seem to be seldom in practice. In case the manufacturer is paying compensation to the consumer, the manufacturer can claim compensation from his suppliers under the Product Liability Directive. **Essentially, the B2C liability claim is passed on B2B along the supply chain of a given product**.

From the perspective of farmers, this liability regime remains hard to enforce: In a stakeholder interview, one farmer confirmed that claims directed at a business are usually passed back and forth the addressee and other businesses involved. In any case, the farmer reports to feel liable for his decisions and actions regardless of the underlying legal regime. As an entrepreneur, any farmer ultimately needs to rely on own routines to prevent errors and ensuing damages.

Interest associations acting on behalf of machinery manufacturers reported that their members are so far most concerned about product safety: When thinking about damages and liability, their prime concern is to prevent injuries to or deaths of humans. Other cases are so far perceived to entail smaller potential impacts. Concerning contracts for autonomous sys-

[260] Directive 85/374/EEC on liability for defective products. See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN

[261] See the Product Liability Directive: Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN

[262] So far, businesses were not yet willing to disclose their B2B contracts, in particular in cross-border situations. It can, however, be assumed that the contracts applied vary from product to product. On the contrary, it seems contracts are similar across borders as businesses seem to apply common contractual terms and conditions for all businesses (see the example of John Deere above).

tems, no specific liability clauses were mentioned. Instead farmers are assumed to be liable for damages resulting from their operation.

To stop an ***infinite regress of claims***, businesses in practice tend to preclude liability as part of their contractual agreements. Businesses seem to rely much rather on connected sensors, equipment, and devices etc. being capable of ensuring that their products are able to check and recognise the validity and correctness of the data transferred to them by other connected sensors, equipment, and devices, etc. (see also the following section on technical barriers).

As part of the interviews conducted for this case study, stakeholders have argued that liability issues may not only be resolved through legislative action and the enforcement of given rules. The prevalence of liability issues is also subject to market mechanisms that also drive the take-up of interoperable solutions in the area of IoT (see the text box below). For instance, one interest association representing manufacturers of agricultural machines stressed that policy intervention at this stage would even slow down the current move towards industry self-regulation.

Market mechanisms driving developments regarding risk and liability issues:

Although liability claims will always arise in practice, consumers will, over time, choose products that have proven to be unlikely to cause damages. In the area of precision agriculture, for instance, providers of unreliable weather forecasts will not be successful on the market, as well as providers of soil sensors that collect incorrect information on the level of irrigation of fields. Therefore, it has been argued that, in the end, liability may be very important in individual cases only.

Moreover, precision agriculture – as well as IoT in general – are relatively new developments for which take-up by businesses and consumers alike is likely to grow over the coming years.[263] The full potential of the technology is neither achieved already, nor is it known by when it will be.

Therefore, it has been argued that the technology and the respective markets should develop further before current barriers, that may be unlikely to still exist in the future, are addressed by (legislative) means that would themselves pose challenges and barriers in the future – depending on in which direction the market is heading. As part of this argumentation, the development of IoT has been compared with the development of the Internet itself in the 1990s and 2000s – with particular focus on the benefits that the absence of (premature) legislation has brought about for the technology, consumers, and businesses alike.

Potential economic impact of contractual barriers

Apart from the possible adverse pricing effects of data exchange between actors and the market mechanisms driving developments regarding risk and liability issues (see text boxes above), contractual barriers may have positive and negative impacts, depending on the time horizon under analysis, as well as on the type of stakeholders along the data value chain.

[263] One interviewee indicated that 99.9% of farmers worldwide do not use precision agriculture.

From a theoretical point of view[264], the contractual barriers identified may provide short term benefits for all businesses along the data value chain. The reason for this is that new services and products are being developed and marketed, which enables firms to make businesses to generate turnover with each other. This may provide direct revenue for service providers, as well as indirect revenue for service users through the realisation of efficiency gains in their operations. GDP growth is one of the main results of such a development.

In the long run, however, it could be argued that – while some of the farming companies on the side of the service users are generating more profit at a faster pace (i.e. work increasingly efficient) through the use of precision agriculture – the large majority of firms that cannot (yet) bear the necessary capital expenditures could have an increasingly competitive disadvantage. As a consequence, monopolies could arise in certain markets (in particular across borders) or incumbent businesses could strengthen their current position vis-à-vis potential competitors. Although such a situation would still contribute to GDP growth, it could be argued that this could happen on the expense of farmers that are not (yet) as advanced as others. In other, more extreme, words, while precision farming could lead to economic benefits in the short run for all businesses involved in the data value chain, it could also lead to long term detriment to the agriculture sector as such, with service providers being able to steer market prices and large cross-country farmers ruling the existing and/or evolving markets. Thus, solving existing contractual barriers could, from an economic perspective, give leeway for growth in the short run while creating and imposing other barriers on businesses (especially SMEs) in the long run. Careful governance and involvement of all types of actors in policymaking is, therefore, crucial.

Technical and other barriers

Interoperability is one of the most important enablers for the precision agriculture market, both in the B2C and the B2B context.

B2C interoperability

In the **B2C context**, software providers can ensure access to and (re-) use of data through the use of an **interoperable** solution – OpenAPI, a vendor neutral description format[265] - which enables farmers to transfer the data they receive from the software provider to any other software they want to use, e.g. Excel or other data analysis software provided by third parties.

The use of vendor neutral description formats is one of the most important market trends – not specifically for precision agriculture but across all types of industries.

There are two distinct views on the development of interoperable solutions:

- The market-driven point of view regards interoperability – or much rather the lack thereof – as temporary barrier that will resolve itself over time as interoperability is developing into a sales argument towards customers; and
- The more legalistic point of view focuses on patents and intellectual property rights and emphasises that, so far, only very few exceptions have been granted under na-

[264] Meaning that, so far, no evidence was identified to support this argument.
[265] See: https://openapis.org/

tional law to access data inside proprietary software which leads to reduced interoperability and freedom of choice.

The market-driven point of view

In the B2C context, interoperability improves customer experience[266] and is therefore crucial to the success of products on the market. This is due to an increasing number of actors along the data value chain – especially SMEs and consumers – generally reluctant to commit themselves to only one service provider. As a consequence, service providers that do not provide for interoperable, vendor neutral description formats will – in the medium run – face challenges regarding their customer base and, most likely, be pushed out of the market (e.g. through competition or through acquisition by larger market players).

In the current situation, larger software providers do not always use open APIs for their products and services but rather proprietary software that is not interoperable with other firms' offerings. However, an increasing number of larger firms realises that this can cause problems in the future.

Therefore, these firms start to purchase smaller, open API-based companies in order to provide for both proprietary and interoperable software solutions, depending on the clients' needs.

It has been argued in the interviews for this case study that this trend could lead to a market concentration in the future, with a relatively small number of larger market players that absorb smaller businesses. As a consequence, farmers could face a situation of decreased freedom of choice, as well as increasing prices by software providers.

Therefore, the lack of interoperability of products and services is not only a barrier for the businesses that sell non-interoperable products and / or services, but also an impediment to the development of the IoT market as such.

The legalistic point of view

Patents and intellectual property rights[267] are a relevant factor to consider in relation to interoperability and innovation as they may have conflicting impacts on the market:

- Patents help to induce an environment fostering innovation through continued investments in technologies; and
- Patents restrict access to data inside the software if it is protected by technical measures like use of encryption, proprietary data transmission and storage protocols or absence of export interfaces.

[266] This means that, for instance, newly purchased devices by a certain manufacturer can be used with already purchased hard- and software from other providers

[267] Between 2010 and 2014, 5,337 new patent registrations related to agricultural equipment (precision and conventional) have been recorded worldwide. These concern, among others, sensor technologies, automated machinery or autonomous and guided driving vehicle technologies (for harvesters or mowers). More than 70% of patents were filed in the U.S., another 15% in Europe, see Poppe, K et al. (2016): *Precision Agriculture and the future of farming in Europe. Briefing paper 4: The economics and governance of digitalisation and precision agriculture*, p. 34

In the European Union, circumvention of these restrictions aimed at free transfer of data or the change the underlying software may be prohibited under Directive 2001/20/EC *("2001 EU Copyright Directive"*), unless national law provides exceptions. So far, these exceptions appear to be few and relatively static, as Poppe et al report. [268] This situation has two relevant implications for farmers:

- *Reduced interoperability*, i.e. when protocols and formats used in software are proprietary and thus incompatible with other software, or even completely lack export interfaces altogether; and
- *Reduced choice of software for machinery* i.e. future options to choose from once a certain model or brand of machinery has been purchased (even if its software does not include desired functions offered by competitors).[269]

From the **perspective of farmers**, this may present farmers with the need to manually transfer data between two software suites via manual data entries, or force them to buy and use a third software that facilitates this conversion and exchange. These solutions raise costs, and time needed to maintain databases while increasing possibilities for errors or down times.

Practical example for interoperability issues:

During stakeholder interviews, one affected farmer provided an illustrative example for the situation described above: His tractor came with a brand-specific infrastructure of transmitters set up around his farm that processes (open) GPS signals into a proprietary location signal with higher precision. The harvester he owns (from a different manufacturer) is by default neither able nor licensed to use this enhanced location signal.
Thus, he had to use a third party service to (legally) modify the receiver from the tractor to be able to transfer and install it in either vehicle.
In addition, he was not able to export all data from his machinery to his office (i.e. his farm management software).
Thus, he concluded, even the newest devices and machinery are not necessarily designed to enable smooth exchanges. He identifies a need for more possibilities to negotiate specific contractual clauses that refrain from restricting one service to one specific product.

From the **perspective of manufacturers and software developers**, these barriers may not only result from deliberate business decisions. Instead, rapid innovation may lead to a diversity of protocols, applications and IoT sensors.

[268] Poppe, K et al. (2016): *Precision Agriculture and the future of farming in Europe. Briefing paper 4: The economics and governance of digitalisation and precision agriculture*, p. 29

[269] In the past, farmers have expressed concerns that they do not have the right to modify, change or even update software in tractors or agricultural robots as they wish. Indeed, the sale of a machine usually does not entail the transfer of intellectual property rights (in this case the right to access the software apart from its designated use). New maintenance contracts and wireless software updates over the internet now offered by manufacturers have reportedly subdued these concerns, See Poppe, K et al. (2016): *Precision Agriculture and the future of farming in Europe. Briefing paper 4: The economics and governance of digitalisation and precision agriculture*, p. 29.

While the previous section illustrated possible new business opportunities for firms offering universal data hubs or services enabling exchanges, full compatibility may be hard to achieve for individual manufacturers (especially for SMEs with less resources).

The medium-sized Dutch agricultural machinery company *Kverneland* reportedly encountered 50 different farm management software suites and 40 relevant machinery companies used by their customers when assessing compatibility options for their products. In this case, full compatibility in the present market environment would demand continuous monitoring of all proprietary and free protocols as such and in all their possible 2000 combinations.

In an interview, an interest association representative reported a growing awareness of these developments within the industry: Manufacturers are increasingly negotiating potentials for standardisations (e.g. through organisations like the *Agriculture Industry Electronics Foundation*) of interfaces.

B2B interoperability

The interoperability of products and services is also a key enabler of effective and efficient **B2B relationships**, as well as a safeguard in liability cases (see also the section on risk and liability). It has been argued as part of the interviews conducted that product safety regimes that are based on interoperable solutions are, in practice, more important for B2B relationships than contractual liability regimes. This can be illustrated by means of an example:

- A farmer uses a smart silo that makes use of smart sensors to monitor the types and amount of cereal seeds within the silo. The silo indicates to the farmer that enough cereal seeds are contained in the silo to start seeding the fields.
- This monitoring is being done by means of sensors. The sensors are not manufactured by the silo company but by the sensor company.
- The farmer wants to start seeding the field. However, he recognises that the silo has apparently sent incorrect information. In other words, the sensors within the silo have not triggered the silo to order cereal seeds.
- The farmer cannot seed his fields and therefore has a financial damage, as his harvest will be smaller than expected. Therefore, the farmer claims liability from the silo company.
- The silo company forwards the farmer's claim to the sensor company, asking for compensation because it was due to the data sent by the sensor that the silo did not order cereal seeds.
- However, the sensor company denies liability on the ground that – although its sensor indeed sent data that should not have been sent to the silo – the silo did not recognise that the data received from the sensor was incorrect.
- The silo company cannot claim compensation from the sensor company as its product was not smart enough to recognise the incorrectness of the information, e.g. by using other judgment parameters (for instance that a silo needs to be filled between two harvesting seasons).

Therefore, although from a contractual perspective a liability regime is in place under the PLD, the more important issue in this case is the interoperability of the sensor and the silo

regarding the mutual check and recognition of the *correctness* of the data received.[270] This can, for instance, be ensured through pre-market testing and certification of both products.

In the end, this means that interoperability between products and services can also be regarded as a means to preclude liability claims in the B2B context in case the end-consumer suffers damage.

Cybersecurity and network integrity

Apart from hardware failure, software bugs or misconfigurations remain the major cause for ICT system failure in general. As the number of connected networked devices increases, their occurrence and relevance may thus be expected to grow in the future.[271] Apart from singular malfunctions and human error, possible far-reaching consequences from external disruption (e.g. general power outages) may also trouble farmers.[272]

Until now, the topic has failed to attract much attention in the debate around data-driven agriculture.[273] Nevertheless, as explained in the textbox below, high profile attacks may raise awareness and fears of farmers. A growing sense of vulnerability together with ensuing additional investments in fail-safe system components, may present technical, economic as well as psychological barriers to the continued adoption of technologies.

Outlook: Cybersecurity implications for liability questions

Over the previous years, European citizens learnt of a rising number of hacks, ransomware[274] or distributed denial of service (DDoS) attacks focusing on high profile political and economic actors and personal computers of ordinary citizens alike.[275] These pose new questions for future IoT system security in general, yet also for connected precision agriculture technology in particular.

Possible future **liability questions** arise from the recently observed surge of DDoS attacks, employing hacked IoT hardware like routers or smart surveillance cameras to shut down websites and services for political reasons or criminal gains.

[270] In that sense, the product liability regime applied in practice is an incentive for businesses to manufacture safe products.

[271] See BBC News (06.01.2017): *2017 tech trends: 'A major bank will fail'.* http://www.bbc.com/news/business-38517517

[272] See Capgemini Consulting and Wageningen UR (2016): *Cybersecurity in the agrifood sector. Securing data as crucial asset for agriculture;* https://www.wur.nl/upload_mm/4/6/a/f74a893e-c829-4bf3-9884-e357929ff5d6_Cybersecurity%20in%20the%20agrifood%20sector.pdf

[273] As a stakeholder phone interview with an interest association for agricultural machinery producer conducted by Deloitte revealed; See also Capgemini Consulting and Wageningen UR (2016): *Cybersecurity in the agrifood sector. Securing data as crucial asset for agriculture.*

[274] The term ransom-ware describes malicious computer programmes that infect operating systems, remove basic functions or encrypt users' files until a ransom is paid to the attacker (most commonly in virtual currencies).

[275] For further information see European Union Agency for Network and Information Security (03.11.2016): Major DDoS Attacks Involving IoT Devices, https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices; or Akamai (2016):*Q3 2016 State of the Internet – Security Report, https://content.akamai.com/pg7407-soti-security-report-q3-en.html*

Who is to be held liable, if systems are not adequately secured and subsequently used for attacks or develop malfunction may become a matter of debate in the future? Producers of agricultural machinery so far emphasize the role of the software provider to ensure the safety and integrity of their networks.[276]

The **confidentiality of information** presents concerns closely related to cybersecurity. Primary data generated on the field as well secondary data from analysis and planning tools included in farm management software contains sensitive business information. As illustrated in the subsection on data-ownership and (re-) use, this information may be used to the detriment of farmers by other parties.

For instance, one farmer stressed that he only uses a small-scale cloud with a friend and neighbour. He cited two reasons for this:

- On the one hand, this choice is grounded in convictions, that third parties would not be able to handle this kind of data adequately. Likewise, uncertainties about data ownership play a role when passing on data gathered on fields owned by other persons; and
- On the other hand, he expressed worries about certain business models used by cloud farm software providers. An example provided was one provider explicitly informing farmers that uploaded information may be sold to third parties yet also offering to store sensitive documents (e.g. insurance policies or personal data about the landlord) uploaded by farmers in their cloud.

Representatives of machinery manufacturers have likewise observed avoidance strategies due to privacy and confidentiality concerns: In an interview, one representative of a machinery manufacturers' interest association explained that, some farmers even intentionally disable network access of their machines in order to avoid data sharing.

Internet access in rural areas

Albeit high-speed connectivity is available almost everywhere and at every time within urban areas, farmers face barriers with regard to the use of services when Internet access is limited. The percentage of households that are not equipped with broadband internet connection ranges from almost 20% in urban areas to nearly 30% in rural ones. During stakeholder interviews, farmers mentioned two aspects in particular which they experienced as limits two data flows in practice:

- *Limited bandwidth* represents a bottleneck to complex data streams (i.e. reducing the number of possible parallel sensors),; and
- *Limited signal strength* reduces stability of transfers (i.e. making a loss of data in transit more likely), in particular if data is uploaded from the machine to the farm management software.

While some service providers try to mitigate this challenge by providing software solutions that can be used offline and synchronized with the system afterwards, not all available programs are capable of this so far. Accessing and using data in real time, e.g. on the field while

[276] See for example: Agricultural Machinery Association Germany (2016): *Inter-Operational Data Management - Recommendations for Data Protection & Security*, Position 16/2016.

farmers are planting seeds, is crucial – yet it is still an issue and holds back the use of big data in certain areas.

With its 5G Action Plan[277], the European Commission has set out a roadmap for future investments into related infrastructure. To this date, it is not yet clear to what extent farmers will benefit from corresponding investment plans.

Technical literacy of ageing workforce

Furthermore, the ageing workforce of the agricultural industry is a challenge for digitalisation. While younger generations often adopt technical solutions at an early stage of deployment, the agricultural industry is coined by a lack of a younger farmers that possess the willingness and tech-savvy to implement up and coming technologies in their own business.

Given the **growing demands in technical literacy**, these issues may present barriers to the willingness of farmers to implement complex interconnected systems in their work routines. Fears concerning a loss of control may be the result.

[277] See: https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan

Financial services

In order to adequately assess the different challenges in relation to data access and sharing in the financial sector, this case study will look both at the perspective of big players and SMEs. The second category will provide precious insight on the views of newcomer fintech players and of start-ups applying emerging business models while the former illustrates how well-established banks see the issues related to data access and sharing for their business models.

It is worth nothing here that the financial sector is one of the most regulated area covered by the present assignment and that is undergoing structural changes, also due to the new legislative framework put in place at the European level.

The driving force behind these major changes is the revised Payment Services Directive (PSD2) which is set to accelerate the competition and digital disruption that are already re-shaping the financial services industry across and beyond Europe[278]. The PSD2 in fact mandates the opening of banks' application programming interfaces (APIs) to third parties if the account holder provides consent (article 66 and 67)[279]. This directive therefore stimulates innovation and it is highly appreciated by the fintech and start-ups dealing with financial data as it ensures them access to data in an automatic way. Although extremely important for establishing a framework for exchange of data, it is worth mentioning here that the PSD2 applies to personal data (financial data of the account holder, hence categorised as personal) rather than non-personal data as covered by this assignment. There is a link between these two categories of data and with data access and sharing overall as the same APIs used to share the data of the account holders with the third parties can also be used, as already done by some innovative banks[280], to develop data ecosystems and to share aggregated datasets which do not enter in the realm of personal data anymore. Nonetheless, strictly speaking the PSD2 does not force financial institutes to open up all their data, and especially the aggregated datasets which would be the most valuable for innovative businesses.

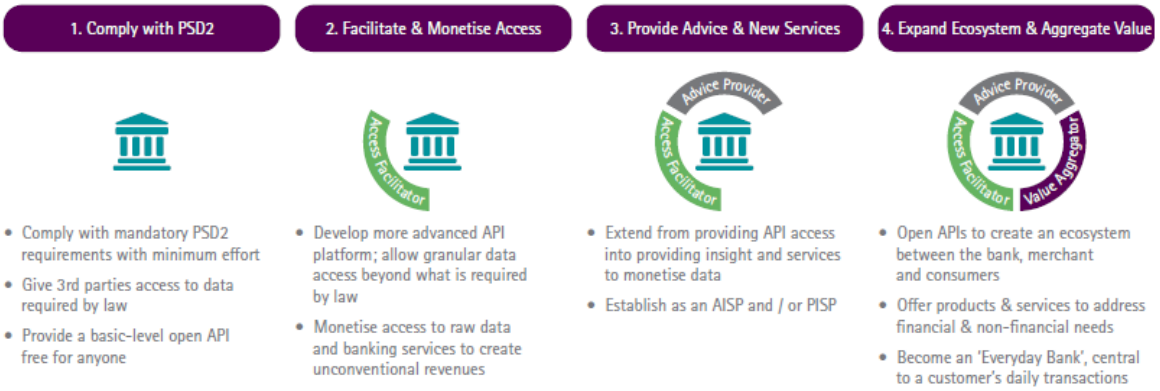
This being said, banks need to adapt to the changes introduces by the PS2 Directive and they can implement different strategies for doing so, ranging from limiting themselves to be compliant with the rules to develop innovative products on top of the data and position themselves within an ecosystem of stakeholders. The picture below shows how the literature illustrates these diverse approaches.

[278] Accenture, Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive - PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking, see: https://www.accenture.com/t20160505T180127__w__/ca-fr/_acnmedia/PDF-15/PSD2-Seizing-Opportunities-EU-Payment-Services-Directive%20(1)%20(1).pdf

[279] See: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=en

[280] See section 4.9.1 below

Figure 24: Adaptation of PS2D - Options for banks



Source: Accenture[281]

In addition to the PSD2 there are other legislative initiatives of the European Commission affecting the exchange of data in the financial sector and these are of course the GDP Regulation[282], the eIDAS Regulation[283], the anti-money laundering directive (AMLD4[284]) and the NIS Directive[285].

The smooth implementation of all these combined rules is key for an effective and valuable exchange of information and data in the financial sector[286].

It is important to notice that the European Commission recently carried out a public consultation on Fintech, to seek input from stakeholders to further develop the Commission's poli-

[281] See: Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive - PSD2: A Cata-lyst for New Growth Strategies in Payments and Digital Banking, see: https://www.accenture.com/t20160505T180127__w__/ca-fr/_acnmedia/PDF-15/PSD2-Seizing-Opportunities-EU-Payment-Services-Directive%20(1)%20(1).pdf

[282] See Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on free movement of such data, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[283] See Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[284] See Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

[285] See Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[286] See the European Parliament Draft Resolution on Fintech: the influence of technology on the future of financial sector 2016/2243/INI , http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-597.523&format=PDF&language=EN&secondRef=01

cy approach towards technological innovation in financial services[287]. Some of the elements covered by the Consultation relate to the overall Data Economy, such as for instance the section on interoperability and standards, as both topics are mentioned as being particular barriers for smaller players willing to enter into this market[288]. In this respect, available literature already suggests that: "national governments should engage with the financial industry for private led standards (...) data standardisation and harmonised definitions could also allow financial regulators to enable their efficiency"[289].

The next section describes traditional banks are adapting to this new environment following different strategies. Furthermore, the section on start-ups examines the situation from another perspective, taking into account the (re-)users side of the ecosystem.

Big players: traditional banks

Context, business models and actors

For some of the most traditional banks, the PSD2 Directive does not change dramatically the way of looking at data and at the business models. It is worth noting here that banks are not built in a "data-centric" way as their historical products are not linked to data; availability of data is only a consequence of the business, not a raison d'etre or a service in itself. Therefore, some major banks see the question of opening up data through APIs to third parties more in terms of compliance with the legislation that in terms of window of opportunities for inventing new services and products. This can be due either to the fact that is too early in the process (the implementation delay for the Directive is not even expired yet) or because of a conscious strategy.

In the first case, a later assessment of how the banking sector is adapting to the PSD2 could show a larger impact on the data sharing across stakeholders than the one that could be identified at this stage, which is very limited. In the second case, the data market for banks will most likely change very slowly (if not at all) in the coming years. In fact, some traditional banks argue that the full exploitation of internal and external data for business purposes deserves a thorough refection. They are not sure they are willing to embark in this kind of journey knowing that it could decrease the public trust in their services and therefore backfire at them. While they acknowledge the very interesting things that fintech are doing with data (showing to bigger players what the "art of the possible is"), they consider themselves as too subject to scrutiny from the authorities to be really able to try something new without being certain that it is possible, valuable and not dangerous in reputational or legal terms.

They also believe that fintech are more able to take risks, not only because of their dimension that allow them to pass below the screening line, but also because penalties for them

[287] See: https://ec.europa.eu/info/finance-consultations-2017-fintech_en

[288] See Consultation Document: "Fintech, a more competitive and innovative European Financial Sector".

[289] See Communication of the European Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on Consumer Financial Services Action Plan: Better Products, More Choice, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:139:FIN

remain quite limited (up to 4% of the turnover, which in case of start-ups can be close to none). This is not the case for major banks who can suffer severe losses if they happen to be sanctioned for illegal proceedings. Therefore, a common remark from big players concerns the need to create a level playing field in which the scrutiny obligations are similar for big and small players. This is one of the condition for the major banks to be able to risk more and share their data beyond what it foreseen in the PS2D.

One of the interviewees talked about this issue as a "clash between business innovation and compliance". If, on the one hand, business departments within major banks push for developing new approaches to data and new products based on analytics, the compliance departments very often warn against the risks of such an approach, especially in the European context. Indeed, in the Unites States the case law philosophy offers some insights to innovators on which proceedings are allowed and which are not and banks can justify themselves in courts based on previous judgments on the same or similar topics. In the EU on the other hand, the interpretation of existing laws often leaves a marge of uncertainty that is perceived as very risky by compliance departments. Also, courts are not bound to the same uniform interpretation of the law across Member States. This uncertainty will be further discussed in the next sections.

In this context, the question of which actors and stakeholders populate the data ecosystem of these more traditional banks is not yet very relevant. Indeed, as one of the interviewees argued "there is no exchange of data yet and therefore the question of the role of the bank in the data ecosystem is not addressed for the moment". Some complained about this lack of strategy on the long term while others argued that, for the bank to remain trusted institutions, prudence at this stage is highly recommended.

Considering all these general elements, and especially the fact that data sharing "has not even started", the elicitation of barriers for traditional banks cannot be expected to produce a well-nourished list of obstacle to flow of data. Nonetheless, some considerations can be drawn on contractual and non-contractual barriers already at this stage.

Identified legal barriers

Most of the legal and contractual barriers mentioned during the interviews concern, more than a specific provision on data ownership or liability, a general uncertainty surrounding questions around data in Europe. Laws are unclear in many respect:

- **In terms of (re-) use of data**: there is a general lack of clarity on what banks can and cannot do with their clients' data. General principles are available in this respect but specific boundaries are very hard to find. Fintech can play around with this ambiguity and eventually cope with it very well because they are less afraid of economic and reputational losses. Traditional banks on the other hand have much more at stake and they are conscious that "testing the boundaries leads directly to reputational losses". One example that was mentioned in this respect was the one of ING. Back in 2014 ING wanted to test a pilot exploring if customers would be interested in receiving tailored

discounts from third parties in line with their spending behavior[290]. The pilot would have worked only on opt-in basis and by asking the explicit consents of the customers. This however led to very bad press reviews and high reputational losses for ING[291][292] as well as to an intervention of the Dutch data protection authority which argued that "banks should show utmost restraint in profiling their customers in such a far-reaching manner"[293]. One of the interviewees considered that this story taught a lessons to all major banks about the risk of daring too much with clients' data and reusing them for purposes which are not the original ones.

- **In terms of data protection legislation and privacy**: there seems to be a certain degree of confusion on how the GDPR and its categories of data must be interpreted. Some of the interviewees suggested that this uncertainty linked to the categories of personal and non-personal data adds burden on all financial players and, overall, it advantages the bigger banks who dispose of more legal capacity. One interviewee argued that "if we would have to apply the letter of the law to the full extent, we would be completely incapable of doing any kind of data analytics on top of data". Although nobody challenged the utility and the spirit of the GDPR, many argued that its provisions are too vague to offer certainty in interpretation and that such uncertainty kills innovation. Due to this vagueness, banks are afraid to take risks and be then penalised by the scrutiny authorities.

If for (re-) use and data categories there is a common agreement on the fact uncertainty restrain the innovation possibilities, the same does not apply to liability issues. Indeed, when asked about liability clauses and potential barriers linked to them, most of the interviewees from traditional banks considered that this is not one of the main obstacles to the exchange of data. In fact, big banks are quite confident in the quality of the data they have and do not see yet major risks of being held liable for providing incorrect datasets to (re-) users. However, they admit that it is probably too early to draw conclusions on the eventuality of risks linked to liability as the real sharing of data has not even started yet.

Identified technical and any other barrier

Contrarily to many other interviewed stakeholders, traditional banks do not acknowledge interoperability as one of the major issues linked to the data access and sharing. In fact, they suggest that, although interoperability barriers do exists, they are easily solvable as it is just a matter of developing interoperable systems. This of course involves a cost, but bigger banks believe that the issue affects more start-ups and smaller players that have less money to invest in interoperability systems. Interoperable standards and interface could contribute to the creation of a level playing field for all business players but they are not the main barriers preventing big banks to develop new strategies based on data sharing.

[290] https://www.ing.com/About-us/ING-and-the-use-of-customer-data.htm
[291] https://www.nrc.nl/nieuws/2014/03/11/we-doen-dit-voor-de-klant-heus-1353871-a1246767
[292] http://www.demorgen.be/binnenland/ing-belgie-gaat-data-van-klanten-gebruiken-b9b18635/
[293] https://www.bloomberg.com/news/articles/2014-03-10/ing-plan-to-share-customer-payment-data-spurs-privacy-concerns

SMEs perspective

Context and business models

Financial SMEs and start-ups are now successfully proliferating within the financial sector due to the potential of the data stored and to the new regulatory framework of the PS2D. In fact, with respect to other sectors, the clear and forward looking legal framework of the financial sector enables different players to exchange data in an automated and secure way thus fostering the development of new business models.

Nonetheless, despite a favourable environment if compared to other domains, the fintech and start-ups operating within the finance sector may face some challenges concerning the exchange of data. These are detailed below.

Identified contractual barriers

Overall, the interviewed SMEs and start-ups did not mention overarching issues disrupting their business models and preventing them for providing innovative services and products on the market. On the opposite, they all underlined how the new payment Directive was a turning point for the financial sector in opening up access of small players to data and allowing to generate new business opportunities. Before the Directive in fact, the biggest players on the market were very often denying the access to data or making it very difficult based on technical barriers or reputational ones. In fact, in some cases banks were discouraging their client to use start up services based on privacy or any other kind of risk associated to sharing their data.

This is not the case anymore thanks to the payment Directive which defines clearly the types of data that must be provided and in which conditions. Therefore, start-ups and fintech are now benefiting from a new business environment in which there is much more transparency and guidance for both small and big financial operators. Also, no contracts amongst these smaller firms and data sources is needed for the exchange of the data: based on the Directive, the former need to have direct access to the clients' data when authorised by them. In cases of access to other types of datasets, contracts might be needed but all players benefit from contractual freedom and the start-ups and SMEs did not express any particular concern in this respect.

Data ownership and (re-) use

The Revised Directive on Payment Services (PSD2[294]) establishes that data ownership remains with clients and provides for their right to access, share and transfer their data (also to another provider), through open APIs. PSD2 in fact forces banks to allow third parties to access a given customer's data, where that third-party is acting as a data consumer or a delegated authority[295]. This provision was often mentioned by the interviewed SMEs and start-

[294] More info: https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/

[295] The PSD2 describes third parties as "third party providers (TPPs) [who] offer specific payment solutions or services to customers.

ups which argued that, as they operate on the basis of a customer mandate, the ownership of the data remains clearly on the customer side. When the customer withdraws the delegation and/or ceases the subscription to the start-ups services, the data are deleted as they cannot possibly be retained without the customer's consent. However, the aggregated datasets of their clients' data are "owned" by the start-ups themselves which use them for statistical and data analytics purposes (but in an anonymised way). No issues have arisen around this element so far.

On the other hand, (re-) use of data has been mentioned as somewhat more complicated to handle, at least at the legal level. As one of the start-up founder argued: "we rarely get a clear answer to the question of the (re-) use of data. Even when asking law firms, we often receive contradictory information. Therefore we treat (re-) use opportunities on a case by case basis". Therefore, a demand of clarity emerged on the limits of (re-) use. The lack of clarity in fact entails additional costs to be borne by start-ups that have to consult several law firms in order to get an answer to their question. This element is probably less relevant for banks and big players that have more in-house lawyers and therefore internal capacity to address this challenge.

Risk and liability

As for data ownership, risk and liability do not present major challenges for start-ups and SMEs at this stage. This does not prevent them from taking precautions such as informing their clients that errors in the data can happen (linked to issues in the data themselves as provided by the data sources or in the technical solutions adopted by them) and that risks exist. However, as one of the start-up founder mentioned: "the risk is more reputational than legal", a point of view which is shared by both smaller and bigger players on the financial market. If something goes wrong with the service provided by the start-up indeed, the consequences of losing clients are more severe than the ones strictly linked to liability itself. In this perspective the position of SMEs and start-ups is very similar to those of the banks and bigger players. However, according to the start-ups, data quality is highly variable and is generally low with the exception of the largest players. The start-up believes that standardisation would not only facilitate exchange of data but also improve quality and decrease the risk of error.

On the other hand, cybersecurity is recognized both as a key concern and as an area that needs to be further developed. One of the interviewed start-up highlighted that in the financial sector the management of risk in relation to IT and cybersecurity is strictly regulated, both in terms of defined technical requirements and the allocation of resources to cover eventual losses that may arise in this context.

Identified non-contractual barriers

If contractual barriers are not seen as major obstacles for innovative start-ups and fintech companies, the non-contractual barriers on the other hand present some severe challenges for them as they involve bearing additional costs.

Interoperability and technical barriers

In the financial sector, interoperability is a relevant issue with respect to both data interoperability and interface interoperability. With respect to the former, almost each data source uses a specific format and a specific semantic approach to data. Interoperability is therefore one of the main cost drivers for start-ups and SMEs aggregating data from different sources. A lot of time and resources are spent in cleaning the datasets and making them interoperable. This might also cause errors in the provision of the services and this is the reason why smaller players strongly advocate for interoperability standards and semantics to be agreed upon at the European level. As one of the interviewees put it: "standardisation and full interoperability are keys for us to avoid errors and provide the most efficient service possible".

At the same time, interoperability of interfaces is also a major problem. The major banks have different types of interfaces to which the smaller players need to adapt in order to be able to scrape the data and this constitutes an entry barrier for start-ups as it entails sever costs. In the European Interoperability Framework, the European Commission recommended to improve the interoperability of interfaces of public administrations that internally use different standards[296]. The interviewed SMEs and start-ups argued that a similar approach should be taken within the framework of the financial sector and especially for those data covered by the PSD2 Directive. Also, the banks offering APIs for the access to data have very limited interest in providing a well-functioning service as long as they are compliance with the Directive's obligations. Therefore, the interviewee consider that banks' APIs currently work very badly. For this reason, most of the interviewed start-ups had to create their own API system in order to overcome this challenge.

Interoperability of datasets and of interfaces can therefore be considered as substantial barriers for smaller players, although not an insurmountable ones. No other technical barriers were mentioned by the interviewees.

Legal/technical uncertainty of categories and confidentiality of data (personal/non-personal)

The uncertainty related to the categories and confidentiality of data was mentioned as possible barrier for SMEs and start-ups. More than the distinction between personal and non-personal data (which is now clarified by the General Data Protection Regulation) the issue concerned the difference between sensitive and non-sensitive data. There seems to be some confusion around these terms amongst the start-ups and across countries, as some categories considered sensitive in one Member State might not necessarily be seen that way in another one. On the other hand, the categories of personal and non-personal data are now sufficiently enlightened by the GDPR Regulation.

[296] See European Interoperability Framework (EIF): "Recommendation 12. Public administrations, when working to establish European public services, should develop interfaces to authentic sources and align them at semantic and technical level". http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

Chemical sector

The present case study is based on desk research and semi-structured interview with Sean Jones, former Vice President Information Services Business Relationship Management at BASF and Founder and Partner at Yukon Digital[297], a provider of digital solutions to companies involved in the Chemical, Petrochemical and Oil & Gas Industries, about data science, innovation cycles and the state of the chemical industry.

Sean Jones and James Thomas founded Yukon Digital in 2015 to respond to the growing interest in big data analytics solutions of the chemical industry and other process-oriented industries like oil, gas or pharma. Yukon Digital was formed due to the identified gap in the market for a smaller, agile company that can work closely with clients to identify operational and process improvements through the use of big data.

Context

The initial situation within the market

The chemicals industry is acknowledged to be as one of the biggest manufacturing sectors in Europe. It represents around 7% of the European industrial production; has sales amounting to EUR 527 billion (2013), which is about 17 % of global chemicals sales; around 1.1 % share of EU GDP; and provides 1.15 million direct highly-skilled jobs (2013)[298].

This industry is characterised by being energy intensive and highly regulated in order to protect workers safety, consumer's health and the environment. Thus, this sector is today experiencing a rapid structural change due to major challenges such us increased international competition - especially due to the growth of China, India, Korea, the Middle East, South East Asia, Nigeria, and Brazil, rising energy and feedstock prices, labour costs amongst other cumulative cost effects due to climate, environmental, and energy policies. In consequence, this sector is confronted with a pressure to increase resource efficiency and a need for innovation.

The chemical industry produces petrochemicals, polymers, basic inorganics, specialties, and consumer chemicals, and involves the use of chemical processes such as chemical reactions and refining methods to produce a wide variety of solid, liquid and gasesous materials. Those processes operate in chemical plants to form new substances in various types of reaction vessels. In many cases the reactions take place in special corrosion-resistant equipment at elevated temperatures and pressures with the use of catalysts. The products of these reactions are separated using a variety of techniques including distillation especially fractional distillation, precipitation, crystallization, adsorption, filtration, sublimation, and drying.

[297] See: http://www.yukon.digital/
[298] See: https://ec.europa.eu/growth/sectors/chemicals_en

The processes and products are tested by dedicated instruments and quality control processes to guarantee the safe operation and that the product meets all required specifications. R&D laboratories inside chemical companies carry the testing processes in their research facilities.

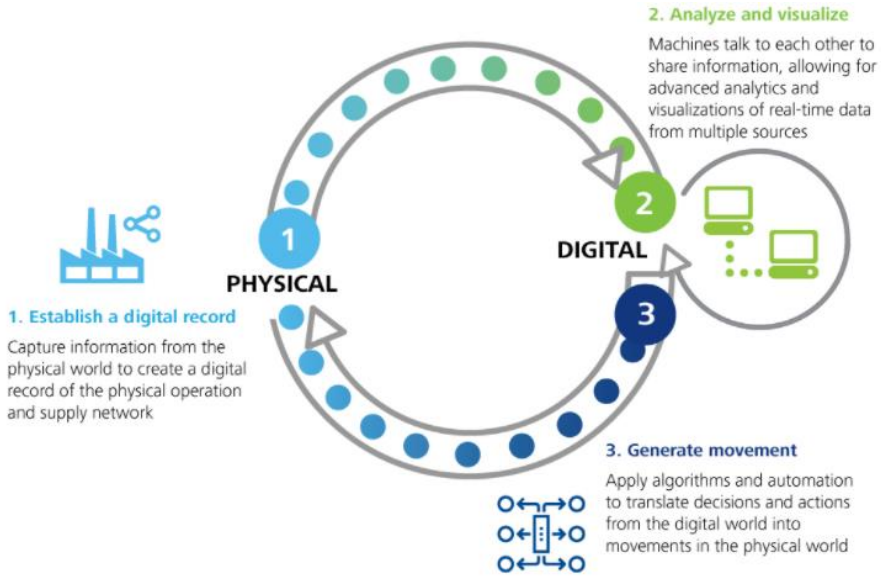
The chemical industry is still largely focused on maximizing the value of its production assets, reducing downtime through improved operational effectiveness, optimizing batch yield, continued inventory and delivery reliability improvement especially across global site networks through the link between demand planning and production planning.

Another relevant characteristic about this sector is the broad spectrum of customers that it serves, across various industries. Chemical companies seek to support their customers to be more successful, but understanding the customer segments and their needs is a challenge and prioritizing resources and effective pricing to those segments constitutes also a data intensive task. Some chemicals manufacturers are going one step further and they are trying to generate new business models by stepping into their customers' value chains and providing data-intensive services to optimize farming yields, painting processes and knowledge.

Overview of the impact of Big data in Chemical sector

The chemical sector has embraced the benefits of implementing information technology in the design, process management and process modelling, for many years. Connected technologies inherent to the Internet of Things (IoT), including analytics, additive manufacturing, robotics, high-performance computing, artificial intelligence, cognitive technologies, advanced materials, and augmented reality, are having an impact on the physical act of manufacturing in the chemical sector.

Figure 25: Interaction of physical and digital processes in manufacturing



Source: Deloitte University Press

Big Data is used in the chemical industry mostly for detecting product defects, boosting quality and improving supply planning by enabling better operational decisions in real time. Although the potential of big data is already acknowledged by some industry players in the

chemical sector, the uptake is still limited and big data is primarily used at the level of business operations because of the volume of historical sensor data collected by chemicals businesses over the years.

Examples:
Already in 2005, Dow Chemical started using advanced analytics to develop freight and logistics cost models as well as raw material spend analysis. This enabled the procurement teams to be better prepared to make decisions when renegotiating contracts, which led to considerable cost saving benefits. Similarly, DSM and Sinpoec started using IT to enhance spend reporting and analysis to substantially improve and speed up the procurement decision-making processes.

There are four main areas of interest for chemical companies when implementing big data: operations, supply chain, marketing and sales and new business models.

In ***operations***, the main goals are automation and increasing the productivity of people. Chemical companies with the support of data companies or analytics providers seek to understand how to increase performance with data, either through increasing reliability or decreasing maintenance costs. Improvement in business operations can be obtained in two different ways: by improving productivity and/or by reducing risk. In general terms, the productivity of chemicals plants can be increased through diverse smart manufacturing techniques: process control, predictive maintenance, and production simulations, among others. On the other hand, reducing risk, involves managing supply chains and in-house operations to respond to changing customer needs and to improve safety and quality.

In the ***supply chain***, the problems that company try to address are of a different nature. Visibility is one of them. For instance companies are still struggling to exactly track and locate where chemical container are. Although a decade ago DHL, UPS and FedEx developed these very transparent supply chains, those still do not exist in chemical industry, due to the complexity and vast amount of players playing a role in the chemical supply chain from production to the first transportation stage to shipping, to distribution. This is a key challenge if companies seek to optimize inventory levels for required delivery reliability, or to connect both the sales forecast with the production plans.

Chemicals companies usually operate on a B2B model where they sell products that are then used by their customers to generate a set of new products. In some cases, those customers need that those products are delivered within a specific range of temperature or pressure so that they can adequately use it for subsequent production processes. In consequence, the monitoring of chemicals during transit is a key issue and it is still challenging. Some of those companies are already using in the upstream and downstream value chain tools such as Ovinto satellite monitoring devices on railcars. The device is used in combination with a GPS to track the location of the railcar, together with a variety of sensors, which measure the physical properties of the chemicals, as well as the condition of the railcar via data such as shock impacts. The visibility that is provided by the direct, periodically interaction among the railcar and the chemicals company, makes possible a better supply chain planning while enabling to ensure safe transport of dangerous chemicals. In this example, is already clear the

variety of players involved in this ecosystem: the transport operator, sensor provider, satellite network operator, and the technology provider for the storage of data on the cloud and finally the analytics and visualization provider.

Regarding ***marketing and sales,*** the main goals are micro-segmentation and optimization. The customers in the chemical industry are very unique. Thus, seeking to better understand what are pockets of improvement, whether chemical companies can increase prices or improve market share or potentially even change a product, is something that traditionally has been done very manually, often still with tools like spread sheets. Today data company and analytics providers are helping chemical companies to figure out from a very complex product and customer environment what are actual opportunities for improvement.

Finally, the last main area of interest for chemical companies when applying big data is to build ***new business models***. The main challenge for those companies is to take a classical chemical product and change the business model in order to increase loyalty and revenue streams. It usually requires getting into a closer cooperation with the customer. The main questions that companies are asking in that regard are: How can companies get data from the customer's product usage to detect patterns? How can they better understand the drivers of usage and help customers better solve whatever chemical or material problem they have? Answering those questions can help inform future spending in product development, because it enables companies to allocate money to the right areas. Although this domain of application is extremely interesting and players within the industry recognize in it a great potential to significantly increase revenue and competitive advantage, it is still very immature.

Trends in the implementation of Big data in the Chemical sector and examples of technical solutions in the market

The main four areas of application already described above can be broken down into different trends that chemical companies are embracing in the implementation of big data.

a) Smart production

In chemical manufacturing plants, technology is being used to ***automate production***, to implement and progressive improve of process controls, integrate asset sensors, enable better supply planning, and to take the most of manufacturing execution systems at the enterprise resource planning (ERP) level. The smart production combines IT, such as Internet of Things (IoT), artificial intelligence, and advanced analytics, with OT, such as additive manufacturing, advanced materials, and robotics. Within this context, big data goes one step beyond and enables to "connect the dots" from diverse data sources to incrementally improve asset utilization and to make better operational decisions in real time.

For instance, on the shop floor, terabytes of data that has been generated by pump monitors, valve vibration analysis, agitator torque tracking, variable pressure meters and other types of data are used to identify the optimal production, reduce waste and increased ROI.

One of the main aspects of Smart production is related to ***process management and control.*** Traditionally, control rooms of petrochemicals companies have been used to have control-

lers along the walls; operators walked around the room and manually checked the readings to assess and monitor plant operations and conditions. Today, data is gathered through connected systems and is presented to operators digitally, without the need for manual reviews, which dramatically saves operators' time and effort.

Digitization is only the first step. Technology supports also *prediction,* alerts, and prescriptive responses. Data is also used to predict equipment failure, schedule preventive maintenance and document production processes, which are a key issue to support safe working environments and to comply with regulations.

In that respect, ***predictive maintenance*** is one of the key applications of big data in chemicals and one of the characteristics of such smart production. The chemicals sector is characterized by being high asset intensity. In consequences, IT/OT technologies can dramatically support companies to optimize their maintenance spends and improve their asset efficiency with predictive and digital maintenance. Thanks to the granular data gathered from sensors and critical equipment such as turbines, compressors, and extruders, data analytics tools are able to identify patterns to later predict possible breakdowns. Practically, smart equipment sends warnings and information messages to operators about any required maintenance, potential breakdowns, and delivery schedules. This is a key aspect of big data usage by those companies because it helps manufacturers to progress from reactive reparation to predictive maintenance. In addition, data from similar equipment, which is placed in different, locations can be gathered, compared and analyse to carry predictive maintenance, performance optimization, and design of new facilities.

Data used for predictive maintenance is not only useful for the chemicals company but also other players within the supply chain, such as the equipment manufacturer, who can improve also aftermarket performance: equipment working according to the performance contract has agreed-upon payment revenues, while the payment for equipment that has experienced failures or breakdowns in the promised life cycle is lower. Those kind of arrangements are a key aspect for the chemicals industry, where their equipment is usually complex, sophisticated and costly.

Example:
An international chemicals company faced several times downtime due to an extruder that failed more than 90 times in one year, which led to losses in production, scrap, and overtime labour. Thanks to real-time monitoring, the company collected structured data from the extruder sensors together with unstructured data from maintenance records, training records, and other sources, and developed failure prediction models. By analysing the data and identifying some patterns that led to evaluate some cause-effect relationships, the prediction model was capable to generate alerts and recommendations on the extruder performance. This predictive maintenance model resulted into 80% reduction in unplanned downtime and operational expenditure savings around $300,000 per asset. This implementation transform

the company's operational model and thus it started considering deploying similar asset management systems for other critical assets[299].

Another interrelated area with predictive maintenance is ***safety management***. Due to the sensitive nature of chemical products, it is especially important that chemicals companies guarantee the safety of their employees, supply chain partners and also customers throughout the whole product life cycle. Compared to the safety methods traditionally implemented in order to monitor the product life cycle, big data is supporting companies in their on-going monitoring. As an example, within smart production for safety management, one could highlight the use of drones by chemicals manufacturers in order to inspect dangerous plants. Traditionally, the company used ropes, ladders, and bucket trucks for monitoring elevated structures. However those inspections are challenging because of the flare temperatures, which could go above 2000 degrees Celsius, which also require the plant to be closed for a manual inspection. Drones, on the other hand, are equipped with cameras that are able to capture high-resolution images, and those are combined with the data gathered by multiple sensors. The combination of both can increase the efficiency of maintenance engineers together with the safety of the plant and areas surrounding it.

In addition to those applications within smart production, big data also enables to generate variants of already existing products. Those variations may generate production processes that decrease the production cost per unit or that produce a higher-quality alternatives with increased profit margins. One way through which they are doing it is with **production simulation**. Chemicals companies are using 3D visualizations and virtual reality for training operators and maintenance staff. For instance, a Chinese chemical company –Sinopec Engineering, used SmartPlant 3D, which is an advanced plant design software, to plan the structure of the plant, machinery and piping models for a project in Maoming and improved their workflow[300].

Furthermore, Big Data is used for ***energy management*** to analyse which components cause the most emission or pollution and replace them with new products. The energy costs contribute significantly to a chemicals plant's production costs. In a typical plant there are multiple activities with several interactions, and it is difficult for operators to select optimal operating conditions. Thanks to smart technology that enables to monitor energy consumption, data collected is analysed, and leads to an optimization of energy consumption. Moreover, regarding sustainability, Big Data is also helping chemical companies to formulate new compounds that are more environmentally friendly. Researchers are able to model factors like toxicity or energy consumption and in consequence develop products that support both profitability and long-term sustainability. For bio-based chemicals, analytics can be used to model the pathways in micro-organisms that make the most efficient use of new feedstocks.

[299] Deloitte University Press: Industry 4.0 and the chemicals industry (July, 2016)

[300] Sarah Everts and Matt Davenport, "Drones detect threats such as chemical weapons, volcanic eruptions," *Chemical & Engineering News* 94, no. 9 (2016): pp. 36–37; Federal Aviation Administration, "The Dow Chemical Company—exemption no. 11259," April 3, 2015, https://www.faa.gov/uas/legislative_programs/section_333/333_authorizations/media/The_Dow_Chemical_Company_11259.pdf.

The chemicals sector has a high degree of automation, and most of those plants monitor standard variables such as temperature, flows, tank levels, and pressures to derive optimal plant working conditions. However, Smart production technologies (also called Industry 4.0) which involves soft or virtual software sensors are increasing these data points with additional information and enable control of nonstandard process variables to improve energy efficiency. Soft sensors are neural-network–based inferential estimators that are capable to process a variety of variables gathered through standard instrumentation, estimate new process and equipment parameters, which would be not gathered otherwise, and improve operator effectiveness and plant efficiency. Soft sensors are considered to be useful when the physical instrumentation is expensive or difficult to install[301].

Example: Borealis, a leading manufacturer, uses data mining and modelling to develop dynamic target values for the energy consumption of a plant—accounting for factors such as the current conditions of the plant, outside temperatures, fouling of the systems, aging of the catalysts, etc.[302].

Finally, the combination of operational and financial data may streamline chemical supply chains and distribution systems. In that sense, regional exchange-rate risk models describe where to acquire raw materials and how to set a price for finished goods.

Example: BASF used Multivariable Testing analytics software from QualPro to optimize manufacturing processes, reduce costs, increase yield and improve product quality at its Freeport facility in Texas. Thanks to the advanced mathematical methods able to gather 40 variables simultaneously, multivariable testing analytics is applied to ideas brainstormed among staff and management to test multiple concepts in a short-time period, quickly identifying what factors have a positive, negative or no impact on business decisions. Due to this application of Big data, BASF was capable of quickly identify ways to make great improvements such as increasing sales, reducing waste, increasing production, improving advertising strategies or optimizing service levels. These improvements have resulted in total savings of US$36 million over a three-year period for the facility.

b) Pricing strategy

In the chemicals sector a robust pricing strategy is one of the most relevant commercial operation because it determines profitability. Pricing decisions are extremely and increasingly complex in this sector due to the diversity of raw material inputs and products offered along with markets served (geographic and application). As prices are being announced, the data on which they are based become out of date. There are many factors that have an impact on the price of chemicals. Some examples include market demand, raw material and energy pricing, exchange rates, competitor strategy and even the weather.

Traditionally, the pricing strategy within the chemical sector was based on little more than spreadsheets, gut feel and experience of the decision-makers. With the disruption brought

[301] Hiromasa Kaneko and Kimito Funatsu, "Database monitoring index for adaptive soft sensors and the application to industrial process," *AIChE Journal* 60, no. 1 (2014): pp. 160–69,

[302] Deloitte University Press: Industry 4.0 and the chemicals industry (July, 2016)

by big data, more advanced analysis of the diverse data sets is enabling to develop competitive pricing strategies based on accurate, timely data from a variety of sources, and in general more informed pricing decisions. One example of such practice is embodied in a leading EU chemical company who integrated internal data as well as external marketing and sales data to identify a set of key value-based drivers for customer behaviour[303]. Based on this combination of datasets, the company has been able to make informed pricing decisions in alignment with field sales operations, providing specific pricing guidance during contract negotiations.

Such impact in pricing strategy is also helping companies to fine-tune their product portfolio. Being now capable of understanding the distribution of existing prices and having the capacity to review margin outliers among their customers, businesses within this sector can now understand the underlying causes of underperformance for specific products and in consequence adjust their production portfolio accordingly.

Example: Dow is one of the companies implementing advanced analytics, and more specifically in the following domains: for cost based and exchange rate analysis, enabling more effective timing of buying of raw materials and pricing of finished products; for sophisticated data enhanced staffing models enabling acquisition of the right resources at the right time; for early enough indication of monthly target achievement to enable corrective action; or even for improved sales forecasts with fewer errors, our next section.

c) Market Forecasting

Reliable market forecasts, both short-term and long-term, are critical to the effective production, procurement but also investment planning in the chemical sector. Companies in this sector can achieve capacity optimization through demand forecasting and responsive scheduling. Forecasts in this market are recognised being complex and again traditionally have relied on experience and intuition. With the advent of big data and the capacity to mine abundant historical data sets and uncover potential indicators for future demand and trends, are starting to be seen extremely beneficial. Accurate short-term and long-term forecasts to support effective production, procurement and investment is being used by companies within this sector, being especially important for those global chemical companies that serve multiple markets across regions.

Three examples:

Green Shoots Growth[304], has been using data analytics in market forecasting. One of their clients wanted to identify the optimal decision based on the cost of the neutralisation agent and the potential revenue generated from the sales of the sulphate produced. As they explained: "*We purchased off the shelf market studies, but it became apparent that through intelligent interrogation and basic analysis of freely available trade statistics (and trading*

[303] Marketing executives learning to leverage big data for pricing and profitability, Pros, http://www.pros.com/about- pros/news/fourth-source-marketing-executives-learning-leverage-big-data-pricing-and-profitability/

[304] Advanced analytics support a world of business decisions, SAS website, http://www.sas.com/en_us/customers/dow-chemical-analytics.html

sites like Alibaba), costs and potential revenues could be derived in real time without purchasing expensive and often out of date market reports".

Dow Chemical has reported a number of sales and marketing benefits with advanced analytics. Sales forecasts are accurate within 10 percent, versus an error rate that was sometimes as high as 40 percent previously. Business unit leaders know by Day 12 of each month how to adjust strategy to meet targets.

BASF has deployed a predictive analytics approach combining two types of data: the company's historical data with economic data. This combination has enabled the company to forecast demand. The forecasting model takes into account external factors like seasonal effects, macroeconomic data for customer industries at national and regional levels, regulatory changes, and internal factors such as BASF's strategies—expansion, mergers and acquisitions, divestures, and other transactions. Using this model, BASF can plan and adapt its plant runs as demand changes[305].

Market forecasting can go to early stages of the value chain. For instance, chemicals companies can use sensing software to monitor construction-relevant discussions on social media and from there, to draw analysis about consumer behaviour and sentiments. These data can be combined with other types of data collected from other sources. Such forecasting efforts are helping chemical companies to identify demand indicators and expand their production capacities accordingly.

d) Customers relationship improvements

Due to the intense international and local competition, chemical manufacturers need to better understand the profitability of customers, products and individual sales transactions. This can be achieved not only by understanding the existing price variability but also the demand elasticity. Big Data implementation allows companies to analyse and understand the underlying factors that explain the differences between customers. Since the chemical manufacturing process is complex, it becomes difficult to customize products, but precisely those data analysis described help to create variants of existing products. Big Data allows businesses to make these types of decisions based on customer analysis, but it can also anticipate future customer requirements and industry trends.

e) Improved workforce management

It is becoming increasingly difficult for managers to find the right people with the right skills in the chemical industry. One of the most troubling factors is in particular the growing shortage of applicants with science, technology, engineering and mathematics degrees.

In general, new technologies but especially the use of big data, are supporting Human resources departments to evaluate and make evidence-based decisions that support their decisions when identifying and retaining talents. Using internal data combined with industry data from third-party sources, managers can identify trends and patterns and quantify fac-

[305] Robert Blackburn et al., "A predictive analytics approach for demand forecasting in the process industry," International Transactions in Operational Research 22, no. 3 (2015): pp. 407–28, DOI:10.1111/itor.12122

tors that influence employee job satisfaction, forecast workloads and measure employee engagement against peer benchmark data. Thanks to big data managers are able to revealing uncover insights, such as who is most likely to leave based on benefits or salary, all relative to industry benchmarking data.

f) New Markets: a shift in business models

Big Data is also being a key factor for developing new markets for chemicals. For instance, with Precision Farming the detailed analysis of weather, soil conditions, seed traits and historical yields on a field-by-field basis has helped farmers in their decision-making processes, specifically in their capacity to identify exactly what to plant, when to plant and what types of crop protection chemicals to apply. This is increasing demand for agro-chemicals and related products to serve this rapidly growing market segment[306].

Furthermore, the implementation of big data is also facilitating more information for today's demanding customers, which include: technical data sheets, certificates of analysis, safety data sheets, samples, customized labels, pricing documents, call reports, marketing analysis and other highly specialized reports[307]. Customer service representatives in fact are starting to be able to process nearly any request due to the big data technology, which relies on the availability of data.

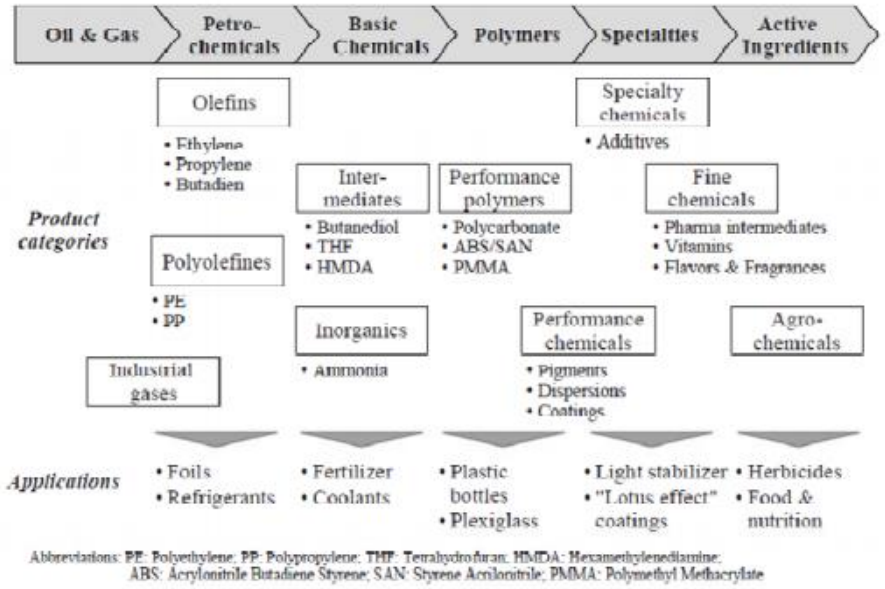
Actors and challenges

The chemicals value chain is characterized by its complexity compared to other sectors. The figure below shows the structure and value chain of the entire chemical industry starting with oil and gas which is transformed, in the following steps, in petrochemicals, basis chemicals, polymers, specialties and active ingredients. This industry provides raw materials and inputs for many other industries since its products are used in multiple applications cross-industries.

[306] Agricultural Adjuvants Market Accelerating Rapidly, Precision Farming Dealer, 13 July 2015, www.precisionfarmingdealer.com/articles/1542-agricultural-adjuvants-market-accelerating-rapidly#sthash.RhPls9Qy.dpuf

[307] KPMG (2016) What do data and analytics and changes in the personal care industry mean for chemical companies today?

Figure 26: Chemicals value chain



Source: Kannegieser, 2008[308]

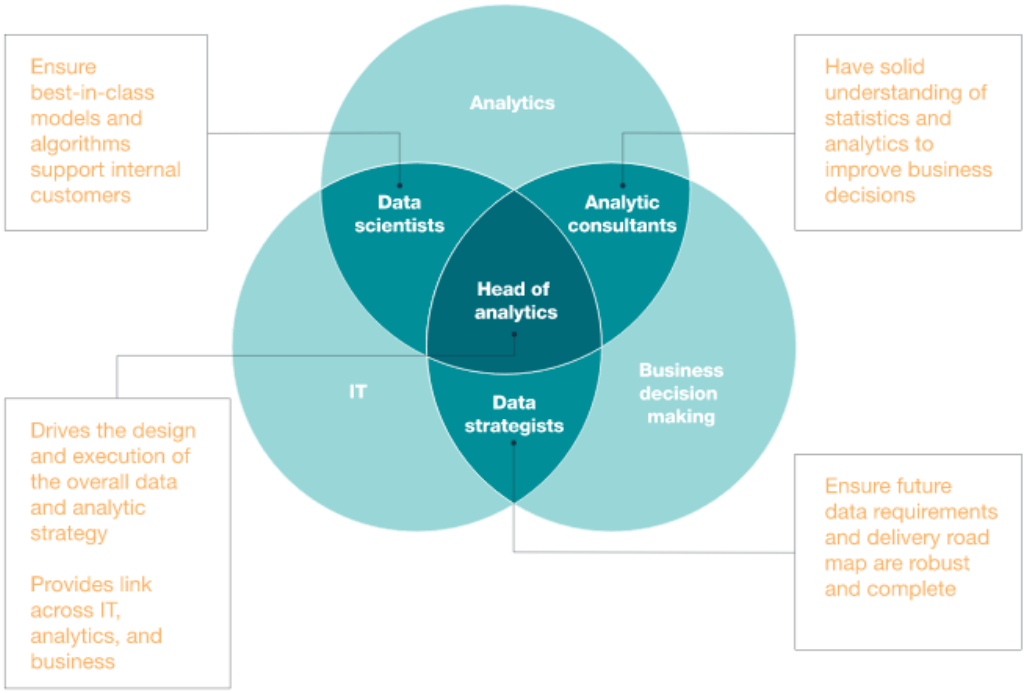
Regarding the implementation of big data within the chemical value chain, we usually see chemical companies using large IT platforms (e.g. Microsoft, Amazon, Google, SAP, IBM, General Electric) which are important as they provide the security and connectivity to the different data that chemical companies want to exploit. However, companies are craving for better micro-services –algorithms- so that they can do the optimization processes described in section above. The need for customization will slightly decrease in the future; successful companies move towards intelligently connecting those main areas described above: operations; supply chain; sales and marketing; and new business models.

On the other hand, maximising the potential of big data will increasingly require new skills and new ways of working. Talent is a relevant issue when trying to extract the most business value from data. Advanced analytics requires not just software programmers but also analysts who can combine the chemicals domain knowledge with software capabilities.

Just as an example, Dow has recruited 10 PhDs in computer sciences supported by a team of advanced analytics experts to work alongside its own business intelligence and analytics staff. The main challenge is not only identifying the need of those type of skills and discover those scarce talents but also, for senior executive mind-sets, to take the advice from those typically young (often in their twenties) “geeks” which usually have a more casual approach to business.

[308] See: Kannegiesser, M., Value Chain Management in the Chemical Industry, Global Value Chain Planning of Commodities, Physica-Verlag Heidelberg, 2008

Figure 27: Identifying people who can bridge different functional areas



Source: McKinsey & Company -2014

While companies try to build internally diverse capabilities in big data infrastructure, management, integration, validation, and analytics to take the most advantage of the implementation of big data, they are also requiring collaborations that usually take the form of a sub-contracting data analytics with data company providers and other stakeholders. One of such example is provided by BASF who sub-contracts analytics service to Yukon Digital.

Chemicals companies have customer's data related to their assets, manufacturing processes and customer behaviour data; however, often, those data are underutilized. For that reasons, chemicals companies are collaborating with data companies and other players to exploit those data to draw insights on developing smart chemicals products and service-based value propositions, and devising new revenue models. Data analytics companies, which provide those services, have no right to (re-) use these data as stated in the contracts and agreements signed as it is clear that data ownership is for the chemicals company (demand-side).

Finally, chemical companies are looking at concrete business cases, trying to avoid larger investment programs. Typically SMEs for instance seek to copy what is done by bigger companies. Therefore, change within this sector is happening incrementally, as the chemical industry is relatively conservative, especially in the IT area. Despite some examples such as BASF who is actually implementing a large program, which is called "BASF 4.0", other companies try business cases and look to what other companies do. Traditionally, the chemical sector is not used to the agile principles of IT. Usually companies need a full plan upfront before implementing anything and they just need to apply the waterfall method for project management. Consequently, triggering change with large scale programs require more time and efforts than those that would be required in the framework of smaller business cases.

Types of data generated and used by different actors

Data management includes all the activities associated with data-value chain: the collection, aggregation, storage, and analysis of data. Chemicals companies face the challenge that their data are stored in different systems: financial, sales, and marketing data are stored in one system; operations, production, and manufacturing in a different system; and R&D and engineering in another.

In order to truly realize the value of data, these data are starting to be combined due to the demand of third-party organizations (data provide) who are helping those chemical companies (demand-side) to provide the data analytics. This combination is what enables those agile and usually small companies offering the analysis layer to offer a holistic view of the organization and in consequences a great business value by taking the most of this data.

Looking at the types of data provided by and exchanged between businesses, four main types of actors can be distinguished. These actors provide different types of data and expertise (see the table below).

Table 22: Types of actors along the data value chain and their respective contributions to it

Type of actor	Contribution to the data value chain
Chemical company	The chemical company generates data through their activities. The data is generated by the machines used for these tasks, as well as from sensors deployed.
Data company	Aggregates the data and provides the analytics
Third-party providers of data expertise	Data scientists which are freelancers, software companies, research organizations carrying modelling and data-specific activities that support the activity to the data company. Data company networks with a set of stakeholder to provide the analytics services to the chemical company (client).

Source: Deloitte

Business model and actors: A typical service offering

Big data is undoubtedly impacting the way chemical companies operate and grow their businesses. They are today shifting away from the pay-by-the-ton revenue model to provide more value-added products and services to their customers. The present strategic moves of each of those companies will have an impact on their future competitive advantage, taking into account that it is a highly competitive market where each player needs to differentiate itself from the rest.

Some examples of chemicals companies going beyond the offer of traditional products, include for instance services provided via apps or software that seek to help customers to determine the right choice and application of chemical products. Chemical companies are starting to offer “Smart solutions”, that go from product to service offering.

Example: Eastman Chemical offers an online "solvent comparison tool" and a web-based "resin calculator" for its coatings customers. This tool is helping other businesses to compare resins and solvents based on a technical description of their properties. When the user of the tool introduces a selection of raw materials and resin parameters, the model carries a set of calculations to suggest a resin product that meets the desired parameters[309].

Another illustrative example of this business model shift from "product offering" to "service offering" by using of big data, consists in traditional manufacturers who in addition to selling water-treatment chemicals, are starting to provide water-treatment recommendations to their customers based on site visits and their understanding of materials and assets. Thanks not only to big data but also in general to Smart production trends, chemicals companies have direct visibility into and interaction with their customers' operations, and can provide real-time recommendations to optimize the operations and improve the design of water-treatment facilities[310].

The current challenge for chemical companies is therefore how to enhance business operations via asset optimization, process and energy management, and safety processes, while thinking in parallel about ways to grow their business through advanced material discoveries, smart chemical products, and new service-driven value propositions. For this reason it is critical that they prepare their technology but also their data landscape to support the progressive changes in their products, services and new business models to achieve a competitive advantage for themselves in the long-term.

Potential contractual barriers

This section provides a brief analysis of potential contractual barriers, businesses in the chemicals sector may face.

Data ownership, access to, and (re-) use of data

Currently, as illustrated above, chemical companies usually **sub-contract data analytics** to third companies. Therefore, due to the contractual relationship between the parties (sub-contracting) and the common business practices in the domain, the question of data ownership in the chemical sector is rather clear: the data-holder company (the chemical company) is the owner of the data.

Given that data-sharing between businesses and third party organisations is still a very limited practice within this sector, the (re-) use of data and its potential impact in generating great business value is still to be seen. Data companies, such as Yukon Digital, are today providing the analytics services to the data gathered by the chemical company (data-holder such as BASF), and by contract they do not have right to (re-) use it for other services that go

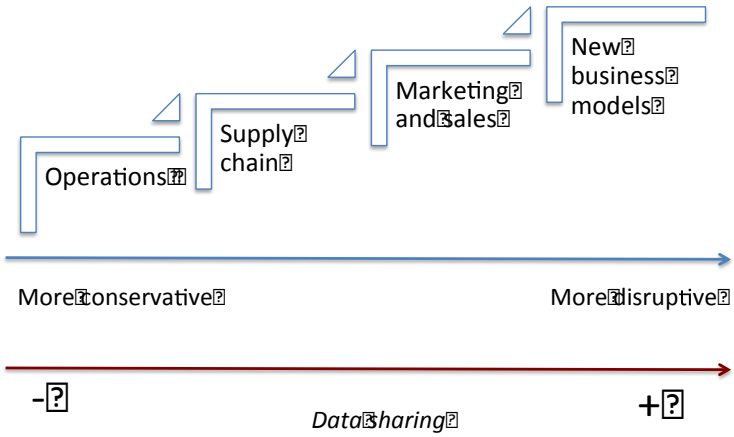
[309] Eastman Chemical, "Online tools," http://www.eastman.com/Products/Pages/Chemical_Wizards.aspx, accessed April 5, 2016

[310] Ecolab, "Water management technologies," http://www.ecolab.com/innovation/core-technologies/water-management-technologies/, accessed May 12, 2016

beyond those provided to the chemical company releasing the data. Still today, Yukon Digital has not been able to (re-) use the data provided by their clients in any other circumstance.

Companies providing data analytics services see a considerable potential in the possibility of re-using data from third parties because they would have the possibility to merge great amounts of data from different datasets, which could generate intelligence and business value for their customers (Cattaneo et al., 2016). In addition, this type of intelligence provided by data companies, would support chemical companies not only in the areas of operations and supply chain, but also, more interestingly, in their shift to new business models based in service offerings with greater value added.

Figure 28: Application domains of big-data related to data-sharing practices



Source: Deloitte

Usually, when implementing big data, chemicals companies use as a starting point the areas in which they already have a strong background, that is to say mainly operations and supply chain applications, and then they move onto relatively newer, more complex applications, merging their data in market forecasting and finally generating new business models. This progressive move from the application of big data to operations only to the generation of new business models is accompanied by increase in the companies' abilities to merge different datasets coming from different data sources generated by third party players, and thus their capacity to (re-) use data.

According to the expert interview, in the last ten years, there has been a lot of focus on process harmonisation and the standardisation of systems, trying to drive down costs as companies globalised the market. Most companies developed a lot of systems, to archive their records, capture information in the value chain and in marketing and sales, and to store their information in the manufacturing area. However, there is still a lack of optimisation of the data collected and this constitutes the focus for the coming years.

Risk and liability

With regard to risk and liability in the B2C context, the interviewees argued that the purpose of data exchange is to improve the performance of the players along the data value chain.

In that respect, risk and liability does not constitute a very mature issue at this stage for the data access and sharing although is a key aspect for the relations between the chemical company and the data company providing the analytics. The data company in fact only provides recommendations to the chemical company which can then decide whether or not to implement them. Liability issues will increase in importance when there will be even further automation and smart production within the sector. The type of recommendations that the data company provide consist in suggestion of this style: "according to our calculations, with this percentage of probability we predict this particular failure in the equipment". Currently, the data company just provides the results as recommendations to the client, and the implementation or not relies in the executive and operational management who takes the decision.

There are several reasons why liability does not concern the data company directly:

- First, the data company is still too small to bear this liability. The responsibility of shutting down a chemical plant involves millions of dollars.
- Secondly, the maturity of the predictive modelling that the data companies are offering is still not extremely high (e.g. 80% of probability of prediction that something happens, but there is still a remaining 20%).
- Finally, even when you predict or even when you know that something is going to fail or that there is an anomaly in your chemical plant, the key question remains what you are going to do. This suggests that there is an entire action plan and change management process the operational and executive staff in the chemicals plants have to put in place with goes beyond the data company responsibility. Globally, the scope of the collaboration between the chemical company and data company has not achieved yet such mature stage to be subject to these liability challenges.

Potential non-contractual barriers

Firstly, the ***access to data*** is one of the main barriers**.** Although the clients are theoretically open to share their data with the data company, the latter usually experience difficulties when trying to download the data, and the in terms of data storage and exchange (e.g. via mail is not safe enough for some companies). Sometimes, access to data also requires for the data experts to have preliminary access to databases and understand the data available, clean it so that the data company can work on it. Although data companies would generally prefer to store the data from the chemical companies in the Cloud, there is a strong aversion of the sector for this practice because of the sensitivity and risks linked to uploading the data in this system.

Another of the main barriers to data access and sharing in the chemical sector is that companies do not see the benefit of doing it. Furthermore, they point out at the potential threat which would be constituted by competitors having access to these data directly or at the possibility for the data company to develop software or added value services for their competitors by using this data, which could damage their competitive position in the market. Other type of partnerships and revenue models should be foreseen between the chemical company and the data company so that they would have incentives for sharing the data.

Other non-contractual bottlenecks include ***cultural barriers***. The chemical industry is about assets, that is to say "steel in the ground". As Sean Jones, founder of Yukon digital, explains: "*The topic of IT has always been one to avoid and most IT departments are still organised within the CFO function, which means it is more about minimizing costs. The topic just appears to be not as "sexy" as others, but we have probably also not seen the real use cases in many areas outside of process optimization in the last five years. So, naturally, people rightly ask: where is the business case?*" As he explains, describing and presenting business cases is something that has not been effectively done by consulting companies or IT companies who sell software. Therefore, this is something that data companies specifically address when they meet with a potential clients within the chemical sector in order to engage with them.

Consequently, typically data companies start collaborating with chemical companies in what is considered the "easiest" areas for the clients in terms of business cases: operations aimed at increasing productivity. As the interviewee put it: "*We are starting in manufacturing, because it's easier to explain and the use cases are somehow clear*".

Although data companies already see the larger business value creation and the opportunities with respect to marketing and sales and to new business models, they start focusing in this area that has a clear business case for the chemical company. CEO usually asks them how those big data company are going to help them. As Sean Jones explain, because marketing, pricing and sales are exposed to such a volatile environment, compared to manufacturing and supply chains, they start with those areas where the executive management is more open to get started with.

This culture and combined with the risk aversion approach explain why there are such incremental changes in big data usage in the chemical sector. As Sean Jones from Yukon Digital describes: "*I think it will probably take another two to five years for it to fully arrive on the executive agenda. In the chemical industry, margins are just bigger, compared to sectors like retail, which have already heavily adopted data-driven solutions and even transformed their business models accordingly. In the chemical industry, there is still no pressing demand and – to some extent – a lot of companies seem to just wait and see, sort of go with the flow*". Although there are a couple of strong innovative companies who are leading in the usage of big data, until they have proven their initial success, the rest will wait. In consequences, some data companies like Yukon Digital try to focus on larger clients to help them increase margins so that other players within the sector will notice and follow.

Technical barriers

Some of the technical barriers that chemical sector face for data-sharing is related to how data is managed. The client company gathers heterogeneous dataset from different IT systems, and provides them to Yukon. They could refer to data from sensors in the plant, from internal IT management, from laboratories. Data are neither standardized nor interoperable; they are gathered by the client company and transmitted to Yukon via traditional means, such as e-mail, cloud, and sometimes in-site analysis.

Yukon carries out an intensive effort to harmonise the data and make them usable. However, this work used to employ 90% of the resources of the projects, while today thanks to in-

creasing openness of the systems it only requires 50%. Hence more resources can be devoted to actually analysing the data and providing added value, rather than polishing them.

The effort for data harmonization and cleaning is part of the services provided by the company, but certainly it raises the costs of big data analytics without producing visible benefits for the client. In a recent interview, Yukon founder Sean Jones puts it clearly: *"connecting different data sources together is still one of the biggest challenges – whether it is for internal or external processes. Additionally, the data is oftentimes not just stored in an operational storage but also in laboratory information systems. So bringing the different data with different formats together and then merging it into a data set that is adequate for predictive work is one of the biggest challenges."*

There is a clear trend towards greater interoperability of the data provided by the different IT systems and sensors. In perspective, the benefits of data sharing are becoming more visible to data holders, and the costs of data curation are going down. That could pave the way to a strong acceleration in innovation, in particular when it comes to applying machine learning techniques and artificial intelligence to industrial data.

Aviation and aerospace

"Aerospace is one of today's most data-intensive industries. Today's aircraft contain sensors and embedded computers which are constantly generating data"[311]. Airports, Air Transport Companies and aviation service providers in Europe all rely on accurate and timely data for delivering their services and they are also forced to exchange some of these data in order to function. However, as mentioned in chapter 2.1.2, the aerospace sector is characterised by a rather in-house approach to data and its exchange is not very frequent besides the sharing of information needed in the context of Air Transport Management systems (ATM). The latter does not concern directly the domain of B2B data access and sharing as it results from legal and security obligations coming from the different countries and the EU and it does not entail directly the creation of new services or business models, also considering that the provision of data from ATMs to business operators for commercial purposes is unlawful.

Nonetheless, as argued in the business model chapter, analytics services might be subcontracted to third companies and there are also new apps building on data generated by the ATMs and flights providers. An example of such an innovative business is for instance FlightRadar24. This is a flight tracker that shows live air traffic from around the world. "Flightradar24 combines data from several data sources including ADS-B, MLAT and radar data. The ADS-B, MLAT and radar data is aggregated together with schedule and flight status data from airlines and airports to create a unique flight tracking experience"[312]. However, most of the apps developed within this sector concern the airline companies internal flights and do not entail exchange of data.

At the same time, within the aerospace value chain, exchange of data between components manufacturers and aircraft manufacturers or between manufacturers in general and airline companies are more and more frequent. For instance, manufacturers of aircraft sometimes analyse data of the airline companies in order to provide them with predictive maintenance services. Although this still happens on a more case-by-case basis and the market is still emerging, there is a strong interest in this sector for such types of business models and services.

The present chapter analyses the aerospace sector from two main perspectives: the perspective of organisations delivering Air Transport Management in Europe and the perspective of aviation and aerospace companies. The combination of these two angles allows to have a comprehensive view of this sector which, although being extremely data intensive, does not offer yet full maturity in terms of B2B data access and sharing.

[311] See: https://www.cmu.edu/news/stories/archives/2015/october/boeing-analytics-lab.html
[312] See: https://www.flightradar24.com/how-it-works

The Air Transport Management (ATM) perspective: Eurocontrol

Context and actors

Eurocontrol is "an intergovernmental organisation with 41 States, committed to building, together with its partners, a Single European Sky that will deliver the air traffic management (ATM) performance required for the twenty-first century and beyond"[313]. This organisation is, inter alia, in charge of:

- The European air traffic flow management system on behalf of its Member States and the European Union as "Network Manager": which manages air traffic management network functions (airspace design, flow management) as well as scarce resources (transponder code allocations, radio frequencies), as defined in Commission Regulation (EU) N° 677/2011.
- The Maastricht Upper Area Control Centre, which provides an air traffic control service for the Netherlands, Belgium, Luxembourg and northern Germany.
- The Central Route Charges Office, which handles the billing, collection and redistribution of aviation charges.
- Supporting the European Commission, EASA and the national authorities in regulatory activities.
- Contribute to research in the domain and in the activities of the SESAR Joint Undertaking.
- Coordinate civil-military aviation dialogue in Europe[314].

To fulfil the tasks set out in the Eurocontrol international Convention and related Instruments, this organisation relies heavily from data coming from third parties and especially from airports and airline companies.

Article 8 of Commission Regulation (EU) N° 677/2011 in fact establishes that: "the operational stakeholders shall provide the Network Manager with all the relevant data"[315]. The data concern primarily routes, radio frequencies, Special Service Request (SSR) codes, position reports and other operational data. These data, once collected and processed by Eurocontrol, are made available by the latter to airline operators through the Data Distribution to Aircraft Operators (DDS to AO)[316]. "This flight data consists of the 4D flight profiles calculated by the Network Manager Operations Centre. These 4D flight profiles are initially calculated from the flight plan received, but they are regularly re-computed to take into account the latest information received, such as surveillance data"[317]. This service is currently available free of charge but on subscription basis. However, this solution is only provided to Aircraft Operators.

[313] See: https://www.Eurocontrol.int/articles/who-we-are
[314] See: https://www.Eurocontrol.int/articles/our-role
[315] Commission Regulation (EU) N° 677/2011 laying down detailed rules for the implementation of Air Traffic Management (ATM) network functions and amending Regulation (EU) n. 691/2010, see: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02011R0677-20150101&from=EN
[316] See: http://www.Eurocontrol.int/publications/data-distribution-aircraft-operators-dds-ao
[317] Ibidem

Towards a wider public, "until very recently, Eurocontrol had a policy of **non-disclosing data unless**". In 2012, this policy was reverted in **disclosing data unless not**"[318] due to new EU level obligations increasing transparency and access to documents held by administrations for citizens. However, in the past few years, according to an internal report of 2013, this did not translate automatically into major openness of data. This is due to the strict confidentiality requirements put on Eurocontrol by the data providers in the form of legal contracts. Most of the data are commercially sensitive in the sense that their disclosure to the public is likely to prejudice the commercial interests of the data providers. In addition, the agreements that the organisation has with the ATM data providers limit the use of their data for operational and technical purposes related to the tasks of Eurocontrol, also as Network Manager for the EU.

The section below goes more in-depth into the main obstacles to the exchange of data between Eurocontrol and the above mentioned stakeholders.

Access and (re-) use of data

Eurocontrol exchange data based on contractual agreements which determine conditions for data access and (re-) use as well as all the other aspects of the data management. Eurocontrol obtains enormous amount of data from different organisations/companies and for different purposes (ranging from air transport management and safety reasons to R&D and environmental policy needs, to name a few). Obtaining the data is not an issue for Eurocontrol as it is foreseen in its tasks in International Convention and related Instruments, and carried out also in direct application of the European Union ATM network functions laid down by European Union law.

The bilateral contractual relationship in place for obtaining the data also has implications in terms of sharing the data with third parties. Regularly in fact, Eurocontrol receives requests from third parties (research centres, individual, other international organisations, businesses) for datasets which are not immediately available on the website. Whenever an organisation requests Eurocontrol for data the latter has produced or received from third-parties in executions of its tasks, Eurocontrol checks whether the data can be disclosed or not, based on its legal obligations towards the data sharers. In case of doubt, it goes back to the data originator asking for the permission to share the data. In most cases, the data originator has an interest for granting the permission as it is for instance the case when datasets are used for research purposes. Nonetheless, it happens that the data originator denies the request for access of these third parties and in this case Eurocontrol strictly respect this position.

It must also be considered that Eurocontrol is often not authorised in the legal agreements to transmit data to third parties which can aim at exploiting them for commercial purposes. This also explains why the (re-) use of data for commercial purposes is not acceptable for

[318] An air traffic management data regulation on public access was adopted by the EUROCONTROL Agency to enhance the handling of requests for access to data from third-parties, including the general public. See in this regard Open Data for Air Transport Research: Dream or Reality?, Marc Burgois and Michael Sforyeras, 2014, see: http://www.opensym.org/2014/08/12/open-data-for-air-transport-research-dream-or-reality/

data originators. Nonetheless, Eurocontrol has the obligation to verify not only that the use of the data from the third parties is lawful but also that the release of data is possible with respect to the obligations pending on Eurocontrol itself. The various services in the Agency represented in the Eurocontrol Data policy advisory group, are in charge of examining the requests for the access of data and checking the compliance with all the obligations. In most cases, there are international regulations or special agreements establishing a right of access on Eurocontrol data from certain players (e.g. other international organisations, Member States) but requests from non-aviation players must each time be examined carefully.

Since the datasets are enormous and composed of many different sources (regulated by different data protection regimes and contracts) this task of processing the data and handling requests for access and (re-) use is becoming more and more difficult and resources consuming. This is the reason why the role of Eurocontrol is considered so important in managing air traffic management data in the interest of both the aviation community and the general public.

Liability and risks

Liability clauses and penalties in case of misuse of data are defined in the contractual agreements. Eurocontrol indeed negotiates safeguard clauses in these contracts and also monitors the (re-) use of the data by the organisations which requested the access, in order to spot irregularities. Whenever such control results in the identification of cases of misuse, Eurocontrol contacts the organisation in order to ask the withdrawal of the data and, in extreme cases, can also prevent any further access of the organisation to its datasets.

Interoperability and other barriers

Interoperability is not a barrier for Eurocontrol in gathering and dispatching data. The interpretation of data itself on the other hand could be an issue in some situations. Mostly, Eurocontrol gives back the results obtained by data to the data originators in order to a) validate its interpretation and b) provide a return in investment to the organisation sharing the information. This system of validation and incentive is a solution to the problem of interpretation of data, which can be difficult without the involvement of the data originator.

Conclusions

There are no major barriers preventing Eurocontrol from carrying out its data related activities. This is also due to the specific agency's responsibility and its role in the overarching aviation framework. However, the burden of checking the compliance of each data request against the applicable contracts should not be underestimated. Discussion with aviation organisations on these topics could be encouraged to share experiences and identify possible approaches to the common challenges.

Aircraft and aircraft components manufacturers

Context and actors

In the aviation and aerospace sector, it is difficult to talk about business models concerning data in general terms. The business models in fact present different characteristics according to the types of data considered:

- In case of data generated by the aircraft themselves (e.g. data from on-board sensors, equipment faults and warnings, etc.) also mentioned as operating data by some interviewees, the amount of data exchanged remains rather limited for the moment. The exchange of this kind of data happens on the basis of bilateral contracts (also including non-disclosure agreements) between the parties, for instance between an airline and an aircraft manufacturer. Moreover, the exchange of this data generally only occurs for specific reasons (such as improving fuel efficiency, improving airline decision-making through a better knowledge of the state of the aircraft and allowing predictive maintenance activities for instance) and in the framework of the provision of additional services, e.g. by the aircraft manufacturer, to the party opening up the access to the data, e.g. the airline.
- This should be distinguished from the regime applicable to other types of data such as technical data. For instance, product information (data related to the design, production, maintenance or operation of a product (e.g. technical information such as configuration dossiers) is exchanged in a very extensive but controlled way. In fact, delivering such data, even in part, is a core element of delivering an aircraft. Of course this type of data is subject to intellectual property rules, legislation, and contractual conditions[319]. Such data is also very sensitive in the sense that uncontrolled disclosure can quickly have safety impacts.
- Commercial data can also be very sensitive and, as in other industrial sectors, are considered a key asset by the businesses which therefore try to protect them through trade secret or IP legislation. This type of data is not normally exchanged.
- Satellite service typically entails a bigger exchange of data in general (as for instance in the case of images of the earth or other geospatial information which are exchanged with different national and international agencies or private customers). However, one should be careful to treat aviation and space sectors separately as they follow different logics with respect to access to data.

Identified barriers

Data ownership, access to data and contractual barriers

Aircraft manufacturers and airlines do not use the term ownership with regard to data generated by the aircraft themselves. These raw data typically do not currently carry intellectual property rights, unless they are structured in databases (which then can be legally protect-

[319] Other types of data can be considered. For instance, Aircraft Communication Adressing and Reporting Systems transmit to ground stations data relating to the geolocalisation, speed and altitude of an aircraft. Such data is provided in a public and non-controlled manner. It is used notably for real-time aircraft tracking.

ed)[320]. The aircraft manufacturer or aircraft component manufacture is not typically in possession of the data generated by its aircraft, the airlines or lessors owning such aircraft are. Indeed, the interviewees mentioned a "pragmatic approach" which relies on the concept of "data sovereignty" of the buyers of the aircrafts or components, that is to say the airlines companies. To obtain access to data generated by the aircraft, the aircraft manufacturer therefore needs to gain access to data through negotiations with the airlines. Such access is given to allow the provision by the aircraft manufacturer of services to the airline (e.g. to address fleet improvement issues or to increase the efficiency of the vehicle). The operators give access to such data only when they have a commercial interest in doing so. The agreement on the access to data is therefore reached on contractual basis.

This contractual dimension implies that there are negotiations to be carried out, which are already challenging for large players in a B2B context and could be even more difficult for other smaller components suppliers or SMEs, for which the balance of power is more similar to a B2C relationship. Indeed, as argued by one interviewee, the reliance on contracts for the exchange of data does not pose particular issue in a pure B2B dimension and amongst players with similar bargaining power. However, bigger players can impose clauses on smaller players if the relationship is really unbalanced, as it happens with companies imposing clauses to consumers. Also, this shows that access to data is only granted in a rather limited way, as for instance only to support service provision.

In terms of (re-) use of the data exchanged, the limits of this practice are defined in the contracts signed between the parties. This entails that, whenever there is a case for using the data for another purpose, the contract needs to be renegotiated. This constitutes a speed gate, as it takes time and might be another limit of the contractual/bilateral approach.

It must also be noted here that contractual agreements vary greatly from one to another. For instance, the question of what is personal and what is non personal data is addressed differently by different airline companies. Indeed, it is rather easy to come down to a specific pilot driving styles when carrying out efficiency analysis of the aircraft. As one of the interviewee argued, at this stage of the technological development the performance of the machine is usually the same but the driving style might have an impact on safety, consumption of fuel etc. Therefore, for some companies the level of anonymization of data and the granularity of the analysis performed on them must not allow for the identification of single individuals while others have a more flexible approach. These contractual issues are dealt with on a case by case basis, depending for instance on the activism of the pilot trade unions of one specific airline companies etc.

[320] To provide a full picture, it should be noted that data *per se* can attract IP protection (or at least this cannot be simply ruled out) possibly via proprietary data formats and as tabulated information in a software form (protected in the same way that software can be protected under copyright). Data can also be considered as confidential depending on context. Also, the raw data are in fact 'created' technically – perhaps not in the sense of a human-authored copyright work, but one could not exclude the possibility of machine-created data as having the status of IP and having been 'created' as understood under IP law. Contemporary IP law in technology contexts is constantly adapting to 'new' situations such as this.

Hence, this bilateral approach to exchange of data "leaves some business opportunities on the table" as argued by one of the interviewees. In this perspective, manufacturers also consider how to provide enhanced access to third parties to the operating data coming from their products. However, in this respect, there is the challenge of analysing and interpreting the dataset and to derive technical information from it (reading the data generated by a specific sensor on the aircraft, for instance, does not present much added value unless you know for instance exactly where the sensor is situated and its relation to other sensors and components). For aviation, access to operating data must also be controlled to prevent security and safety risks. In this complex sector, understanding the meaning of the data and ensuring its security and integrity therefore goes in parallel with their access. A deep knowledge of the structure of the aircraft and the interplay of equipment and sensors is needed to interpret the data (such knowledge being itself IP protected).

In general, some companies argued that more access to aircraft data could be a way of improving the efficiency and airlines overall as the company would be in the position of interpreting better how the aircraft is behaving and identifying earlier potential safety or performance issues. More immediate and thorough access to data could lead to more anticipation of risks which would result in increased safety, efficiency, and environmental performance of the sector in general, to the benefit of citizens. It must be noted here however, that some interviewees had a different position, suggesting that that sufficient safety of the airplane operations is already guaranteed without large exchange of operating data. Therefore, according to some manufacturer companies, the exchange of operating data would rather have an effect in terms of increased efficiency of the airplane than in terms of safety of passengers. This is important as one could see a case for imposing opening of data in case of increased safety but one would not be so inclined to impose access for increased operational efficiency only.

However, the manufacturers do not advocate for a hard policy measure forcing operators to open up access to data, which may be business sensitive. It could also expose the aircraft to serious security and safety vulnerabilities, by potentially providing opportunities for hackers or ill-intentioned actors to access deep and sensitive technical details of the aircraft design and operation. Due to the complexity of the sector, the competition on the aviation business and the multiplicity of stakeholders' interests, such a regulatory solution would finally be very difficult to develop. Furthermore, a relevant regulation would also need to distinguish between the diverse potential objectives of data sharing:

- Is the access to data aimed at developing new products or improving existing products?
- Is it aimed at increasing safety of the aircraft?
- Or to improving efficiency of the operations?

These different purposes do not present all the same value for the society and therefore do not all justify the same policy measures. Currently, in the aviation sector there is no regulation preventing companies from exchanging data or enabling them to do so, as it happens in other sectors. The sector is very heavily regulated, by the EASA agency (which depends directly from DG MOVE) as well as by the ICAO organisation (UN) at the international level. . A

sectorial approach is therefore very important as there is a particular security and risk framework that needs to be respected by all players. In addition, for this sector in particular, the international dimension is crucial as airlines from non EU countries operate in Europe and because the market is global. Airlines operate on a worldwide basis, aircraft and equipment manufacturers sell on a worldwide basis. Therefore EU measure forcing companies to open up access to their data would raise concerns as to its admissibility and enforcement in non-European countries. Maintaining an even playing field in this sector is key.

The airlines in general do not seem to have a common and clear approach to sharing data as there are many questions still unanswered. The result is a case-by-case situation: sometimes they accept to share their data (for the performance of services) sometimes they are more reluctant due to competition concerns. Airlines in fact need to balance two interests: exchanging data and generating value on one side, or losing advantage if data are made available to competitors. Also, various types and sizes of airlines exist, which are not all as well equipped to manage a data policy.

It would in any event be useful to create a discussion around data at the sectoral level to go over these challenges and opportunities (for instance through a sectoral discussion forum).

Data liability and risks

Due to the bilateral/contractual approach to data exchange described above, liability clauses are included in the services contract associated with the data. This is similar to what happens in the framework of any other type of contracts and does not pose a major issue for the moment.

However, it must be noted here that the manufacturers pointed out the potential issue of linking more access to the data with more liability. This is to say that, in case a manufacturer would obtain more access to the vehicle product or equipment data, one should not held the company liable for processing all the obtained information and providing alerts on the risks. It is in fact impossible to constantly process such a volume of data and have a preventive analysis of what could happen in real time. Therefore, although more access to data would be allow to improve the situation, notably from a security perspective, this should not entail a modification in the liability regime binding for producers of the vehicles or equipment in case of damage occurred to third parties or to a contractor, which may have been mitigated or avoided if data analytics would have been performed.

Data interoperability

There are some issues linked to interoperability in the aviation sector as this barrier was mentioned by all contacted interviewees standing in different position within the value chain. In fact, the many different parts of the vehicle aircraft can be provided by different vendors and therefore interoperability must be ensured. For instance, the data collectors are produced by one vendor. The data collector sends the data to a router (which can be provided by multiple vendors) and then the router sends the data to the ground. The airlines must therefore guarantee interoperability across all these components, which is costly to do. Many airlines do not capture detailed technical data due to this complexity. This is also due

to the fact that big and small airlines do not have the same resources for ensuring interoperability. Once again, the coherence at the international level is important for interoperability as airlines and manufacturers operate in multiple national markets.

As argued by one interviewee, interoperability is a truly transversal barrier in the aviation sector and sectorial standardization activities would be welcome to address this shortcoming which imposes further costs on all actors of the value chain.

Other barriers

Another truly transversal barrier mentioned during the interviews is cybersecurity. Indeed, the risk of seeing the data stolen and misused can also be considered as a main obstacle to sharing data and information, especially if businesses do not trust each other cybersecurity systems. At the same time, cybersecurity risks are unavoidable and can only be mitigated (also through industry level initiatives possibly), not extirpated.

Machinery data in global value chains and industrial platforms

Within this domain, we cover features of machinery data in global value chains and industrial platforms in general as well as **MindSphere** – Siemens Cloud for Industry and an example of a Mindpshere customer (Gehring, provider of honing machines and services), furthermore a typical service offering of the machinery firm TRUMPF/AXXOOM, and another service example from the field of (IoT connected) professional Coffee Machines.

Context

The initial situation within the market

Modern industrial production is not anymore a business where single and parallel working value chains are established. Instead, modern industry is a platform based business in which sectors or manufacturers establish their own technical form for data and information exchange and form more flexible production and service networks instead of subsequent chains.

Data-driven industrial production is also referred to as Industry 4.0 in Germany[321] or in the USA as the "Industrial Internet Consortium" (IIC).[322]

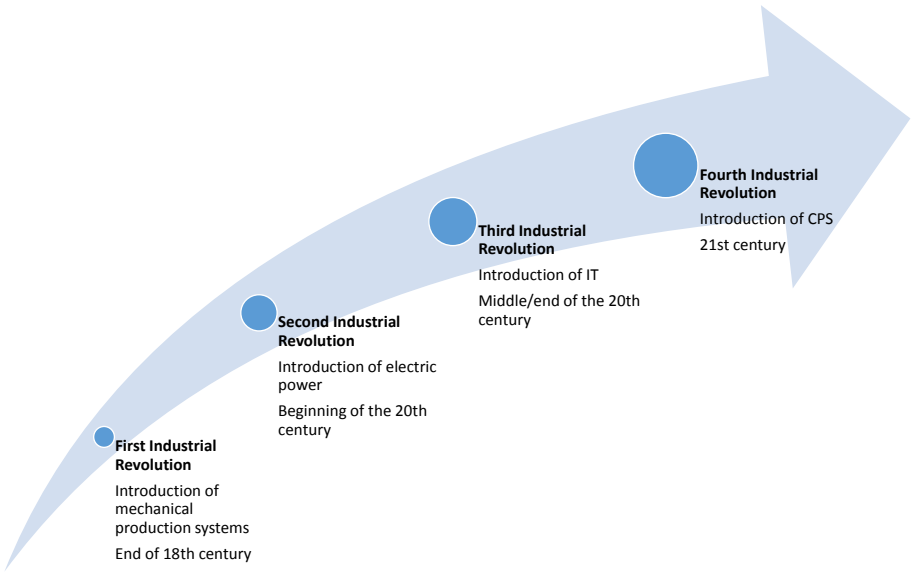
In a data driven industrial production, component suppliers, also customers, and other subcontracted service suppliers generate data, for example through sensors in the production chain, in the after sales services, or through additional services. Modern industrial production "integrates manufacturing with state-of-the-art information and communication technology. This smart approach makes it possible to deliver tailored products to meet individual customer requirements - at low cost and in high quality. The Industry 4.0 factory looks like this: smart machines coordinate manufacturing processes by themselves, smart service robots cooperate with people on assembling the products, and smart (driverless) transport vehicles cover the logistics side on their own. Industry 4.0 defines the entire life cycle of a product: from concept to development, manufacturing, use and maintenance - and on to recycling."[323]

[321] Industry 4.0 is a German agency comprised of government, business and trade union officials, which promotes the computerization of manufacturing and supports its implementation. It also focuses on focus on systems security, work and education training, and legal issues, see http://www.plattform-i40.de and see GTAI – German Trade and Invest (2014): Smart Manufacturing for the Future, https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf

[322] The Industrial Internet Consortium is the global not-for-profit public-private partnership of 250+ member organizations to accelerate the Industrial Internet, to share best practices and to solve the challenges like interoperability and security, see https://www.iiconsortium.org/. Both initiatives collaborate on a roadmap to future interoperability.

[323] http://bmwi.de/EN/Topics/Economy/Industrial-policy/industrie-4-0,did=708234.html

Figure 29: The evolution of industrial platforms – Industry 4.0



Source: based on BITKOM 2014, adapted by WIK.[324] (CPS: Cyber Physical Systems)

The above figure depicts key developmental steps of industry development from the end of the 18th century to the present, as well as the expected future dominated by data exchange.

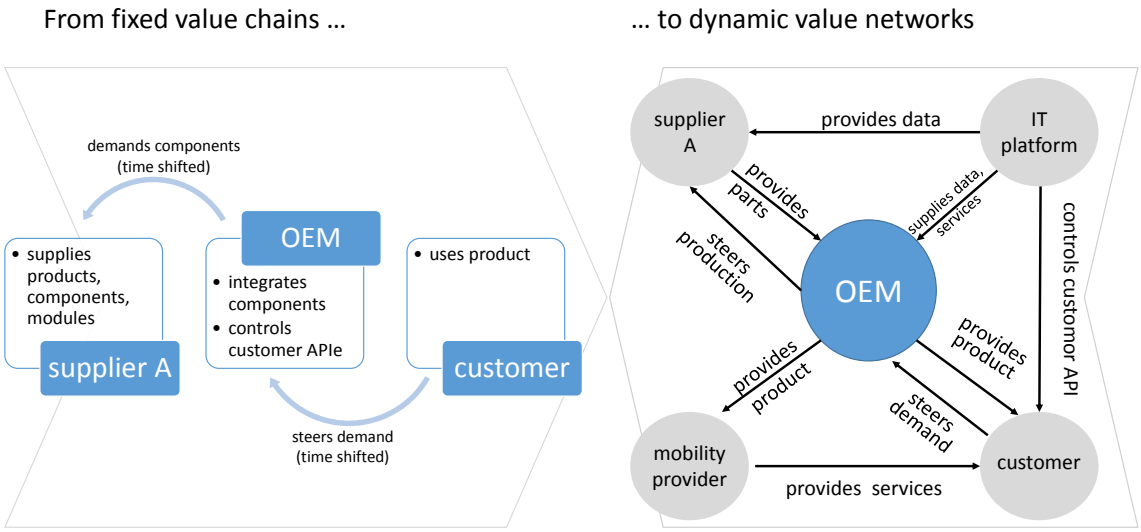
Until today, industry developed from an extremely labour-intensive field of work in which entrepreneurs focused on mechanisation and automation to a value chain of dependent stakeholders driven by digitisation.

One of the main challenges of today is that the vertical integration of the value chain is replaced in favour of dynamic value networks (see figure below)[325] In these networks, partners for products, components and modules supply can be chosen in a more flexible way. All partners of the network add to its information basis and the production process is not any longer steered by demand of the original equipment manufacturer (OEM) but more by the data services provider who controls the access to the customer API and supplies (near) real-time data to the whole production process.

[324] See BITKOM (2014): Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland. Study, p. 10.

[325] See Roland Berger Strategy Consultants (2015): Die digitale Transformation der Industrie. Analysen zur Studie. Im Auftrag des Bundesverbands der Deutschen Industrie e.V., 17. März 2015, p. 10.

Figure 30: Transformation of value chains to value networks

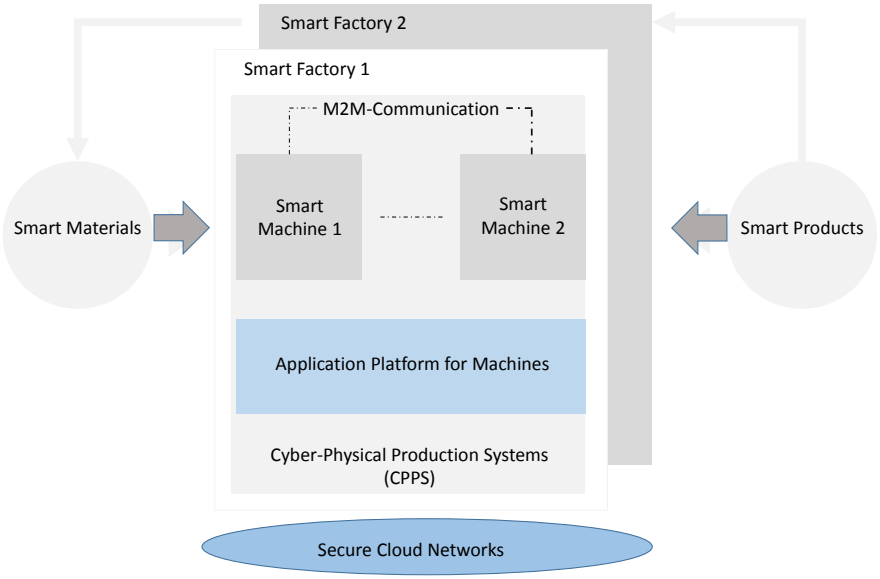


Source: Roland Berger (2015), adapted by WIK

For small and medium enterprises (SMEs) as well as the skilled crafts sector, the take-up of relevant digital technology has still to be improved.[326] These companies have to invest in relevant data, soft- and hardware, as well as other technology to become part of the network complexity of Industry 4.0.

Data generated in an Industry 4.0 environment can be analysed by a third party service provider and be send back to the respective client or, on an anonymised basis, to the whole sector platform community or other third parties like e.g. sector regulators or benchmark designers. In such a smart factory pipeline cloud based secure networks play a central role (see figure below).

Figure 31: Industry 4.0 Smart Factory Pipeline (cloud based secure networks)



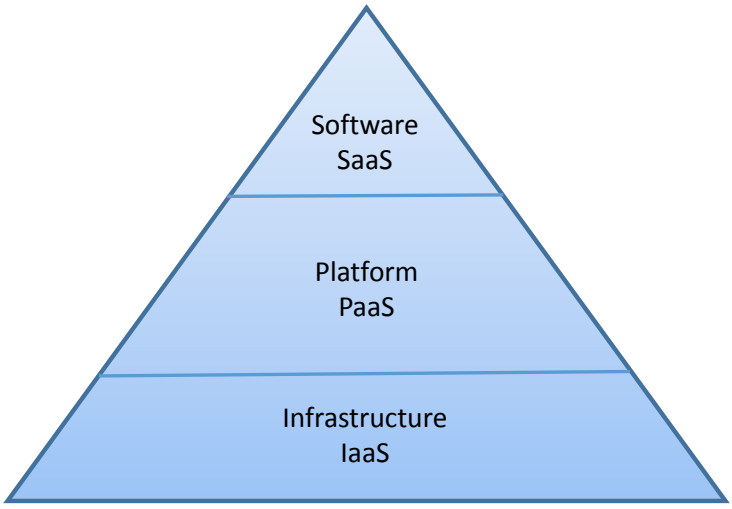
[326] For example, the German Government fosters this development with their programme SMEs-digital.de

Source: DFKI 2012, adapted by WIK

Cloud solutions, i.e. virtual storage and collaboration platforms accessible via the Internet, enable all suppliers and especially SMEs to overcome their limited resources for Industry 4.0 IT investments through smart use of the following options:

- Infrastructure as a Service – IaaS: remote access to IT infrastructure for flexible and scalable storage of large amounts of data
- Platform as a Service – PaaS: remote programming environment to develop and offer IT services within the own company or to third parties
- Software as a Service – SaaS: remote access to software solutions and dedicated services, options to composite applications for own use or third parties.

Figure 32: Cloud service levels



Source: based on Lenk, Alexander et al.: What's Inside the Cloud? An Architectural Map of the Cloud Landscape. FZI Karlsruhe/Hewlett-Packard Laboratories, 2009, adapted by WIK

Cloud computing is defined by NIST as follows: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[327]

By using cloud services – or industrial online service platforms – companies outsource IT infrastructure services (running a network, store data, basic computational services), use a remote environment for programming and executing data analysis and they set up applications, basic as well as refined to create their own business offers.

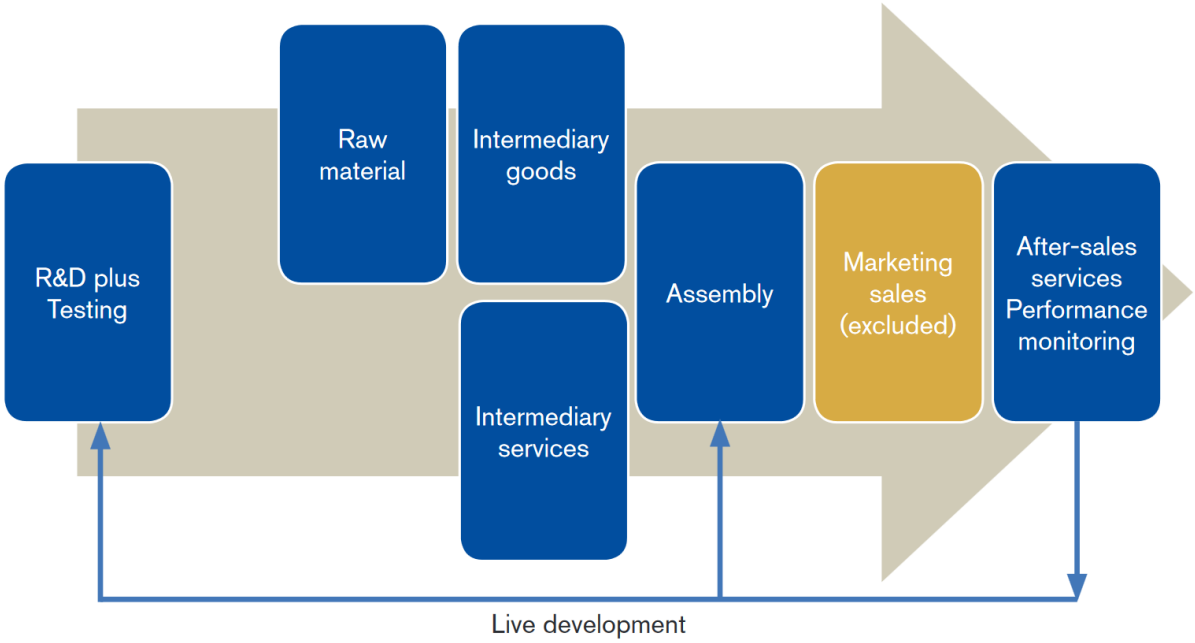
[327] For a definition of cloud computing see SP 800-145, The NIST Definition of Cloud Computing (September 2011), p.2.

Industrial production today

Industrial production today is characterised by global value chains. Production sites are commonly scattered around the world. Consequently, there has been significant motivation to find ways to monitor and maintain machines remotely implying a need to transfer at least some rudimentary data across production sites and most likely across countries. With new possibilities to collect, transfer, store as well as analyse data and the significant economic potential originating from 'industry 4.0' (especially in the context of Industrial Platforms) the motivation to use data is increasing. In fact, the free movement of data is essential to any efficient production process today.

The figure below provides an overview of a typical global value chain and the types of data that originate at each step. Equally, at each step some part of machinery is involved. This machinery reflects the full scope of products that companies from the sector typically produce, sell, and monitor as well as maintain. It reaches from small components or even individual sensors or actuators over individual machines up to complete assembly lines that are planned, configured, and put to work by specialized companies. Commonly, they mix and match their own machines with machines from third party vendors in order to cater the clients' specific requirements.

Figure 33: Simplified global value chain



Source: Kommerskollegium (2015)[328]

Research and Development (R&D) including testing of prototypes is commonly the first step where machinery producers are involved in global value chains. At this stage, data is commonly transferred in order to be analysed by third parties such as research institutes to iden-

[328] Kommerskollegium (2015) No Transfer, No Production – a Report on Cross-border Data Transfers, Global Valuje Chains, and the Production of Goods. Stockholm: Kommerskollegium National Borad of Trade of Sweden.

tify the best configuration of a specific machine or in the case of planning a full assembly line the optimal set-up and interaction of various steps in the envisioned process. The transferred data at this stage is usually very critical and most confidential since it entails potentially extremely valuable information including business and R&D secrets, innovations that are not yet patented, etc.

Wherever machines are used to source **raw materials** numerous sensors are used to either guide the exploitation or even to fully automate it. The latter is particularly widespread when raw materials are sourced from remote and/or extremely inhospitable areas, which is common for oil and gas fields. Data at this stage is transferred to monitor and remotely maintain the exploitation process and the machines involved. Notably, some third party software companies have emerged that provide specified analysis based on complex sensor arrays to maximise output of oil and gas exploitation undertakings.[329]

Since **intermediary products** are usually produced by Small- and Medium-sized Enterprises (SMEs) that are very specialised within a global value chain many such inputs have to be orchestrated, which requires the transfer of value chain management data that enables just in time or just in line production. Also, information e.g. about current market demand or forecasts have to be transferred back to subcontractors in order to enable their own production planning. The same is true for **intermediary services**.

During **assembly**, machines and in particular robots are linked together by data streams that enable production optimisation. At this stage, another trend becomes visible. Robots support human workers more and more on the factory floor usually to menial, repetitive, or physically challenging tasks. Their sensors produce individual data flows that enable both to monitor the robots themselves as well as production performance as a whole. These data may however also enable deduction of personal data about the human workers on the factory floor. Beyond robotics, modern machines are equipped with various sensors whose data is used to improve throughput, maintenance, and material consumption. Finally, data from market intelligence systems is used to adjust production to demand (forecasts).

Companies from the machinery sector are usually not (yet) concerned with further steps in the global value chain including **sales and marketing** as well as **post sales**' data flows. Whereas these latter stages of global value chains may include unstructured data gathered e.g. from social media, the data gathered by machinery companies during the R&D and production process is practically always structured and gathered purposefully. Consequently, data flows and data transfers are commonly planned prior to installing the specific machine and orchestrating it in the respective value chain. Commonly, even the third parties such as software providers who will be able to gain access to the data produced are predefined.

The table below provides examples of types of data that are typically moved along the value chain in order to ensure a functioning production. The value of specific data differs depending on the context quite significantly. Data from the R&D stage of the value chain is almost

[329] See e.g. Lasica, R. (2015): A New Age for Oil and Gas Exploration: Remote-Sensing Data and Analytics Are Changing the Industry. Earth Imaging Journal – 14th July 2015.

always highly valuable because it is likely to contain business secrets and information of products that are not yet on the market.

Process data originating from the sourcing of raw material, production of intermediary products and services as well as the actual assembly can be very valuable if it enabled third parties to infer business secrets or simply the current state of the company as a whole referring to e.g. the utilised capacity of individual production sites or demand for specific products.

Figure 34: List of Data that needs to be moved in production

Control/ coordination	Pre-production	Supply chain management	Production	Post-sales
- Employment data	-Market information	-Customs data	-Data from sensors	-Usage data
- Market data	- Usage data	-Customer data (incl. names and addresses)	-Instructions for robots, incl. communication between robots	-Performance data
- Market prices	- Social media data	-Package tracking	-Know-how/training	-Social media input
- Operations, planning, and processing	- Technical data	-Delivering input services	-Testing final product	-Customer reactions
- Production/ output data (from several facilities)	-Virtual design	-Payments (for products)	-Diagnostics, maintenance and repair	-Diagnostics, condition monitoring, maintenance and repair, incl. spare part management
- Production planning (incl. just-in time and adapting production)	-Test results	-Inventory levels	-Market data	-24 h service
- Monitoring performance	-Names of scientists	-Transport route optimization and transport time	-Product data	-Data from third parties (e.g., retailers)
-Demand forecasting	-Location data	-Procurement details	-Quality control	-Content as part of product
- Know-how/training	-Know-how	-Communications (e.g. e-mail)	-Technical data	-Storage management
- Licensing	-Customer data	-Info to logistics partners		-Data on parts availabilities
- Customer data	-Communications (e.g., e-mail)	-Orders, orders data		- "Life of product" (what version a customer has)
- Energy and material consumption	-Project information	-Sales data		-Technical data
-Internal communication (e.g., e-mail)		-Production schedules		-Product offer data
		-Performance metrics (quality data, lead times, queuing delays, service performance)		-Sales guides
All categories				
Storage				
Back-up				
Software installation and updates				
Troubleshooting and data repairs				
Documentation of work flow				

Source: Kommerskollegium (2015)[330]

It has to be noted that the processes and individual value chains, in which machinery is used and collects as well as transfers data, can be very complex. Furthermore, it has to be noted

[330] Kommerskollegium (2015) No Transfer, No Production – a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods. Stockholm: Kommerskollegium National Borad of Trade of Sweden.

that machinery producers are commonly only a part of a larger (data) value chain (e.g. involving Industrial Platforms). Consequently, the table below only provides examples of data that typical machinery companies may have access to depending on the specific contractual agreements with their clients, who use their components, machines, or assembly lines.

Table 23: Types of actors along the data value chain and their respective contributions to it

Type of actor	Contribution to the data value chain
Component manufacturers	Their components, which can be individual sensors or actuators just as well as powertrains or driving shafts, can generate data. Usually, these data are fed into the machine, in which they are employed. The manufacturer of the individual rarely gains access to the data across various machines, in which their components are used. In the future, such an access appears to be technically possible, but given the knowledge that could be inferred from such process data, it is unlikely that these data will be widely transferred back to components manufacturers.
Manufacturers of machinery (machines)	Machines are commonly equipped with various sensors and actuators that enables precise control, monitoring, and optimisation of production lines. Since remote maintenance is a principle that has been established in machinery for quite a while, it is also common that manufacturers of machinery can access their machines remotely and gain access to (relevant) data.
Development of production lines	Developers of production lines need access to specifications and capabilities (including data collection) of individual machinery to be deployed. If they also offer to run and maintain production lines as a service, they will also be able to gain access to data that is relevant for the task.

Source: Deloitte

Actors, challenges, and technical solutions in the market

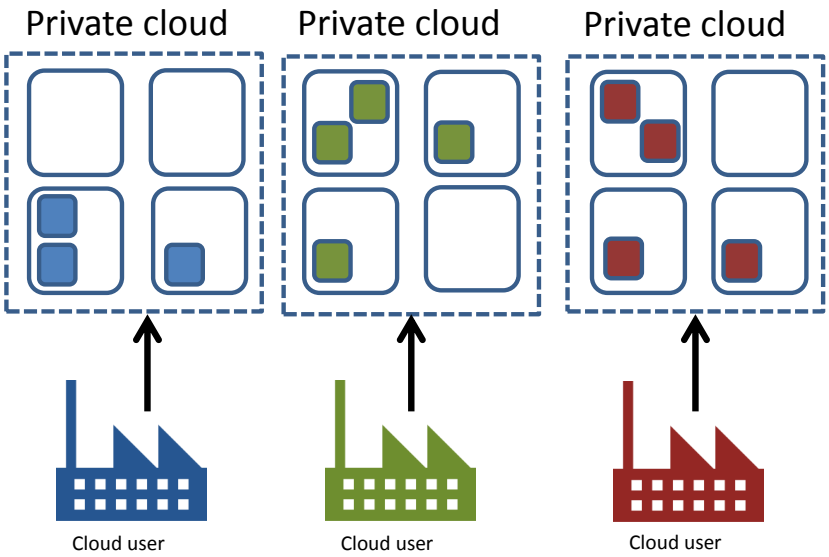
In general, there are private clouds and public clouds on offer. Private clouds[331] are secluded environments where different SaaS, Iaas, or PaaS services are only used by one company. Here, service level agreements for the safety of data, security measures (rights and roles management), and services provided are dedicated to the specific customer. A private cloud provider will offer secluded services to different business customers but the hard- and software used as well as the data centres hosting the cloud service are not necessarily used exclusively by only one customer. This leads to competitive and professional IT services even for smaller companies without extensive Investments in infrastructure and personnel.

General advantages of private cloud services include

[331] See NIST (2011): "The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises." p. 3.

- fully scalable IT resources, even available at short notice help to avoid expensive investments/lock-in effects and to ensure long-term profitability in a fast changing digital environment
- cloud-based workflow and file sharing for extended collaboration: access to data anytime and from anywhere allows flexible working environments within the company with subcontractors and customers
- integrated security and robust disaster recovery increases safety of the whole company
- automatic software updates enhance state-of the art business development for all sizes of companies, esp. SMEs
- subscription based tariffs for usage (pay as you go) to reduce IT costs

Figure 35: Private cloud – stylized example



Source: Deloitte

To a public cloud similar advantages apply concerning collaboration and data exchange options. However, a public cloud serves different purposes: Customers, i.e. industrial service suppliers, component suppliers, subcontractors of all kinds or after sales service suppliers connect to the cloud to store or process their own data and share the information at the same time. This data contribution can be used to be analysed and provided to the whole cloud community or even the sector or other third parties (e.g. for scientific or regulatory purposes). The main aim of a community cloud is to facilitate collaboration within a sector and to enable synergy effects.

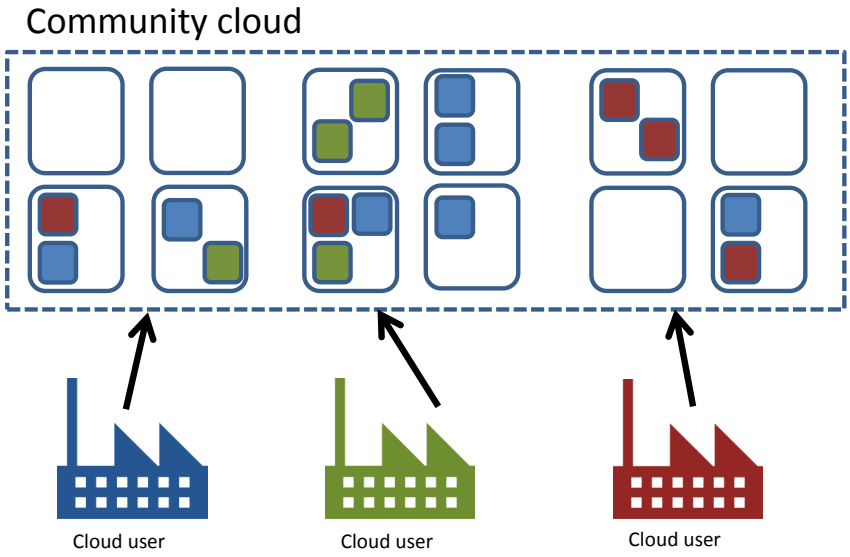
Most of the cloud applications in industry relate to the efficient management of processes. Cloud service providers offer platforms to which all stakeholders can upload data to monitor the status of production quality compared to the sector.

In a public cloud, the cloud infrastructure is provisioned for open use e.g. by the general public or, for exclusive use by a specific community, i.e. sector related businesses: “It may be owned, managed, and operated by a business, academic, or government organization, or

some combination of them. It exists on the premises of the cloud provider."[332] The question where the data centres of the cloud are situated determines which national rules apply. For example, if the data centres are in Europe, European data protection law adapted by the specific member state applies.

Hybrid cloud solutions where the infrastructure is a composition of private and public cloud service offers are also possible. As we will see in our use case example, Mindsphere based on the SAP HANA open cloud solution may serve as a private or public cloud for a customer (hybrid cloud offer) and is meant to be an industry community cloud used by different stakeholders.

Figure 36: Community cloud – stylized example



Source: Deloitte

Types of data generated and used by different actors

Looking at the types of data potentially provided by and exchanged between businesses, several main types of actors can be distinguished. The business users can provide different types of data, which then can be analysed (see the table below).

Table 24: Types of actors along the data value chain and their respective contributions to it

Type of actor	Contribution to the data value chain
Original Equipment Manufacturers (OEMs)	The OEM is the manufacturer of the original equipment (industrial machine), i.e. the company that assembles and installs parts supplied by subcontractors. The OEM sells the finished product and customizes designs based on demand. The company closely works with their subcontractors and uses their data for optimization and for defining service level agreements.
Third-party	Third parties (i.e. subcontractors of OEMs) provide data about their pro-

[332] See NIST (2011), p. 4.

Type of actor	Contribution to the data value chain
suppliers of products, components, modules	cesses and about their products, which then can be used by the OEM to steer their processes.
Machine owners ("end-users")	Machine owners generate data through their production activities on their premises. The data is generated by machine parts, as well as additional sensors deployed in the factory.
Third-party providers of data analysis and IT Infrastructure provision	IT firms (or cloud service providers) offer solutions by means of which OEMs, subcontractors (products, components, and modules suppliers) as well as after sales service suppliers can collect and analyse the data and process it through algorithms. These algorithms create the benefit of the data for the all stakeholders in the value network who are then able to use the information for process optimization and product enhancement.
After sales service suppliers	In addition to production data, data is generated by machines on their operation incl. e.g. maintenance and repair needs. This data is relevant for both the machine owner activities, as well as for the manufacturers themselves that want to improve the performance of their machines.

Source: Deloitte

These different types of actors in the value network, as well as their respective data and information supply are closely connected and each provides added value in relation to the optimization of the production process and of the actual use of the industrial machines.

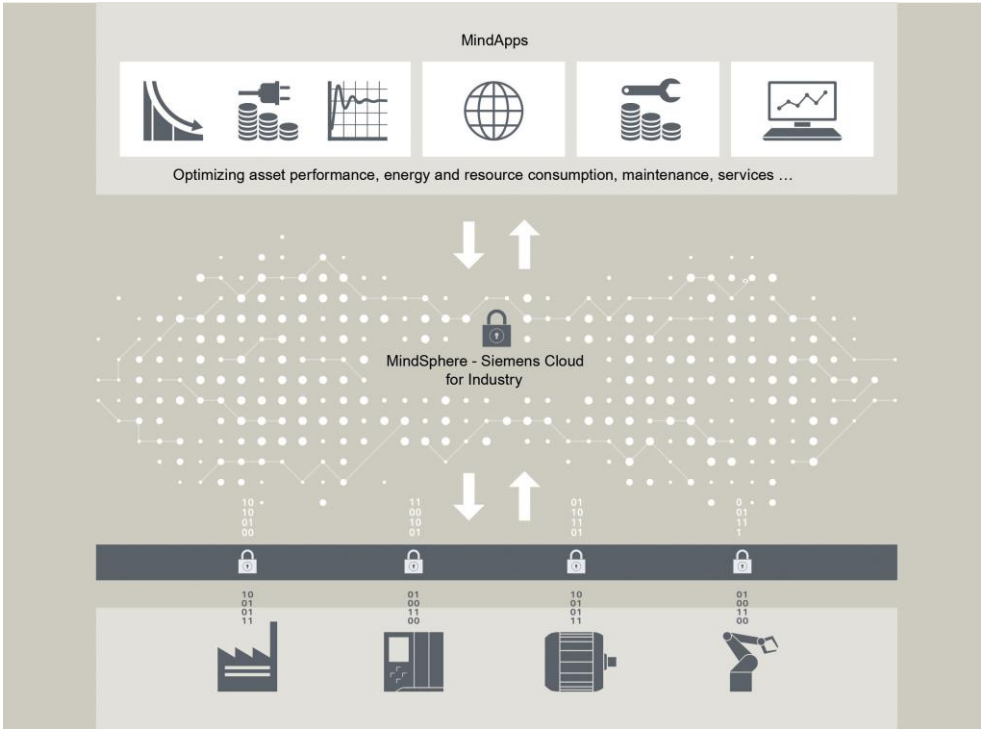
Business model and actors: Mindsphere by Siemens, a typical service offering of industrial platforms

For this study, we selected Mindsphere, a solution by Siemens333, as a use case. It was first presented at the Hannover Fair 2016. Siemens launched it after a pilot phase and the solution is now available (see figure below). In short, Mindsphere offers industrial enterprises an open infrastructure based on SAP HANA cloud solution and allows the creation of new digital services "on the path to Industry 4.0". [334]

[333] Siemens AG (Berlin and Munich) is a global technology manufacturer active in more than 200 countries with 348,000 employees, focusing on the areas of electrification, automation and digitalization. In fiscal year 2015, the company-generated revenue of €75.6 billion and net income of €7.4 billion, see http://www.siemens.com/press/en/materials.php. Information for this case is based on expert interviews, official documentation of Mindsphere and Siemens website information.

[334] "MindSphere - Siemens Cloud for Industry. An essential element on the path to the digital enterprise", product information, 2016

Figure 37: MindSphere – Siemens Cloud for Industry



Source: Siemens.

The "Digital Enterprise Software Suite" with its core feature "MindSphere – Siemens Cloud for Industry" supports the optimization processes within a company. The community cloud solution bundles several services for manufacturing companies who aim at cutting throughput times, increase flexibility, and enable individual mass production, as well as optimizing their energy consumption and, finally, deployment planning.

The platform will support the companies' entire value chain from design, production planning and engineering to services and includes the following services:

- Connectivity to Siemens and third party products via Open standard (OPC).
- Access to existing Siemens products (configuration in the TIA Portal).[335]
- General Cloud service by an optional cloud infrastructure – public or private cloud or location-specific solution.
- Community cloud service by MindSphere - Siemens Cloud for Industry with open application interfaces for individual customer applications.
- SaaS, Paas, IaaS cloud solutions provide opportunities for new business models for Siemens customers (e.g. offering machine-hours for sale).
- Cloud-typical pay-per-use pricing model (without the need to track usage in detail).

Siemens' services include data recording, transmission and safe storage, as well as a cloud environment for the development of new applications.

[335] Totally Integrated Automation Portal (TIA Portal) with access to Siemens digitalized automation services, https://www.industry.siemens.com/topics/global/en/tia-portal/Pages/default.aspx

Potential services benefits based on Mindsphere include preventive maintenance, energy data management or remote monitoring of machine fleets for service purposes. Considerations about using data to offer statistics and other information to third parties are not relevant in the business model.

Interoperability is ensured by a connector box, which has been developed during the pilot phase called "MindConnect Nano". The device allows the connection of machines and plants to Mindsphere irrespective of the manufacturer. It is a pre-configured Industrial PC based on free open source software. Transmission of data to the cloud is encrypted.

Use restrictions of the MindConnect Nano[336] device ensure that the purchaser/business user bears the full liability concerning for example the following issues:

- The device shall not be tampered with for sending data to any other application, platform, database or any other target storage or analytics solution. No additional software shall be installed.
- The software shall not be copied, disassembled, decompiled, reverse-engineered or modified in any way or made available to third parties.
- The purchaser has to make sure that he does not infringe the intellectual property rights of any entity or person.
- The purchaser shall not make any use that violates any applicable local, state, national, international or foreign law or regulation.
- Updates and security patches are provided by Siemens but it remains the purchasers' responsibility to implement them.
- The purchaser is responsible for providing sufficient internet connectivity.
- Siemens will not assume any obligations or liabilities towards third parties (e.g. end customer) that use the device.

Service example industrial platforms: Gehring, provider of honing machines and services

Gehring[337] is a globally operating machine tool company in the area of honing technology. To minimize maintenance and repair expenses by performing regular inspections and resulting coordinated maintenance activities Gehring implemented a Mindsphere solution that allows transmitting real-time data from their customers honing machines. The aim is to evaluate data in time so that Gehring can offer support by evaluating the current condition in order to recognize potential need for inspections and cases of damages as early as possible and find a suitable solution even before the customer has detected the need for it. This leads to in-

[336] For the following details see Data sheet MindConnect Nano https://cache.industry.siemens.com/dl/files/514/109485514/att_887965/v1/MindConnect_Nano__Datasheet__Specific_Terms_V1.1_en.pdf

[337] http://www.gehring.de/en-us/company-profile. Gehring is a globally active German based limited liability company specialised in honing. Clients include the automotive, mechanical engineering and other industries. The company has 800 employees.

creased machine availability for production and to more transparency in the whole production chain.[338]

Gehring also gains more data about productivity, resources efficiency during the production process and the overall state of the honing machine tools. The company uses Siemens Mindsphere as a data-hosting platform to realise an improved version of its services including:

- inspection and/or maintenance on your machines according to the Gehring checklist
- Repair, in the case of faults
- Use of qualified Gehring personnel
- Exact report of current condition
- Recommendations for improvement[339]

Business model and actors: A typical service offering of Würth and the machinery firm TRUMPF/AXXOOM

Currently, most manufacturers of machinery still stick to business models and service offerings that have been around for many years now. They typically deliver the components or machinery that is equipped with the sensors that the client requires for its value chain and leave the rest to the client apart from remote maintenance of their machinery. Data are commonly transferred within the value chain.

However, some notable examples of third party involvement within value chains exist. Two examples are described here. The first example is Würth's iBin@WP (intelligent bin at workplace). It is a container for consumables such as screws or collar nuts that is fitted with a camera system scanning the fill of the container continuously and initiating automatic orders for refills. Such containers can play an important role in automatic replenishment regardless of the location and can become an essential factor for flexibility, efficient processes, and maximum supply security in the manufacturing industry.

The second example refers to a much broader service established by the German machinery firm TRUMPF in 2015. It is their subsidiary AXOOM. The company offers a browser-based platform to manage the whole production process. It is also open to third party developers to offer apps for AXOOM's clients. AXOOM profits from the in-depth knowledge and data of TRUMPF as well as other partners. It is one of the first platforms of its kind. According to expert opinions gathered for this case study, such business models and services are likely to become more numerous in the near future.

Notably, data even in such business models is neither generated nor gathered accidentally. Also, data transfer is usually handled in individual contracts and rooted in established business relationships that rely on mutual trust of all parties involved. Otherwise, data are commonly kept as close as possible to the original organiser of the value chain, because they could be used to infer trade secrets, which is particularly harmful in the context of machin-

[338] See Gehring PM 2016/02 (only in German) http://www.gehring.de/sites/default/files/text/gehring_industrie_4.0-de-ww.pdf

[339] http://www.gehring.de/en-us/inspection-and-maintenance

ery manufacturers, who usually only have between 12 and 18 months until the competition is able to reverse engineer their innovations and copy them. Any data leaks may reduce this time lag even further until investment in innovation becomes eventually meaningless.

Service example industrial platforms: Professional Coffee Machines

Another interesting example on how connectivity of independent machines via platforms can lead to new service models forms the case of professional coffee machines used in coffee bars.[340]

Coffee machines are highly automated but till now, information about usage and maintenance was only available on the premises of the coffee bars. Data can be accessed via the local user interface. Neither the manufacturer nor the maintenance service, the owner of the coffee shop (or the franchise) or the coffee roaster is in possession of the full information. The maintenance service is called in case of problems, and performs its maintenance duties accordingly.

In an innovative IoT environment, coffee machines are able to collect information and send these information to a cloud application platform, usually set up by the manufacturer. The manufacturer who before was only informed about the location of the machines and their performance is now in a new, more central position in the value chain that allows him to collect and use data creatively in many ways. Then, data flows in both directions: Status and usage information go to the platform (a SaaS cloud service the manufacturer has established, usually with the help of specialised cloud providers) and recipes, set-up parameters, or instructions can be sent remotely to the machine, i.e. the coffee shop provider. Today, leading companies in these markets are running various pilot projects.

In this new scenarios, manufacturers will benefit from data that gives information on

- the correct use of the machine (maintenance periods, coffee beans used, cleaning processes etc.) which might affect liability or guarantee issues)
- information that might affect the design (valuable information to be used in research and development)
- interesting data that can be provided to third parties

Dealers of coffee machines who are often offering maintenance as well are also interested in the data to provide better service to their customers. By using the collect data or even have access to (near) real-time data they can

- note faults and disruptions (even before the coffee bar owner)
- make remote diagnoses (and thus reduce repair time: they can plan repairs ahead by predicting them, bringing the right spare parts to the site etc.)
- reduce time for routine check visits

Coffee roasters might also be interested in the data to avoid fraud (baristas attempting to use other coffee brands in order to reduce costs) and to ensure the coffee shops provide the

[340] The example was explained in detail at a workshop held during the course of this study: Internet of Things and Data Exchange: The Case of Professional Coffee Machines, Massimo Vanetti, SBS IoT Expert (The Transformative Effect of Access and Re-use of Data for Smart Industries, Bruxelles, June 6th, 2017).

right consumption of coffee flavour to the users (e.g. through control of the recipes and remote process conditions set-up directly), and finally, to collect general statistics about the type of servings and business performances by location. Franchises might have a similar interest in the data, as they are bulk buyers and own large fleets of machines. They probably would like to compare performance in-between manufacturers.

Finally, coffee shops are interested in better maintenance (reduced and less costly time to repair) and reduced outage, therefore they will benefit from overall statistics generated by all participants in the cloud service.

Looking at the boundaries and mitigation actions, the main questions from the view of all stakeholders is who “owns” the data. Most experts think that data belongs to the originator, i.e. coffee shops, but some also share the view that the data “owner” is the owner of the equipment, i.e. the coffee roaster, or the franchise.

However, in the process now examined and put on trial by the manufacturers, the data access is tied to the machine, it is a part of the machine itself. The manufacturers have established a swift and effective way to put up the industrial platform and store and process all the data.

In the end, the manufacturer might be able to fulfil a gatekeeper role in this environment and regulate the (re-) use of data. He can host all data for its own analysis and can decide which stakeholders to give access to (maintenance, roasters/franchises, and coffee shops).

Then, all stakeholders have to enter into a specific data distribution contract with the provider of the platform (in this case the manufacturer). In a scenario where maintenance, roasters/franchises and coffee shops are more or less dependent on few large coffee machine manufacturers who have more bargaining power due to their more value-added performance in the value chain, the actual process of finding a satisfactory contract or terms and conditions for all sides without any further liability restrictions or contractual limits to use and re-use of data might get near to impossible.

The nexus between data ownership, access to and use of data, and the interoperability of services in Industry 4.0 in general

Given the fact that practically all data are gathered purposefully and systematically, individual contracts can cover data ownership, access to and use of data among firms along the value chain or with third parties that offer services to plan, manage, or optimise the value chain. Commonly, all involved parties arrange data exchange, ownership, and re-use in individual contracts. Intensive planning usually ensures interoperability of data formats and services.

In praxis, the data goes to the manufacturer (who is in fact also the provider of the industrial platform cloud service) and so he gets involved because data access is tied to the digital control, which is internal to the machine: a part of the machine itself.

According to experts, this happens all the time in almost every type of industry (e.g. see the example of coffee shops, of Siemens and of car repair maintenance (see chapter on automotive sector). However, access and re-use of data is still subject to individual contracts.

As Industry 4.0 becomes more prevalent in all kinds of sectors, the number of such contracts may increase beyond what a typical SME manufacturer of machinery or mere buyer/owner of a machine is able to manage. Consequently, it seems likely that a sort of code of practice might emerge striking a balance between opening interesting data within the value chain and possibly even to third parties and protecting valuable know-how.

In light of the current character of the factory floors, experts from the sector do not see the need for a Robot Law or something similar, because robots and machines are commonly used within continuously monitored and controlled environments. Any autonomous decision that they can take is commonly predefined and accounted for in the production line. Thus, the environment and gravity of autonomous (mis-)behaviour is less severe than for autonomous cars or robots that support carers in homes for the elderly.

Data localisation and the specific rules that apply especially to personal data or data from which personal data can be inferred can be an issue in global value chains. It may also curb some service business models for machinery manufacturers, who intend to offer services solutions across values chains and countries. However, it should be highlighted that data localisation was not mentioned by industry experts with regards to EU Member States.

Potential contractual barriers

This section provides a first analysis of potential contractual barriers, companies who use an industrial platform like Mindsphere may face. We also conducted interviews with stakeholders from the electronic industry, from insurances and from skilled crafts and small businesses associations to get a more complete picture of potential barriers.

As we have described before, Siemens is offering Mindsphere services only for a short time and is still collecting further information for improvements provided by their reference customers. It is therefore too early to give a definitive assessment of whether the present success will be sustainable and which potential contractual and non-contractual barriers occur in future.

The section first discusses contractual barriers related to data ownership, access to, and (re-) use of data. Second, potential risk and liability issues are described. In the end, the section gives a high-level assessment of the potential impact of potential barriers.

Data ownership, access to, and (re-) use of data

Data ownership and access to data

In Industry 4.0 or IoT contexts, manufacturers often seem to want to control data not only within the boundaries of their machines but also beyond, i.e. via a platform. Customers fear that in the end they have to

- pay extra for the access to data (even their own machine´s data)
- pay for software, that establishes APIs to the platform

- give up control over their machines

However, there are general rules and practices for using clouds today and these regulations apply at least to the industrial platforms which are operational and were reviewed for this study.

In a cloud environment today, the files stored in a cloud are owned by the person who created the file. This does not mean that the content of the file (text, data, etc.) is protected by copyright but the file itself belongs to the person or company who set it up. This is practiced in everyday business and is also used by private cloud users on a daily basis (e.g. access to photo albums).

Cloud computing can be described as IT "renting". The temporary provision of (virtual) hardware as PaaS resource or as storage-as-a-service, can also be defined as a rent.

The data stored in a cloud also remains the property of the customer when the use of a cloud is part of IT outsourcing strategies. This must be taken into account when drafting an outsourcing contract. In the case of contract data processing, the responsibility for data protection of personal data is with the customer and the latter controls the contractor (cloud provider). The user must therefore have control rights to the cloud provider.

To sum up, access to data can be given on a contractual basis to anyone by the "data generator". In the interviews and the workshops held during the course of the study several stakeholders highlighted how "machine data" can also be seen as "raw data" which does not belong to anyone and should be treated like a resource. Apparently, this leads to a proactive storage of machine data by OEMs and cloud service providers (especially PaaS providers) today order to keep all options of re-use open for the future. Small and medium enterprises (suppliers of parts etc.) do not share this view and see their trade secrets and confidential information infringed. On the other hand, many of them claim to have the right to access and use "machine data" as well.

(Re-) use of data

In a community cloud, (re-) use of data is based on terms & conditions as well as individual contracts. The SAP HANA cloud solution[341] includes a graded series of (re-) use of data depending on the areas the customer is using. The private area can be secluded from other customers but if a customer uploads data in the public area this data may be used in the terms defined beforehand. The customer bears the risk which area to use. This also includes the risk of violating other third-party intellectual property rights.

The contractual agreements for outsourcing between cloud providers and business customers contain some potential for conflict, since in the description of the quality of the service provider interests on the one hand (standardization and resource utilization in his data centre) may oppose the clients' interests according to company-adjusted solutions on the other

[341] The technological basis of Mindsphere. For terms and conditions for SAP HANA see https://help.hana.ondemand.com/terms_of_use.html and http://go.sap.com/about/agreements/general-terms-and-conditions.html.

hand. In particular, data security, confidentiality and data protection are the most important requirements for the customer (in this case the cloud platform user), which contradict the exploitation of synergy effects in the data centre and cost-reducing solutions for the cloud service provider.

Risk and liability

Cloud providers are companies that, like everyone else, conclude private contracts with the users. They conclude service contracts with customers or outsourcing contracts. SLAs and terms & conditions supplement these contracts. Rather, everyone is "free" to offer such a service and limit risks and liability accordingly.

Industry associations[342] have issued guidelines on the legal implications and the drafting of contracts for the use of the cloud as well as data (re-) use in order to simplify the contractual negotiations for companies with cloud providers and to support medium-sized cloud providers with awareness raising information about differences in security, data protection and quality features from European vendors compared to the market dominant US vendors.

Potential non-contractual barriers

Technical barriers

Accessibility of data might be limited when it comes to cross-brand services. Data access will be provided to other interested parties through the cloud provider who is presumably closely linked contractually to the manufacturer. However, a data user will likely buy machines from more than one manufacturer, or services from more than one maintainer and thus might want to analyse data obtained to compare performance (productivity, quality etc.) of different machine categories. If each manufacturer has its own data silo, the potential data users face the technical problem of having to integrate many data sources.

Interoperability is one of the most important enablers for a well-functioning industry platform based on cloud services. In the B2B context, the platform provider can ensure access to and re-use of data through the use of an **interoperable** solution – an API which enables their business customers to transfer the data they process and download to their own IT environment.

As shown in other use cases in this study, i.e. agriculture, market mechanisms drive the take-up of interoperable solutions. Only the use of open APIs increases the number of potential

[342] Siehe BITKOM (eds.) (2008): Rechtliche Aspekte von Outsourcing in der Praxis. Leitfaden, Berlin

BITKOM (eds.) (2009): Cloud Computing – Evolution in der Technik, Revolution im Business, BITKOM-Leitfaden, Oktober 2009

BITKOM (eds.) (2010): Cloud Computing – Was Entscheider wissen müssen. Ein ganzheitlicher Blick über die Technik hinaus. Positionierung, Vertragsrecht, Datenschutz, Informationssicherheit, Compliance. Leitfaden, Berlin, Eurocloud Deutschland_eco e.V. (Hg.) (2010): Cloud Computing. Recht, Datenschutz und Compliance. Leitfaden, Köln.

customers from the sector and thus enhances the value of the community cloud for each participant.

However, full data portability might not be guaranteed, i.e. the industrial platform customer might not be able to move its data and services from one cloud solutions to another competitor without friction or to use different data from different cloud service providers/manufacturers. This is why lock-in effects cannot be ruled out.

Other barriers

Other technical barriers relate to the technical resources, the qualifications and the knowledge an SME in a certain industry sector might need to connect to a cloud solution. In the interviews, it was highlighted that advantages of transparency and sharing of data are not only perceived as a benefit but also as a risk to reveal confidential information about business secrets, which are otherwise disclosed from competitors. If medium-sized companies like component suppliers, maintenance and repair companies, or other subcontractors of large OEMs are ready to overcome these concerns remains to be seen. It would seem reasonable that, to foster trust in sector collaboration, the technical solutions imposed in industry clouds should take into account high-standard technical security measures.

Access and (re-) use of data: Boundaries and mitigation actions

Just like data ownership, (re-) use of data is commonly managed through individual contracts. Experts commonly agreed that these individual contracts are sufficient to manage the control of access and (re-) use of data as well as defining liability risks and corresponding remedies for the parties involved. Stakeholders agree that an overarching ruling by legislators or regulators is not opportune at this moment, since business models still have to evolve and should not be limited in their innovativeness. Ex-post analysis of specific cases where problems emerged should however be planned for.

The French and German Electro-technical and Electronics Industries as organized in FIEEC and ZVEI[343] are especially involved in discussing issues concerning their member companies which are more and more involved in Industrie 4.0, use of IoT as their members are becoming a part of broader industry platforms. In their recent statement on a "business-friendly regulatory environment, fostering the development of the digital economy and Industrie du futur / Industrie 4.0 solutions, enabling companies and new businesses"[344] they rise concerns as regards the improvement of the Internal Market especially through an integrated Digital Single Market taking fully into account the competitiveness of our industries at global

[343] FIEEC and ZVEI, both members of ORGALIME their European association, are one of the major technological sectors in Europe representing 4 600 companies, 1,249 million employees and a turnover of 278,5 billion euros. All organizations were active in the process of discussing the objectives of a European data economy during the workshops conducted during this study.

[344] Joint Declaration 6th July 2016, https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Pressebereich/2016-048_Digitalisierung_der_Industrie_Deutsche_und_franzoesische_Elektroindustrie_stellen_gemeinsame_digitale_Agenda_vor/Pr_2016-048_FIEEC-ZVEI-Joint-Declaration-July-2016.pdf

level; but at the same time stress the need for the reinforcement of digital security and trust and a framework combining the protection of personal data and industrial data, taking into account innovation capacities.[345]

If a manufacturer can, technically, access all data they might be able to get full picture of the business of their customers, and even guess their future strategies. Industrial platform providers are aware of this problem and attempt to handle this, e.g. by dividing the data sets in segments and "anonymize" sensitive pieces of information. The association summarizes the main concerns as regards security, sensitive data, and technical reliability, small and medium-sized enterprises have in the context of using platforms and getting closer cross-linked to suppliers, customers and also, competitors.

The result of the research and discussions with experts show, that these topics are not easily solved and that data collaboration, data innovations and customer demands create an area of conflict in future. Today, there is no consensus or blueprint as how to master these general challenges. The experts generally agree that the market is still at an early stage and regulatory activities would rather harm than benefit users of Industry 4.0 opportunities and industrial platforms.

[345]Cloud service providers like Deutsche Telekom have taken these concerns into account and have created technical and contractual solutions for secure storage and processing, see https://cloud.telekom.de/fileadmin/CMS/Shop/Cloud_Infrastruktur/Microsoft_Azure/Whitepaper_Datentreuhaenderschaft.pdf

Transport & automotive sector

Context: The initial situation within the market

The worldwide trend towards urbanisation[346] creates numerous challenges for public infrastructure and service provision. Among them, managing transport and traffic is one of the most pressing ones. Only a mix of all modes of transport such as non-motorised and motorised private transport, shared non-motorised and motorised private transport, and public transport will be able to solve this challenge.[347] Intelligent Transport Systems (ITS) featuring various data exchange points are essential for a successful adoption of intermodal transport.

The idea of ITS can be traced back to the 1950s and 1960s. In the U.S., visions of self-driving cars, externally controlled traffic, and electronic route guidance were particularly widespread. While a comprehensive plan for an "Intelligent Vehicle-Highway-System" emerged from a broad coalition of private, public and academic institutions, the term ITS was only coined in 1994.[348] Today, ITS comprise the application of information and communication technology (ICT) to solve transport and traffic challenges. Naturally, this touches upon a wide range of different trends including smart cities, smart / connected cars, machine-to-machine (M2M) and Internet of Things (IoT).

The following figure introduces the main applications of ITS. Notably, only some of these are already widely deployed.

[346] According to the United Nations, in 2014, in 63% of 233 observed countries and areas, more than half of the population was living urban environments. In more than one third of observed countries and areas, more than 75% of the population live in urban environments. The UN forecast further strong increases in urbanization worldwide until 2050. Source: United Nations (2015): World Urbanization Prospects – 2014 Revision. New York: United Nations.

[347] E.g. European Commission (2013): Mobilising Intelligent Transport Systems for EU cities. Commission Staff Working Document. SWD(2013) 527 final. This is also reflected in the EU's Horizon2020 work programme 2016-2017 on "Smart, green and integrated transport"- European Commission Decision C(2016)4614 of 25 July 2016.

[348] GSMA (2015): Mobilizing Intelligent Transportation Systems (ITS). GSMA Connected Living Programme.

Figure 38: Main applications of ITS

Source: Transport Canada (2014)

For almost all these applications some degree of data exchange is necessary, either between vehicles, between vehicles and infrastructure, or between vehicles and backend interfaces.

By interconnecting different modes of transport, an integrated concept regarding different possibilities of mobility as well as mobility management can be established. This enables an optimal real time routing for passenger and freight transportation processes. Moreover, an integrated network system can facilitate an efficient and improved use of infrastructure as well as analyse and predict traffic bottlenecks. From an economic perspective, the efficiency of the transportation system can be significantly improved, the transportation safety can be enhanced and traffic related emissions can be reduced substantially.

By design, the integrated network system is supposed to be created in a way so that omni-present and ubiquitous access is possible. Every gap in the information system that prevents the flow of data and information and might have destabilizing effects on the functionality of the network. To demonstrate the complexity of ITS, the table below describes a selection of typical actors.

Table 25: Types of actors along the data value chain and their respective contributions to ITS.

Type of actor	Contribution to the data value chain
Driver / Vehicle	Modern vehicles generate a lot of (sensor) data. Most of them are used only internally for applications like engine management, driver information, etc. If the vehicle features connectivity some of these data can also be transmitted. Commonly, this is realised via 2G and 3G cellular radio. Very few cars feature 4G connectivity. Since, in the vast majority

Type of actor	Contribution to the data value chain
	of cases, only geo-located data are transmitted, 3G and even 2G types of connectivity suffice.
OEM	Collect data from and offer services to drivers, but also from other own and third party sources such as repair shops, market research, or weather forecast services.
(component) suppliers[349]	Depending on the nature of the component, these actors can also collect data themselves or receive data from OEMs or other third party suppliers such as smartphone manufacturers, weather forecast services, market research, sensors installed on roads, or in other traffic infrastructure.
Third party data providers (private)	Provision of software solutions to OEMs and (component) suppliers that enables them to create valuable and actionable information e.g. based on smart algorithms for their respective clients and customers. It should be noted that both OEMs and (component) suppliers analyse collected data predominantly in-house (potentially using advanced software solutions from third parties).
Third party data providers (public)	They collect and hold data from public transport, sensors installed on roads and other infrastructure as well as about current roadworks. While in some cases data are provided to market actors, in many others data are not published or provided to market actors.

Source: Deloitte

These different types of actors along the ITS data value chain as well as their respective data contributions are closely connected – one building on each other with a view to increase the efficiency of routing traffic.

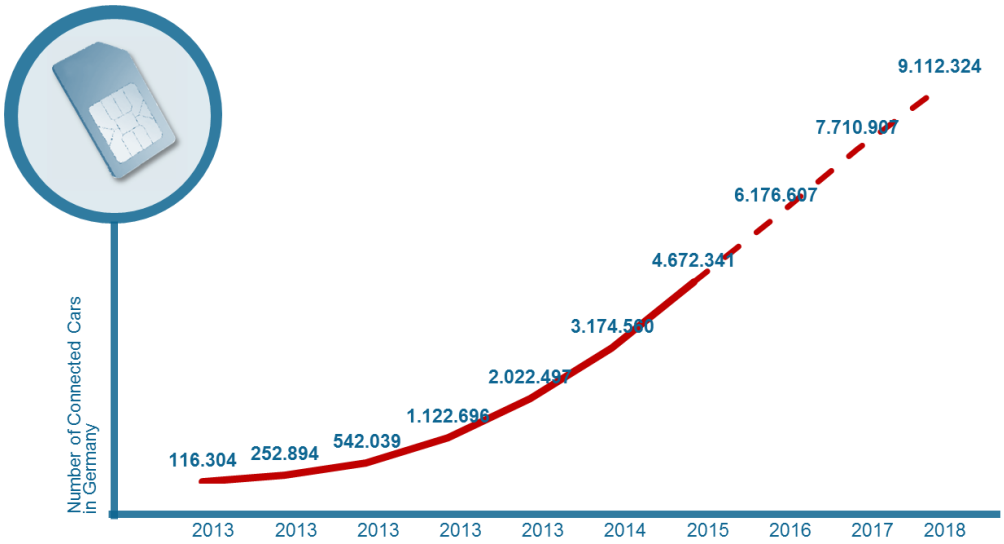
Beyond ITS, which is the focus of this case study, the concept of "connected cars" attracts interest from various actors. With its numerous sensors[350] on board and the capability of receiving and transmitting data predominantly via mobile networks (2G/3G), the car turns into a source of potentially valuable data. This is particularly relevant as the number of connected cars is growing rapidly. The figure below shows the number of connected cars in Germany. It includes both cars with built-in SIM-Cards as well as cars that feature a brought-in solution i.e. a SIM-Card slot fitted in dashboard or connectivity enabled by tethering via a smartphone.[351] According to experts from the automotive and telecommunications industry, this trend is representative for most Western countries.

[349] This includes telecommunication providers, who are mostly instrumental in providing connectivity via their cellular radio networks. However, some of them have also entered the market for automotive components e.g. anti-theft solutions, trace and track application for fleets, or data platforms for other suppliers / OEMs.

[350] On average, there are 80 to 100 sensors in each new car. For premium and luxury cars, this figure can rise to 200 and more.

[351] The figure does not include in-car systems that support solely mirroring of contents and applications that run on an external device like a smartphone or tablet with or without mobile network connectivity.

Figure 39: Development of the number of connected cars in Germany



Source: WIK Connected Car Monitor Germany (2016)

The following figure provides an overview of data typically produced in a connected car as well as their data protection relevance.

For some of these data the purpose and rules of (re-) use are clearly laid out in legislation (row A). Other data are solely produced within the car's internal system to e.g. trigger a specific function or to display some information for the driver. They tend to be transient and are typically only stored as a snapshot e.g. to document a malfunction to ultimately assist in servicing the car (rows D, E, F). Types of data are shown in rows B and C. They refer to modern data services and data introduced to the car's system by the customers themselves. Even within these two categories only immediately personal data such as movement profiles, real-time locating, or the address book and personalised access to third party services (esp. stored passwords) have a high data protection relevance.[352]

The Personal Data Protection legislation[353] defines clearly what is allowed with personal data. However, in the case of connected cars, it is sometimes not quite clear which data are actually personal data. In Germany, VDA[354] and data protection bodies of the federal states have arrived at a common understanding. For them, personal data is any data that can be linked to the vehicle's ID or the number plate. The same memorandum defines that responsibility for data protection relies with the first party that receives any data that are collected online i.e. transferred from the vehicle. Usually, this is the OEM. In some cases, it may also be third parties. This implies that the first receiving party is also liable for any data loss or

[352] VSA (2014): Data Protection Principles for connected Vehicles.

[353] See overview of data protection legislation in the EU, http://ec.europa.eu/justice/data-protection/law/index_en.htm

[354] Germany's car manufacturers industry association

privacy breach. If data are to be transferred, used, etc. by a third party, the first party must ensure that data are used in accordance with the data protection directive. Data ownership is not addressed and appears to be an open issue for personal data collected from connected cars.

Figure 40: Types of Data Produced in Connected Cars and Data Protection Relevance

Data Categories	No Data Protection Relevance	Low Data Protection Relevance	Medium Data Protection Relevance	High Data Protection Relevance
A. The purpose limitation is regulated by law		OBD-II	e-call (EU)	event data recorder (USA)
B. Modern data services	anonymised services car to x	pseudonymised services car to x	Predictive diagnosis, remote display (e.g. electric vehicles)	Movement profile; remote locating
C. Customer's data / data introduced by the customer		Infotainment settings and convenience settings, e.g.: Seat setting, sound volume	Navigation destinations	Address book/ Telephone personalized access to third-party services
D. Vehicle operating values generated in the vehicle and displayed to the driver	e.g. fill levels, consumption			
E. Aggregated vehicle data generated in the vehicle	e.g. fault memory number of malfunctions, average fuel consumption, average speed			
F. Technical data generated in the vehicle	e.g. Sensor data, actuator data, the engine's injection behaviour, the shifting behaviour of the automatic transmission			

Framework conditions should allow customer-oriented and practical solutions

- As far as possible the data collected in the vehicle should be and should remain **"technical data"**
- With some of these data the data controller may have an overriding legitimate interest in terms of **vehicle and product safety**
- A combination of data can lead to data protection relevance.

Source: VDA (2014)

Business model and actors: A typical service offering

Although there are some notable best practice examples for intermodal data exchange e.g. intermodal transport control system for public transport (Cologne, DE), RBL, Light, Intermodal Transport Control System (Stuttgart, DE), Grand Lyon Urban Traffic Management System (Lyon, FR)[355], solutions for data exchange within one mode of transport dominate. In fact, even the best practice cases cited above refer predominantly to public transport and exchange little if any information with actors in (non-)motorised shared or private transport.

In sum, typical service offerings also focus on one mode of transport or a category of transport modes. Furthermore, as the best practices examples in the above underscore, deployed solutions are commonly confined regionally or even locally. As deployed solutions by and large focus on public transport, a regional or local focus often implies that only one transport carrier is concerned i.e. one would expect no or little flow of data between two or more actors.

Another typical and potentially more relevant service offering in the context of ITS revolves around geo-located data. Such data are commonly created and (potentially) collected via navigation devices. These devices can be in-car satellite navigation systems, brought-in navigation devices, or smartphones / tablets with navigation applications installed. This is most relevant in the context of data access and sharing. First, geo-located data are most important for almost all ITS applications, because information about how many vehicles move at which speed and where is essential. Second, potential legal challenges may arise as geo-located data can be traced back to individuals. Third, we find already today business models, in which more than two actors cooperate to provide services based on data exchanges in (almost) real-time. Finally, geo-located data and highly precise maps play a critical role in the roll-out of autonomous driving applications.

Beyond the selected case of intelligent routing, there are two major examples of other services that make use of data produced in connected cars. Service and repair shops make use of data via the OBD-I or OBD-II data interfaces. Based on them data formats, usage policies, etc. are defined in standards as well as legislation. In this case, access to data is possible either via the 'generic' mode or the 'enhanced' mode. While all data available in generic mode can be accessed by anyone with a Data Link Connector (DLC), data in enhanced mode can only be unlocked by the Vehicle Identification Number (VIN) that is typically only available to the manufacturer itself.[356] If any telematics, diagnostic, or similar data are transmitted online to the OEM, access to these data relies with the OEM. There are some noticeable (anecdotal) attempts to gain access to more diagnostics data by large players like Google or Apple. However, the installed base of connected cars is currently too small to attract many new players. Given the growth rates shown in the above, this situation may change soon. In particular, the data created in cars bear significant value for all actors that are active in the aftersales market of vehicles. These actors fear that with increasing access to data by OEMs

[355] Urban ITS Expert Group (2013): Guidelines for ITS Deployment in Urban Areas.

[356] Allegedly, some smartphone apps can decode VINs.

their business models may become less relevant. Consequently, they demand to have the same level of access to data as the OEMs themselves to create a 'level play field'. In fact, the C-ITS platform[357] is intended to work somewhat like the access that Google (with Android Auto) and Apple (with CarPlay) can gain to the vehicle. The vehicle's system is essentially treated as a platform for different application that can draw from data produced in the vehicle and communicate with external servers based on the connection established either by SIM-Card installed in the vehicle or a smartphone with tethering enabled.[358]

The second major example refers to car insurances that make use of data on drivers' behaviour to tailor specific tariffs commonly known as 'pay as you drive' or 'pay how you drive'. Typically, these services do not make use of any data collected by the vehicle. Instead, insurers provide drivers interested in such tariffs with a black box or an app for their smartphone that monitor driving behaviour. The data that are collected are made known to the driver in the terms and conditions of the insurer's contract. Data are commonly only used for the purpose of tailoring the insurance. They are not re-used or exchanged with other third parties. Consequently, typical questions related to data access and sharing do not arise in this case.

The nexus between data ownership, access to and use of data, and the interoperability of services

In the selected case of navigation and the exchange of geo-located data from connected cars, there are two major types of actors both of which use data from various sources. The first type of actor can be described as providers of dedicated navigation solutions, which are commonly built into the car itself or realised using a dedicated electronic device. The second type of actor can be described as providers of software applications for mobile devices offering route planning functionalities.

For the first type, tom-tom and HERE constitute two relevant market actors. While tom-tom is a (component) supplier that also offers dedicated devices to end-users, HERE (formerly Navteq, later owned by Nokia) was acquired and is now co-owned by the three Germany OEMs Audi, BMW and Mercedes in 2015. The purchase of the company by the OEMs was considered a step towards becoming more independent from third party services offerings as well as an investment in a future of automated and autonomous driving.

[357] The C-IST platform was developed by expert working groups in collaboration with DG MOVE between 2014 and 2016 in order to enable a collaborative intelligent trransport system including the access to in-vehicle data through a secure and standardised platform. The final report of the project provides a good overview of the purpose, cost benefit analysis, and use cases of such a platform: C-ITS Platform – Final Report. January 2016: http://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf

[358] Notably, business models would have tob e created in order pay fort he mobile subscription and potential roaming fees for data transfer. Since data would only be transferred if there is a reason to do so e.g. a failure code reading, data volumes are likely to be small.

For the second type, map applications by mobile device / operating system providers such Google and Apple play an important role next to free and paid-for applications by third party vendors.

The technology for such services commonly builds on cloud computing / central data centres. Given the direct relationship between the number of data points imputed and the accuracy of traffic forecasts as well as other outputs, scale is absolutely essential for both types of service providers. Thus, it is not surprising that they try and gather data from as many relevant sources as possible. Concretely, more cars equipped with the technology can provide more information (e.g. traffic and road conditions) and thus enhance the precision of the services. In North America and Europe, four out of five cars use HERE technology.[359] Consequently, the owners of the technology are keen to include more consortium partners as well as customers. As of 2016, HERE technology is integrated into the in car infotainment system of some Jaguar models offering mapping and navigation services.[360]

Since geo-located data is relatively well-structured (as compared to unstructured data retrieved from semantic analyses etc.) and builds on standardised data formats, interoperability is rarely an issue. In fact, even data retrieved from third parties can be brought into a form that makes them usable for provisioning of mapping services.[361] Data ownership is also not an issue in this case. First, given that most connections run on 2G and 3G networks and have to work even in remote areas, where there is bad radio signal, applications are build and operated with the best data efficacy possible. So, only few data points are transferred. Second, data are generally anonymised and split up in a way that re-engineering the original (personal) data is impossible. In fact, with current business models for the considered applications, there is little or no incentive for service providers to collect personal data. Third, if such data are transferred from one actor to another, this is negotiated by clear-cut contracts. In most cases, data ownership is unlikely to be transferred, as fully anonymised data are only used (not owned) by the cooperating actor.

Access and (re-) use of data: Boundaries and mitigation actions

In sum, issues linked to access and (re-) use of data concern only a fraction of the data produced in connected cars. The vast majority of data produced in connected cars is transient and only used to trigger specific functions or display information for the driver. A significant part of diagnostics and maintenance data are available via the OBD-I/OBD-II interface. Tailored insurances do not use any data from connected cars directly.

Issues relating to access and (re-) use of data may arise with manufacturers' so-called enhanced OBD data. However, it has to be noted that the data that are not shared via the OBD-I or OBD-II interface are commonly highly sensitive and concern operational and business secrets. C-ITS can be a potential solution provide secure and standardised access to in-

[359] See Nokia (2014): http://company.nokia.com/sites/default/files/download/nokia_uk_ar14_here.pdf
[360] See Jaguar: http://jaguar.navigation.com/home/de_DE/JaguarEMEA/EUR
[361] This is true for all mapping services. See e.g. Arnold, R.; Kirch, M.; Waldburger, M. & Windolph, A. (2014): Broadband and infrastructure mapping. A study by TÜV Rheinland Consult and WIK-Consult for the European Commission. SMART 2012/0022.

vehicle data. Whether actual business cases can emerge from such an access remains to be seen given the relatively small number of connected cars and the fact that most aftermarket outfits are SMEs, which hardly have the capability that is required to collect, store and analyse data streams from several millions of cars in real-time. It seems more likely that large suppliers like Bosch, Continental, or Valeo will position themselves successfully if such a platform is established.

The second service where data are exchanged among various partners is ITS and in particular intelligent routing, which was the focus of this case study. In this case, access to data is well-organised among market actors through contracts. We received no indication from the experts that we spoke to that there were any issues that would require policy intervention. However, access to data from public transport systems and road infrastructure appears to be a significant issue according to one interviewee. In these cases, tax payers' money is used to fund mostly public and private suppliers who tend to keep data to themselves. This constitutes a substantial barrier to the full deployment and reaping the benefits of an intermodal ITS in the near future.

This perspective is strongly supported by the actors participating in the German IT Summit process organised by the German Ministry for Economic Affairs and Energy whose objective it is to identify relevant obstacles that prevent data flow among the actors and formulate specific targets to overcome the main impediments. In fact, it is one of the prime directives of the IT-Summit process to create and enable a national scope of action for the generation, protection and transparent usage of data in ITS.

Based on their work, it is necessary for the transparent handling of data in ITS to establish data quality criteria in order to create a basis for sustainable and efficient transportation applications and solutions. This has to include standardised access to public traffic, sensor, and similarly useful data to deploy a national or even European ITS.

Potential barriers to data access and sharing and their cost

The interviews with actors in the market revealed that exchange of geo-location data is not an issue. Data are typically exchanged in line with individual contracts and agreements. Actors in the aftermarket however do see potential barriers if the manufacturers gain full control over vehicles' data and can negotiate the access to that data on their own terms, potentially excluding some or all aftermarket (independent) actors or limiting their access to data as compared to the open and standardised OBD-I/-II interface that is now available.

A recent study by McKinsey (2016)[362] values the potential market for car-generated data at US$450 to US$750 billion by 2030. This represents a significant opportunity for various actors ranging from the manufacturer of cars over garages and workshops to third party actors like Content and Application Providers (CAPs). Beyond this direct effect, any degradation to accessing car data via OBD-I/-II or hindrance to effectively access relevant new in-car data

[362] McKinsey&Company. 2016. Monetizing car data - New service business opportunities to create new customer benefits. McKinsey&Company - Advanced Industries.

can stifle innovation and business in the aftermarket. The aftermarket represents around 500,000 companies across Europe and 3.5 million jobs.[363] This is why FIGIEFA (the European federation and political representative in Brussels of the independent wholesalers and retailers of automotive replacement parts and their associated repair chains) strongly claims that in-vehicle real time (vehicle-generated) data are not owned by anybody and has to be open to the (re-)use of aftermarket players (e.g. for independent diagnosis). In FIGIEFA´s view legislation is needed to mitigate the risks of foreclosure to data access and to allow independent automotive aftermarket to continue to support competitive consumer choice.[364]

As a recent study commissioned by DG MOVE also emphasizes, the "model of access to in-vehicle data should ideally mitigate the concentration of power with one group of market participants to prevent the situation where, before competition law can be effectively applied, the market has already been distorted to the detriment of consumers".[365] In sum, with the aim of maintaining a level playing field as regards in-car data policy makers need to ensure fair access to these data. The current legislative framework appears to create in principle the necessary environment by guaranteeing access to data via a standardised interface. These concepts should be transferred into the upcoming much more data-driven automotive value chain.

[363] FIGIEFA.

[364] See FIGIEFA statement, December 2016, https://www.figiefa.eu/wp-content/uploads/FFoD-FIGIEFA-input-Updated.pdf. See one of the examples in the text for competitive advantages: "The predictive maintenance system which is already introduced by vehicle manufacturers such as BMW in new car models (e.g. "BMW Teleservice"). Due to the constant monitoring of the car by the vehicle manufacturer's proprietary diagnosis application installed in the vehicle and displayed to the driver "on the dashboard of the car" the vehicle manufacturer knows first when a certain part needs urgent replacement and can immediately contact the car driver proposing a replacement in one of its authorized workshops. The instant monitoring of the car by remote connection becomes a clear competition advantage over the current "analogue" situation."

[365] TRL (2017): "Access to in-vehicle data and resources", Study for the European Commission, Directorate-General for Mobility and Transport, p. 8, https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf.

Retail sector

Context: the role of data in the retail sector

Retail has long been a data-intensive sector: Traditional retail stores and mail-orders already assumed the role of both data producers and consumers before the advent of the internet and its effect on the market.

Physical stores have increasingly turned into data producers over the last decades due to the proliferation of barcode scanners at the *point of sale* (or the later use of RFID tags). By the 1980s, this data has been used to analyse and categorise typical contents of shopping carts, or to link certain products to certain times of purchase.[366]

Mail-order businesses, on the other hand, have always produced data about their customers. They need names and addresses to deliver goods or use financial data and demographic information about customers to facilitate payments and reduce business risks. Additionally, individual customers provide them with records about their choices regarding product characteristics (e.g. sizes, colours). Mail-orders were quick to employ this data to uncover purchasing patterns and underlying customer preferences, using this information for targeted marketing offers.[367] Third party **data analysts** not directly engaged in retail relationships are not new to the sector either: The first marketing agencies started investigating consumer purchase patterns as early as the 1920s.[368]

In recent years, retail has experienced a disruptive shift from the physical to the virtual world, with high growth rates for **e-commerce** and stagnant to declining sales volumes on high street. Given the opportunity, consumers worldwide increasingly shop online, for a number of reasons such as higher convenience, a wider array of choices and lower prices.[369] This concerns various sectors, including clothes and electronics with a high share of online purchases[370] as well as FMCGs. Although the share of online purchases is lower in relation to FMCGs compared to other types of goods, the market for online grocery shopping has been growing quickly in the past few years.[371]

Considering the retail sector as a whole, a number of stakeholders are involved in the generation, use and analysis of data in this sector. An overview is presented in the following table.

[366] Forrester (25.02.2015): *Big Data in CPG and Retail.*
[367] Master's in Data Science (undated): History of Data Analysis and Retail, http://www.mastersindatascience.org/industry/retail/
[368] Schwarzkopf, S. (2016): *In search of the consumer. The history of market research from 1890 to 1960*. In: Jones, B. and Tadajewski, M. (eds.), *The Routledge Companion to Marketing History. Routledge Companions in Business, Management and Accounting*.
[369] PWC (2015), Total Retail 2015, http://www.pwc.com/gx/en/retail-consumer/retail-consumer-publications/global-multi-channel-consumer-survey/assets/pdf/total-retail-2015.pdf, p.9.
[370] Cf. PWC (2015), Total Retail 2015, http://www.pwc.com/gx/en/retail-consumer/retail-consumer-publications/global-multi-channel-consumer-survey/assets/pdf/total-retail-2015.pdf
[371] See http://www.syndy.com/report-the-state-of-online-grocery-retail-2015/

Table 26: Stakeholders potentially involved in the generation, use and analysis of data in retail

	Not data driven business models/ companies	Data driven business models/ companies
Data producer (sharing data)	- Producers of goods/brands - Retailers, including brick-and-mortar, mail order and online	- Customer loyalty programmes - Shopping apps - Data platforms - Manufacturers of hardware used to generate data (e.g. beacons)
Data user (accessing data)	- Producers of goods/brands - Retailers - Advertisement industry	- Analytics provider - Cloud provider

Source: Deloitte.

Retailers generate and use a **great variety of data points** on products sold, their logistics and supply chain, their customer base, competitors or their surroundings.

Table 27: General examples of data generated and used in retail contexts

Product	*Logistics & Supply Chain*	*Customer*	*Competitor*	*Surrounding*
- Package sizes - Expiry dates - Placement and location - Return rates	- Transport data - Timing of (re-) orders with wholesale distributors - Availability - Stock	- Purchased quantities - Shopping carts / typically combined purchases - Preferences / sizes / tastes - Reaction to pricing / discounts - Repeat and unique visits (frequency) - Financial information - Movements / in-store navigation - Customer service interactions	- Pricing - Range of products - Marketing activities - Locations - Expansion movements	- Queues and cashier waiting times - Temperature in storing facilities *External sources:* - *Weather forecasts (weather, temperatures)* - *Social and demographic*

Source: Deloitte

To increase the usefulness of this data and create additional benefits, retailers may need to **combine various types of data**. For example, before ordering barbeque meat a retailer may check the weather forecasts and consumers' preferences about the type of meat typically bought. Then, it may consider where to place the product based on data on client movement patterns. Once the meat is in the store, the temperature of the refrigerator and the availability of the product needs to be monitored to ensure that the meat remains fresh and in stock. In addition, the retailer may decide to send personalised coupons to customers that are likely to be interested in barbeque meat based on their attributes (e.g. age, gender) and previous purchases.

Table 28 outlines the evolution of data generation and use in retail contexts in the past decades, from simple anonymous recording of physical purchases to more sophisticated collection, (re-) use and re-combination of data provided by customers.

Table 28: Evolution of data generation and use in retail contexts (actor-centric perspective)

	Point of Sale data	***Retailer loyalty programmes***	***Third party loyalty programmes***	***Omni-channel data linkages and big data analytics***
Data quality	crude	medium	detailed	precise
Actors involved	Customer, Retailer	Customer, Retailer, IT-provider (terminal, software)	Retailer, card company, IT-provider (terminal, software, analytics)	Retailer, app developers, IT-provider for real time customer tracking (e.g. networks, beacons, software, analytics)
Scope	Own range of product	Own range of product	Own range of product + insights from partner's ranges of products	Own range of product + insights from partner's ranges of products
Focus	- Sold products - (Combinations of sold products)	- Sold product - customer purchases - customer preferences	- Sold products - Customer purchases - Additional product preferences of customers	- Sold products - Customer purchases - Customer preferences - Future customer preferences - Customer reaction to offers
Data characteristics	Anonymous, information based on own range of product	Personalised, information based on own range of product	Personalised, information based on own and partners' range of products	Personalised, real-time and predictive capabilities based on personality profiles (enriched with data from other sources)

Source: Deloitte

Several stores already experiment with data-driven retail solutions, including closer links between their online catalogue (offering larger arrays of choices) and in-store experience (enabling a physical interaction with products). For example, *Tesco* has been using real-time data and analytics to improve its services, as described in the following text box.

Possibilities of data-driven retail: the example of Tesco

Tesco, one of the world's largest retailers makes use of real-time data and analytics in various ways, optimising its operations.[372]

It **collects data about the situation on its shelves**, making it possible to predict when products need to be reordered. The data from the electronic shelves may also be used to control and adjust the pricing policy. This is supported by the use of **weather forecasts**, enabling Tesco to predict when specific products will be more popular (e.g. a rise of temperature may lead to an increased sale of barbeque meat, lettuce and coleslaw) as well as prevent food from spoiling.[373]

A **customer loyalty card** (Clubcard) collecting data for computerised analysis was introduced as early as 1993, allowing Tesco to better understand the consumer experience. Tesco became the top supermarket of the UK one year later. Today, Tesco uses the data generated by around 16 Mio Clubcard owners as a support for decisions on various aspects of its value chain, including supply

[372] See: Castro, D. and McQuinn, A. (2015), *Cross-Border Data Flows Enable Growth in All Industries*, http://www2.itif.org/2015-cross-border-data-flows.pdf.

[373] Miller, P. (2012), *Tesco uses data for more than just loyalty cards*, http://cloudofdata.com/2012/10/tesco-uses-data-for-more-than-just-loyalty-cards/

chain, sales and services. For example, Tesco is able to offer coupons for customers in a targeted manner based on their shopping behaviour.[374]

Tesco also uses an **omni-channel approach**, e.g. enabling the use of mobile devices to order groceries to be delivered home or the introduction on kiosks in which customers can order products to be picked up the next day.[375]

Furthermore, data is used to **reduce energy costs and waste**. This was achieved by installing intelligent technology in Tesco's refrigerators, which ensures that they stay at proper temperature as they system is constantly monitored.[376]

Consumers benefit as the shelves are always fully stocked, prices are low, products are fresh and the communication with Tesco is targeted to their needs.

This case study presents a sectoral snapshot examining the generation and use of data in the retail sector further, looking into different contexts and business models (cf. the following sub-section). For this purpose, the project team carried out desk research, spoke to two beacon manufacturers, a retailer and two business associations.[377]

Business models

Compared to physical stores, online shops have some advantages with regard to the use of data: They are not only able to accept a lower margin due to lower costs for operations, but are also **often better informed about their customer's tastes and buying decisions**. In the online world, it is comparatively easy to follow the buying behaviour of consumers in real-time, analyse it and adjust business strategies on this basis.

In comparison, physical stores sometimes face challenges, as they often:

- Have limited knowledge on their customers' movement and buying decisions;
- Lack the information and technology to adjust their prices dynamically;
- Experience lower conversions compared to online shops; and
- Forego opportunities to optimise their logistic supply chain.

This prevents retailers from reacting in optimal ways to market changes and consumers' needs. In the market, we see that retailers have started experimenting with different **potential solutions** to these challenges, relating to digitisation and datafication of brick-and-mortar retail. Examples of such solutions include:

- Omni-channel retailing, possibly using online platforms;

[374] Winterman, D. (2013), *Tesco: How one supermarket came to dominate*, http://www.bbc.com/news/magazine-23988795.
[375] Castro, D. and McQuinn, A. (2015), *Cross-Border Data Flows Enable Growth in All Industries*, http://www2.itif.org/2015-cross-border-data-flows.pdf.
[376] Ibid.
[377] We contacted numerous additional stakeholders, including business associations, retailers, software- and app-developers, to reflect the different perspectives as far as possible. Although a number of stakeholders expressed great interest and identified the topic as relevant for practical contexts, comparably few provided in-depth information on specific projects and contractual relationships. For some types of business models, there appears to be a general reluctance to share insights from real-world examples as many stakeholders are currently still in an experimental phase and competition in the sector is high. We also heard that the sector is generally careful with sharing contracts based on an incident a couple of years ago.

- Customer loyalty programs (check-ins through social media, coupons to app users)[378];
- In-store tracking solutions (e.g. in combination with loyalty programmes).

We discuss these points below.

Omni-channel retailing and online platforms

Retailers have started to shift from purely physical and/or online to **omni-channel retailing**. Within this approach, retailers offer their customers a choice of channels for shopping and interaction, including e.g. online and physical stores, smartphones, social media, call centres, and email. This way, consumers can flexibly choose their preferred channel depending on their needs.[379] In a recent study, Herhausen et al. explain how user perceptions of online shopping also influence their offline shopping behaviour. On this basis, integrating internet and physical store channels increases sales and customer satisfaction. They illustrate how pressures are mounting for retailers using several channels to meet customer expectations and physical retail stores competing for those shoppers that do not exclusively rely on online stores.[380]

In this context, **online platforms** facilitating online retail (notably marketplaces[381] such as *Amazon* or *bol.com*) have become increasingly important and have developed at a fast pace. On online marketplaces, goods of various retailers are available to the consumers on one platform. For transactions between retailers and consumers, the marketplace usually acts as an intermediary. There are advantages for both consumers (e.g. bundled offer, possibility to compare prices) and businesses (e.g. possibility to use an existing infrastructure, benefits from network effects). Indeed, there are some retailers that exclusively sell on platforms.

An interviewee highlighted that the use of platforms (or similar institutions) is not specific to ecommerce, it has always been relevant in retail. According to him, online platforms may be compared to supermarkets in the offline world.

As other types of online platforms, online marketplaces accumulate significant amounts of data and thus play an important role in digital value creation. The amount of control over the data and relationships between different participants varies from platform to platform.[382]

---

[378] Hyunjoo Im and Young Ha (2015): Is this mobile coupon worth my private information?, *Journal of Research in Interactive Marketing*, Vol. 9 Iss 2, pp. 92-109

[379] PWC (2015): The 2015 Global Omnichannel Retail Index: The future of shopping has arrived. http://www.strategyand.pwc.com/media/file/2015-global-omnichannel-retail-index.pdf

[380] Deloitte Digital (2017): The future of retail – 11 predictions on the disruptive forces in retail (https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte-Digital-Future-of-Retail-11-Predictions-English-2017.pdf); Herhausen, D et al. (2015): Integrating Bricks with Clicks: Retailer-Level and Channel-Level Outcomes of Online–Offline Channel Integration, *Journal of Retailing*, Vol. 91, Iss. 2, pp. 309-325

[381] There are various other types of online platforms, including e.g. online advertising platforms, search engines, social media or platforms for the collaborative economy.

[382] Cf. European Commission Communication: *Online Platforms and the Digital Single Market – Opportunities and Challenges for Europe*. COM(2016) 288 final.

Loyalty programmes

A structured marketing strategy that also facilitates analysing and re-using the data listed above in a systematic way are **customer loyalty cards** or **cash-back programmes** (e.g. *Tesco Clubcard*). Here, retailers offer customers using membership cards in a transaction:

- A discount (sometimes on selected products or product combinations); or
- An allotment of points for future rewards (or cash reimbursements).

In their initial form, i.e. paper cards stamped by the cashier at the point of sale (POS), these programmes aimed at prompting customer returns by offering (non-personalised) discounts or free products and services after a certain number of visits. In the present form, they require a registration by customers in return for a card containing the information about customers in form of a barcode, on a chip or magnetic strip. This enables retailers (other than mail-orders) to link data on personal characteristics to data generated in transactions for the first time.

Aside from incentivising customers to return, the true value of these accounts lies in their function to produce a detailed individual customer profile and the possibility to analyse aggregated data. In the aggregate, socio-economic and demographic information provided by customers can be used to identify relevant segments of customers, e.g. by their average expenditures in store, their time of visit, etc. Ultimately, this aggregated data helps to predict what certain groups demand or identify when their situation and buying patterns change to adapt in time. *Table 29* provides an overview of the various data points collected in different programmes.

Table 29: Examples for data gathered by providers of selected loyalty card or cashback programmes

Type	Organisation	Card usage data collected[383]
Third-party	*Lyoness*[384] (Europe)	- Data about purchases
	Payback[385] (DE,IT, PL)	- Discounts used - Discount characteristics - Product/service type - Product/service price - Date of use - Retailer/Service - (except for pharmacies and financial services)
Retailer programme	*Tesco Clubcard*[386] (UK, IE, CZ, HU, PL)	- Store (location, etc.) - Products purchased - Product price
	BudniCard[387] *(Germany)*	- Date and time of use - Store location

[383] In addition, all of these programmes collect personal data, usually including at least name and contact details.
[384] https://www.lyoness.com/eu/privacy-policy
[385] https://www.payback.de/pb/id/294154/
[386] Cf. Winterman, D. (2013), *Tesco: How one supermarket came to dominate*, http://www.bbc.com/news/magazine-23988795.
[387] https://www.budni.de/service/budni-karte/online-antrag/

		- Product/service type (sale, return, etc.) - Product/service price

Source: privacy policies of selected companies, tabulation by Deloitte

To set up a loyalty card infrastructure, retailers require:

- Additional hard- and software at the POS to collect the data;
- Databases to store and process data;
- Administrative capacities to register customers and manage rewards; and
- Staff and know-how to interpret customer data and develop incentive frameworks.

These requirements[388] may present certain drawbacks for individual retailers, especially smaller ones: First, they are costly because of the needed hardware and software required to register customers and log as well as redeem their purchases. Second, meaningful information about single customers is only generated through frequent purchases and not for durable goods, such as furniture (where some items are only bought once in a decade). These two points together reduce the applicability and preclude reasonable implementation in SME contexts. Third, even fully functional and effective loyalty programmes of single retailers only generate data on their range of products already held.

As a result, **third party loyalty programmes** (e.g. *Lyoness*, *Payback*) have entered the market: These actors plan and implement the necessary infrastructure on behalf of retailers, potentially reducing their costs while increasing the possible range of benefits for members. These loyalty programme operators are able to increase the quantity and quality of information generated for individual customers, as they are tracked across different shops and service providers.[389] In addition, they may also appeal to retailers mainly selling durable consumer goods due to the potential variety of information on customers gathered across shops. Third party loyalty programmes can also be more attractive for customers as they reduce the number of cards needed and increase the number of opportunities to collect discounts and rewards.[390]

The main data-driven business model for innovation in retail has grown from the aforementioned loyalty card programmes: To improve predictions about consumer behaviour, retailers increasingly turn to specialised **big data** companies which perform **analytics** over their own internal data (often enriching it with external dataset from as social media outlets, beacons and mobile phones).

An example of a start-up creating value based on customer data is the Retail Media Group (RMG).[391] They offer targeted media campaigns based on analyses of customer data of cooperating German retailers. All data is used on an anonymous and aggregated way and it is

[388] Additional challenges and pitfalls for retailers will be discussed in more detail in the section on business models below.
[389] Sharp, B. and Sharp, A. (1997), “Loyalty Programs and Their on Repeat-Purchase Loyalty Patterns”, In: International Journal of Research in Marketing, 14 (5), 473-86.
[390] Sharp, B. and Sharp, A. (1997), "Loyalty Programs and Their on Repeat-Purchase Loyalty Patterns", In: International Journal of Research in Marketing, 14 (5), 473-86.
[391] See: http://www.retailmediagroup.de/

not possible for clients to access the data. They benefit from the aggregation and analyses as they feed into the campaigns.

Thus, depending on the structure of the programme, both forms of loyalty schemes may involve additional stakeholders, for example data analytics companies, customer service providers, hardware manufacturers or software developers. The potential relationships between the different actors are presented further in the next sub-section (see Figure 43), as they are similar for business models related to in-store tracking.

In-store tracking

New, innovative business models that link data analytics and loyalty schemes are emerging based on **in-store tracking**: sensors that allow monitoring of consumers' interactions. Such technologies present potential advantages for retailers, as they facilitate the collection of consumers' behaviour data at the premises of the retailer, and accumulate new types of high quality data that can be used to provide value-added services. Recent technologies enable physical retailers to track customers' movements and buying decisions with a level of precision previously unknown.

While there are different technical solutions to achieve this, the **beacon technology** is widely recognised as an important tool, which could provide retailers with a range of opportunities to close the growing gap to the convenience of online shopping.[392] A beacon is a small, battery-powered transmitter device using *Bluetooth Low Energy* (BLE) technology to transmit a constant signal. In its most simple application, the signal can be used to locate persons via their mobile devices with high precision. The beacon itself is only a transmitter. It is not able to receive (and store) any data concerning its users.

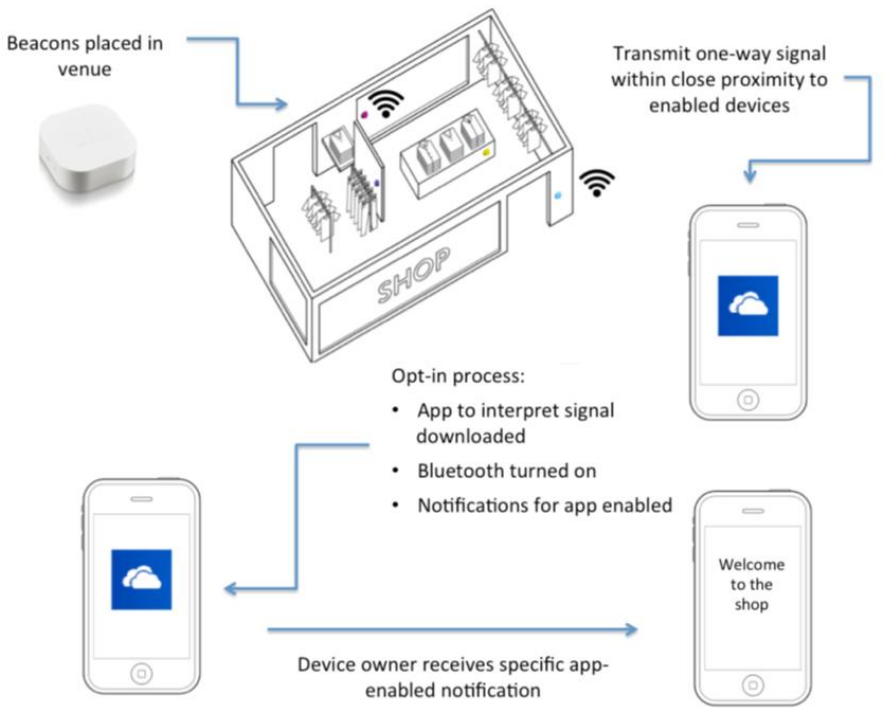
Due to the simplicity of the beacon signal, **an app is required** to enable the full range of possible location-based actions, once it is picked up by nearby mobile devices.[393] While all beacons rely on Bluetooth technology, **a number of *Application Programming Interfaces* (APIs)** or protocols exists for translating the signal information on devices, i.e. in apps.[394] Depending on the API used the signal may, for example, trigger a push notification or open a related app on the smartphone of a customer in the background to enable further interactions.

[392] Among the vast emerging literature on the beacon technology, a concise overview is provided by the Fung Business: Fung Business Intelligence Centre (FBIC) (2015): Beacon trends in the Retail Space 2015, https://www.fbicgroup.com/sites/default/files/Quick%20Take%20on%20Beacon%20Trends%20Jan.%2029,%202015.pdf

[393] Sterling, Polonetsky, Fan (2014): Understanding beacons. A guide to beacon technologies, https://fpf.org/wp-content/uploads/Guide_To_Beacons_Final.pdf

[394] As the technology is relatively new, several major players in in the smartphone and smart device market have started out with different protocols/APIs for developers to build apps like *Apple* (*iBeacon* for *iOS*), *Google* (Eddystone, cross-platform), *Samsung* (*Flybell*, under development) or *Paypal* (*Paypal Beacon*, cross-platform). Increasingly, beacons and apps are able to send and receive several transmission and interpretation protocols to enhance cross-platform compatibility and increase the base of possible users.

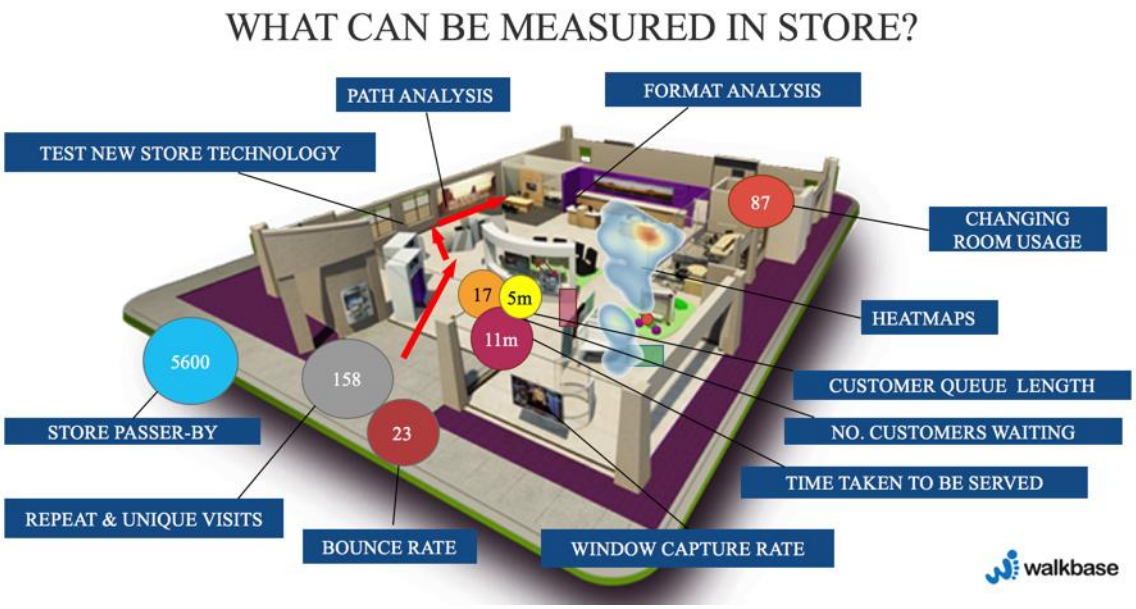
Figure 41: Beacons explained



Source: Sterling, Polonetsky, Fan[395]

An example of the type of data that can be generated and analysed with the use of beacons is presented in the following figure.

Figure 42: Examples for customer tracking applications in retail contexts



Source: Walkbase[396]

[395] Sterling, Polonetsky, Fan (2014): Understanding beacons. A guide to beacon technologies, https://fpf.org/wp-content/uploads/Guide_To_Beacons_Final.pdf

While the possible usage of the beacon technology is diverse, the following **functions** are typically offered/used in the retail sector:

- With the help of beacons it is possible to provide **services to consumers** to enhance their shopping experience, such as:
  - Information about the facilities (e.g. accessibility);
  - Indoor navigation to guide customers to products of interest or sales persons within the store;
  - Proximity marketing, i.e. push notifications about specific offers to devices of nearby customers;
- The use of the apps connected to the beacons **generates data** about consumers' shopping behaviour, helping retailers to improve their services by carrying out **user analytics**, e.g. on:
  - General movement patterns, frequency and duration of visits; or
  - Product interaction and products bought.

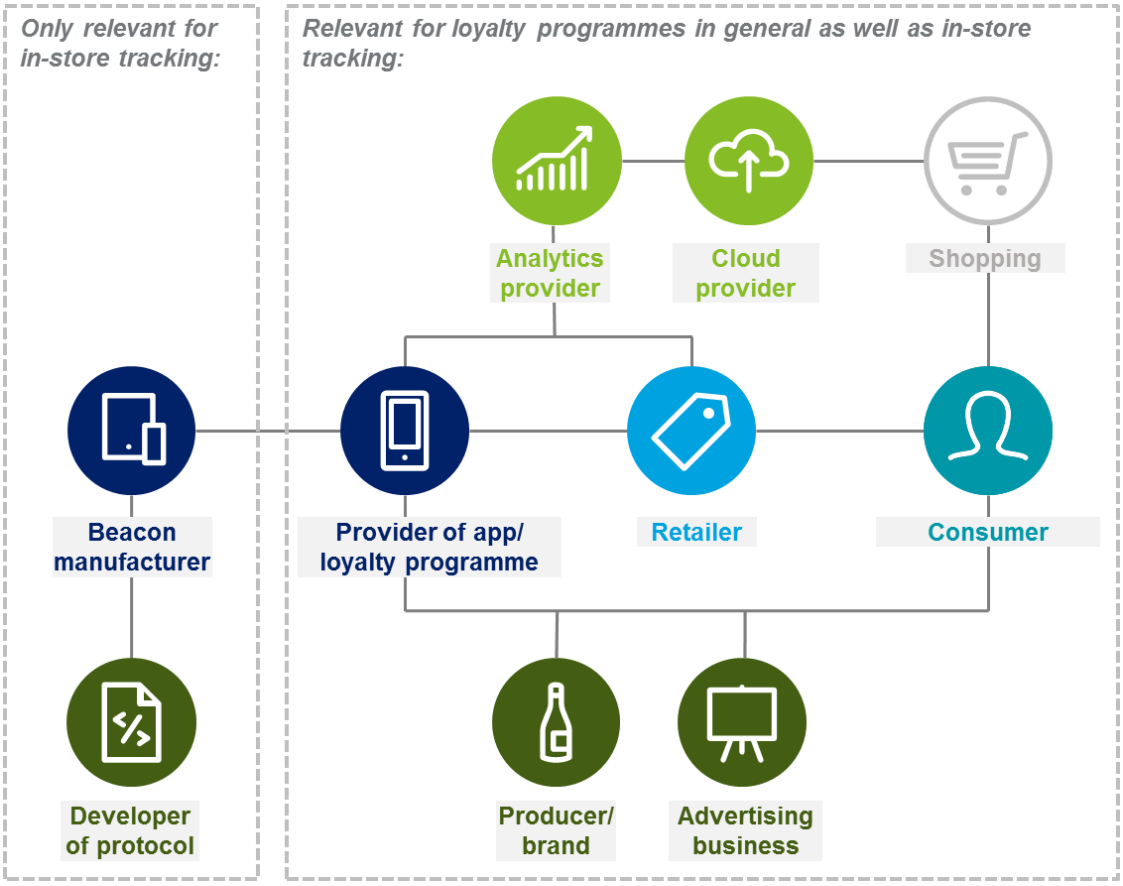
There are different types of business models offering services to retailers in this context: there are businesses that focus on selling the hardware (beacon manufacturers), businesses that focus on software solutions (apps and analytics) and businesses that provide both hardware and software to the retailers. Concrete business models could, for example, entail the installation of beacons in combination with the development of an app and the provision of corresponding analytics software. The apps may be connected to a customer loyalty scheme, e.g. offering rewards to customers for certain actions (entering a store, scanning specific products or their purchases).

While some retailers (the larger ones) may implement the relevant services and technologies largely on their own, many will work with specialised service providers offering relevant solutions.

The following figure provides a schematic overview of the actors potentially involved in relation to in-store tracking solutions as well as loyalty programmes, as these are closely linked. In practice, it is possible that a smaller number of actors is involved compared to the figure below, as some businesses provide several different services together (e.g. combination of hardware and software). Furthermore, the actual connections may vary, depending on the exact business model. This is discussed in more detail below.

[396] Walkbase (09.09.2016): Why heat maps is the least cool thing about in-store analytics, http://www.walkbase.com/blog/why-heat-maps-is-the-least-cool-thing-about-retail-analytics

Figure 43: Schematic overview of potential actors (loyalty programmes and in-store tracking)



Source: Deloitte.

For in-store tracking solutions, the first relevant actor is the **beacon manufacturer** that designs and assembles beacons applicable for a variety of retail scenarios – based on standards of protocols offered by other companies to enable uses by software programmers. The most common protocols are provided by Apple and Google. Usually, the beacon manufacturers provide (at least basic) **software solutions** to program the hardware's actions and analyse the results from interaction data gathered. Only some hardware manufacturers also offer installation and maintenance service on-site.

As pointed out above, the beacon used for **in-store tracking** can only be used in combination with an **app**. There are different possibilities of who may provide such an app. First, there are specialised software businesses offering targeted solutions so retailers. In such a constellation, the software business may acquire beacons from a beacon manufacturer or produce them itself. It may offer a package to the retailer, including the installations of beacons, the programming of a specific app and possibly also the analysis of the information gathered or an analytics software that may be used by the retailer. As an alternative, third-party apps allow retailers to reach a larger user base than those that have installed their (highly specialised) app. Examples include *shopkick* or *bluesource*. Typically, such apps promise retailers an

increase in traffic and may receive a commission for sales they help to initiate.[397] They may also sell the data they generate back to retailers for the purpose of analytics.[398]

Similarly, in relation to **loyalty programmes**, retailers may either use their own programme (that could involve a card or an app and could be developed in-house or with external support) or third-party programmes, as described in the previous sub-section above.

The relevant apps / loyalty programmes are then used by the **consumers** when shopping or browsing. The data may be stored **on clouds or locally**, with the retailer or app provider. The extent to which retailers have access to the consumer data depends on whether they use their own app or third-party apps and the specific contractual relationships. In the case of third-party apps/programmes, consumer data is only shared to a limited extent, usually in aggregated format.

Specialised **analytics companies** such as *ShopperTrak* may support with the analysis of the relevant data. Alternatively, software providers may sell analytics software to the retailer to use on their own.

In addition, **producers of goods/brands** as well as **advertising businesses** may also be involved. For example, *shopkick* cooperates not only with retailers, but also with specific brands. Consumers may earn loyalty points for scanning specific products. This may affect the retailer, as consumers are influenced in their shopping behaviour. Such offers may be part of the strategy of advertising businesses.

Potential contractual barriers

Data ownership

The data generated by online platforms, loyalty programmes as well as in-store tracking systems and apps typically include data on consumers' shopping behaviour, including e.g. online shop or store visits, movement patterns, items that were considered and items bought.

Challenges relating to the ownership may also arise **when retailers use third party loyalty programmes or third-party apps (possibly in combination with in-store tracking systems)**. Usually, third party loyalty programmes usually claim ownership of the data generated with their programmes. Similarly, in the context of in-store tracking systems, it seems that the third-party app providers are usually the owners of the data. The providers of the loyalty programme or app argue that the data is generated by consumers using their programme/app. Usually, they are also in charge of storing the data. Yet, there are some retailers that try to negotiate with the third-party app providers. The retailers may argue that the data is generated by their customers and in the case of in-store tracking systems the bea-

[397] McDermott, J. (2014), Shopkick: driving retail in exchange for data, http://digiday.com/platforms/shopkick-raw-deal-retailers/

[398] http://bmtoolbox.net/patterns/customer-data-monetization/

cons installed in their store. A potential solution could be to cross-license data, ensuring that both parties have rights to access.[399]

Turning to **online platforms**, it is usually the platforms that claim ownership of the data generated via the platforms. Again, there are some companies that try to negotiate with the platforms. However, the platforms are practically in control of the data.

While this does not necessarily present a barrier in itself, it may influence the access to and (re-) use of the data concerned, as discussed in the following sub-section.

Access to and (re-) use of data

One of the main issues in relation to **online platforms** is the relationship between platforms and retailers. For retailers that sell on platforms, it may be very interesting to access the data from the platforms (e.g. browsing data, search info). However, access is usually limited based on the contractual relations. As explained by an interviewee from a business association, retailers usually only receive data or analyses from the platforms to the extent that is needed for them to do their business properly. The interviewee explained that some retailers do not feel they receive relevant information about their customers' behaviour. This issue was e.g. also discussed on a DG GROW workshop on platforms.[400]

In relation to **loyalty programmes and in-store tracking systems**, the situation relating to the (re-) use of data depends on the exact relationship between the programme/app generating the data and the retailer. Two typical constellations include:

- The retailer uses a distinct programme/app, which may be developed in-house or by a specialised software business; or
- The retailer uses a third-party programme/app in which various retailers participate, such as *Lyoness, PAYBACK, shopkick* or *bluesource*.

In the first scenario, it is likely that the retailer controls the data generated by the loyalty card or app. An interviewed beacon manufacturer explained that it is common in retail that customer data generated via beacons and apps is stored locally. It is possible that retailers seek the support of analytics companies with a view to exploiting the data generated via the app.[401]

[399] Walle, T. (2015), *Beacons, Apps and Data Ownership*, http://beekn.net/2015/10/beacons-apps-data-ownership/

[400] See: https://ec.europa.eu/digital-single-market/en/e-commerce-and-online-platforms-workshop-2

[401] While it may seem counter-intuitive, barriers to the data economy might be higher in scenario 1 than scenario 2: Due to a possible "silo mentality" of online and offline retail channels, questions on data ownership, access and (re-) use might also pose barriers within larger companies. See: Piotrowicz, W. and Cuthbertson, R. (2014) Introduction to the Special Issue Information Technology in Retail: Toward Omnichannel Retailing, *International Journal of Electronic Commerce,* Vol. 18 , Iss. 4, pp. 5-16.

In the second scenario, it is often the loyalty programme or app that controls customer data, as discussed in the previous sub-section. This may be a disadvantage for retailers, as they do not have a direct relationship to the consumers and cannot directly access consumer data.[402]

A retailer explained that they partnered with a third party loyalty programme for a while, but then realised that access to data was actually limited. They were only able to access data in an anonymised and aggregated manner based on the contractual terms and the analyses were not what they needed. At the same time, they did not feel comfortable that competitors could actually benefit from the data generated by their customers. Thus, they did not see any added value in cooperating with that programme any longer. As a large company, they preferred launching their own loyalty card instead, which enables them have full control of the data and to carry out customised analyses in-house. However, it has to be taken into account that it can be **expensive** to generate and store data, as the data needs to be properly cleaned and organised to be useful. Thus, in some situations it is cheaper to buy data rather than generating it.

Thus, a challenge with respect to the business model of third-party programmes and apps will be to ensure that retailers will in fact be able to exploit the data generated by their consumers. This depends on the contractual arrangements between the app provider and the retailer as well as the pricing in relation to access to the data and support for the analysis.

In this light, *ShopperTrak* and *shopkick* recently announced a partnership to improve the use of their services for retailers and consumers. Retailers have the possibility of integrating the analytics solution of *ShopperTrak* with *Shopkick*'s award schemes and in-store beacon technology. This way, retailers may be provided with anonymised in-store analytics, allowing them to understand better consumers' shopping behaviour. They may exploit the analytical insight to improve their offer and stores and engage with consumers.[403]

From a **consumer perspective**, the access to data generated in stores might shift existing power relationships. Customers already enjoy a more balanced access to information in stores through their mobiles devices, e.g. to compare products or prices.[404] Taken together with the mobilising potentials of social media, information asymmetries between retailers and shoppers could decrease, while transparency as well as organised action increase.[405]

[402] What is more, it may be possible that such apps use the data of retailers with competitors (although there are no indications that this is actually done). McDermott, J. (2014), Shopkick: driving retail in exchange for data, http://digiday.com/platforms/shopkick-raw-deal-retailers/.

[403] http://www.shoppertrak.com/media/press-release/shoppertrak-and-shopkick-announce-game-changing-retail-partnership/

[404] Piotrowicz, W. and Cuthbertson, R. (2014) Introduction to the Special Issue Information Technology in Retail: Toward Omnichannel Retailing, *International Journal of Electronic Commerce,* Vol. 18, Iss. 4, pp. 5-16.

[405] Hagberg et al. (2016): The digitalization of retailing: an exploratory framework, *International Journal of Retail & Distribution Management*, Vol. 44 Iss 7 pp. 694-712 [p.702]

Risk and liability

In general terms, liability questions are not experienced as a barrier and none of the interviewees we spoke to knew of any practical cases in which liability played a role. Yet, some potential issues have been identified.

An interviewee from a business association mentioned that the *quality* of the data is usually not covered by any agreements/legislation. This could be an issue as marketing sellers usually have an interest in a high return of investments.

From the perspective of **third-party programmes or apps**, liability towards the retailer and the consumers potentially plays a role. We found two Terms of Sale valid between the providers of third-party apps and the consumers using the app. The first provider indicates explicitly that it may be held liable for not performing its contractual obligations. They specify that **product liability legislation applies**. The terms indicate explicitly that liability arising from misconduct of the consumer are excluded, listing also possible instances of misconduct (e.g. changing the app). The second Terms pf Sale state that the app provider excludes liability unless there was proven wilful or grossly negligent misconduct. The provider does not refer to product liability legislation, but only mentions that the limitations of liability do not apply in case of applying legal rules.

From the **perspective of beacon manufacturers**, liability questions are presently not experienced as a barrier in the retail sector. One beacon manufacturer indicated that liability of course needs to be taken into account when marketing a product such as beacons. However, this applies to any jurisdiction. He does not have the feeling that the situation is more difficult in the EU compared to other countries.

Both interviewed beacon manufacturers indicated that, while product liability legislation applies, they avoid liability claims by means of contractual agreements. It was indicated that it is common practice for hardware and software suppliers active in the sector is to rely on general contractual agreements **excluding liability for any damages** and data losses that occur **behind the retailers' *Internet Access Point***[406]. Indeed, the Terms of Sale of a beacon manufacturer we found online denied liability for any damages (including based on negligence), as far as this is possible based on local product liability legislation.

In order to stress the personal responsibility of retailers in this regard, (large) suppliers in the market even demand data and system security audits in their B2B contracts. Secondly, suppliers selling beacon hardware include **monitoring tools** for customers to check transmitter status and battery life – that way entrusting their customers with appropriate insights – while administering maintenance and updates directly over-the-air. A third way to avoid liability claims (as well as data ownership or portability questions) from the start is to **ex-**

[406] In the present context, this term was used in an interview by a hardware manufacturer to differentiate between customer data gathered and processed within in-store (wireless) network and any data processed outside of that the networks of the retailer by the manufacturer. In effect, this rules out liability for any errors in processing and interpretation undertaken by the retailers themselves e.g. caused by faulty hardware and insufficient security safeguards.

clude any possibility to process data collected by retailers via cloud software solutions but rather leave the data stored within customer networks.

Potential non-contractual barriers

Interoperability

Interviewees mentioned interoperability as an issue in relation to data exchange. There are currently different standards for databases. This makes database management more complex. An interviewed beacon manufacturer also mentioned that the connection of various sources does not always work seamlessly in practice. This is not a big problem for large companies, as they have large data sets themselves, as explained by a retailer. However, it may pose difficulties for smaller companies, dependent on buying data. From the perspective of retailers, it would be useful to develop a common infrastructure and develop common technical standards (ISO standards), as pointed out by an interviewee.

From the perspective of **beacon manufacturers**, interoperability is not a predominant topic. Currently, there are **two main standards** allowing mobile phones to pick up a signal by a beacon, which are widely recognised. These are *iBeacon* by Apple and *Eddystone* by Google. The spread and wide acceptance of these standards is an example of industry standard setting. While the existence and recognition of these two main standards facilitates the practical implementation of beacon systems, there may be other difficulties: the interviewee considers it a problem that the two standards are in the hands of two large companies, putting these companies in a monopolistic situation. The optimal solution would be the development of standards at a wider industry level, e.g. by business associations or other relevant standard-setting bodies. Private standards are best according to the interviewee.

Technical barriers

Technical barriers other than interoperability have been identified in relation to **in-store tracking systems**.

Given the fast technological progress in terms of user-friendliness of several in-store analytics technologies, by now even non-experts are able to deploy and administer hardware like beacons up to a store size.

Apart from the fact that users appear to be largely unaware of range limitations through concrete walls or security glass panes, a potential barrier to data access and sharing might be **interferences**. As the number of transmitting devices used by different stores is likely to increase in the future, the functionality of services based on wireless data exchanged between consumers, retailers and analytics applications might deteriorate.[407] This, in turn could increase the likelihood of disputes about sensor errors or decisions based on distorted information and ensuing liability claims as technology in the coming years. A stakeholder

[407] Locationinsider.de (16.02.2015): *Warum deutsche Händler die Beacon-Technologie (nicht) brauchen*, http://locationinsider.de/warum-deutsche-haendler-die-beacon-technologie-nicht-brauchen/

interview conducted by Deloitte reveals that so far, this is not regarded as a serious problem by **beacon manufacturers,** as technological improvements are expected.

From the perspective of the **retailers holding consumer data**, a key challenge when implementing technologies such as in-store tracking is to provide for a well-functioning IT-infrastructure and for data security. This was pointed out as a risk by *Tesco* in its Annual Report.[408] While this may be relatively costly especially for smaller businesses, it is a natural precondition for implementing new technologies and dealing with consumer data.

Another potential barrier relates to **competition between retailers**. Due to the openness and simplicity of the information transmitted, all beacon signals require an application and corresponding API in order to process data for consumer use. Technically any app can process the signal received. Retailers could potentially use this fact to stage what Alastair Nash calls a "Beacon war": Users entering store A, while having an App installed by Store B (or any third-party related to store B) might instantly receive a notification when the beacon signal is received. This note could, for example, present offers by retailer B more attractive than those of retailer A. To prevent this, as one **beacon manufacturer** indicated in a phone interview conducted by Deloitte, measures to encrypt the signal by default have become common practice for a number of beacon manufacturers.[409]

Legal barriers

With respect to all business models studied, interviewees and literature highlight that the application of **competition law** could be complex.

For example, on a DG GROW workshop on platforms it was discussed that competition law may not be sufficient to address the relationships between platforms and retailers.[410]

With respect to **in-store tracking**, standards of competition law need to be taken into account in the context of advertisements, including ads sent to consumers via push notification. In this context, the advertisement company usually needs to acquire the consent of the consumer. However, it may not always be clear who is responsible in this context[411], as several parties are involved:

- The app sending the notification;
- The retail store the consumer is in; and
- The Brand the ad is about.

Questions in relation to **data protection law** arise in particular for the providers of software/apps as well as retailers that use their own schemes. For example, a retailer highlight-

[408] Tesco (2016), *Annual Report and Financial Statements 2016*, https://www.tescoplc.com/media/264194/annual-report-2016.pdf

[409] Interview with stakeholders; see also: Orange Digital UK (2014): Beacons – A digital revolution in the making. Orange Digital perspectives, http://www.cs.odu.edu/~cs441/Papers/beyond-003.pdf, p. 10.

[410] See: https://ec.europa.eu/digital-single-market/en/e-commerce-and-online-platforms-workshop-2

[411] Cf: Süßel, A. (2014), *Beacon Kompendium (2/5) – Die rechtliche Fragestellungen*, https://www.mobile-zeitgeist.com/beacon-kompendium-25-die-rechtliche-fragestellungen/

ed that they make a big effort to ensure that all customer data is protected and secure in line with the new GDPR.

In the context of in-store tracking systems, some specific questions may need to be clarified in relation to data protection legislation:

- Is it necessary to inform the user about the use of beacon technology?
- Is it necessary to explain what beacons are?
- Is it necessary to retrieve an explicit consent about the use of beacon technology?

Further questions may arise e.g. when specific interactions take place in a cloud.[412] An interviewed beacon manufacturer indicated that the data protection laws in EU countries are currently ambiguous and differ from country to country. On this basis, it is preferable to transfer the data to clouds where it is stored in the US for processing and analytics.

Another potential barrier relates to the legal standards on new technologies. An interviewed **beacon manufacturer** explained that the laws in relation to some related services, e.g. "Wi-Fi-sniffing" are unclear, preventing the company from becoming active in this field.

Taxation could also be an issue in relation to all business models that involve the storing of data: For example, when data is stored on different servers in different countries data owners need to be careful to be compliant with tax regulations.

Intellectual property rights could be relevant in relation to online platforms. An interviewee explained that currently a lot of data relating to products and prices is freely available. Sites that offer product and price comparisons accumulate this type of data to offer services to consumers. There are only limited possibilities to restrict this, as database law only applies once the data is presented in an aggregated manner. Although this poses challenges to retailers, they accept this.

Finally, a retailer indicated that the **enforcement of relevant legislation** to protect their data does not always work in practice. There were cases in which the databases were hacked, but it was not possible to enforce their rights. This concerns particularly attacks originating in third countries, but in some cases also those originating in EU Member States.

Other barriers

Another challenge in relation to (re-) use of data relates to the **extent to which businesses are aware of the potential of existing data sets**. It was highlighted by the interviewees that – even if individual businesses had better access to data generated via online platforms, third party loyalty programmes or apps, it would not be clear whether they could actually create benefits from the data. For that, businesses need to have an overview of the existing data and understand its potential. Indeed, some retailers are not aware of the potential of data on customer behaviour and analytics. For example, for some retailers, the most important rationale for loyalty programmes appears to be a wish to increase traffic rather than

[412] Süßel, A. (2014), Beacon Kompendium (2/5) – Die rechtliche Fragestellungen, https://www.mobile-zeitgeist.com/beacon-kompendium-25-die-rechtliche-fragestellungen/

an interest in the data.[413] Thus, a retailer indicated that awareness raising among businesses would be an important step to improve data use.

Going one step further, there are still many aspects relating to the success of retailers that are not properly understood yet. For example, the main principle of data use in retail is to observe customers and then deduct what the customers wish and present them targeted advertisement. However, it is not known yet why marketing strategies are successful or not. Marketing response rate is researched to a sufficient extent.

Regarding in-store tracking, an additional barrier relates to the **awareness of consumers**. It is generally challenging for new technologies to make users aware of their added value.[414]

A potential barrier in this context is that, in a typical case, consumers need to give **multiple permissions** before any interaction between apps and in-store beacons is possible. They have to:

- Download the app;
- Enable Bluetooth on their device[415];
- Accept the request to use location based services with the app; and
- Have to consent to receive notifications from the app.[416]

These multiple layers of opt-ins may work as a barrier to the data access and sharing in the present case, as the extra effort may deter customers.[417] Having said that, these opt-in steps may help customers to understand, what is done with their data and who processes it as part of the terms and conditions of the service. In this context, we also note that consumers still appear to be sceptical of in-store tracking.[418]

In this context, **transparency towards the consumers is imperative**.[419] App providers need to implement a transparent opt-in procedure, ensuring that the consumer validly consents to the use of location data. They also need to assure consumers that their personal information is safe. This appears to be followed at least to some extent by some app providers. In the Terms of Sale of one app provider, there is an entire section on data protection (around

[413] McDermott, J. (2014), Shopkick: driving retail in exchange for data, http://digiday.com/platforms/shopkick-raw-deal-retailers/.
[414] Herhausen, D et al. (2015): Integrating Bricks with Clicks: Retailer-Level and Channel-Level Outcomes of Online–Offline Channel Integration, *Journal of Retailing*, Vol. 91, Iss. 2, pp. 309-325
[415] While most smartphones nowadays offer Bluetooth, many users do not activate it, e.g. because they are afraid that it affects the battery usage. In this context, it is necessary to make users aware of the fact that BLE needs less energy compared to regular Bluetooth and of the added-value users have from using these functions.
[416] Orange Digital UK (2014): Beacons – A digital revolution in the making. Orange Digital perspectives, http://www.cs.odu.edu/~cs441/Papers/beyond-003.pdf, p. 10.
[417] Hyunjoo Im and Young Ha (2015): Is this mobile coupon worth my private information?, *Journal of Research in Interactive Marketing*, Vol. 9 Iss 2, pp. 92-109
[418] Moody, M. (2015), *Analysis of promising Beacon technology for consumer*, https://www.elon.edu/docs/e-web/academics/communications/research/vol6no1/06MoodyEJSpring15.pdf
[419] Piotrowicz, W. and Cuthbertson, R. (2014) Introduction to the Special Issue Information Technology in Retail: Toward Omnichannel Retailing, *International Journal of Electronic Commerce,* Vol. 18, Iss. 4, pp. 5-16.

1 ½ pages), explaining in what ways the data is used and referring to data protection legislation. It is, for example, explained what type of data may be collected (including location data) and in what way this data is used. Furthermore, the benefit for consumers must be clear. In this context, app providers must ensure to **deliver an added-value** to retailers and consumers, while at the same time not flooding consumers with push-notifications on ads or similar. If consumers are annoyed by the app, they will most likely stop using it.[420]

Energy sector: British Gas and SAS

Context: The initial situation

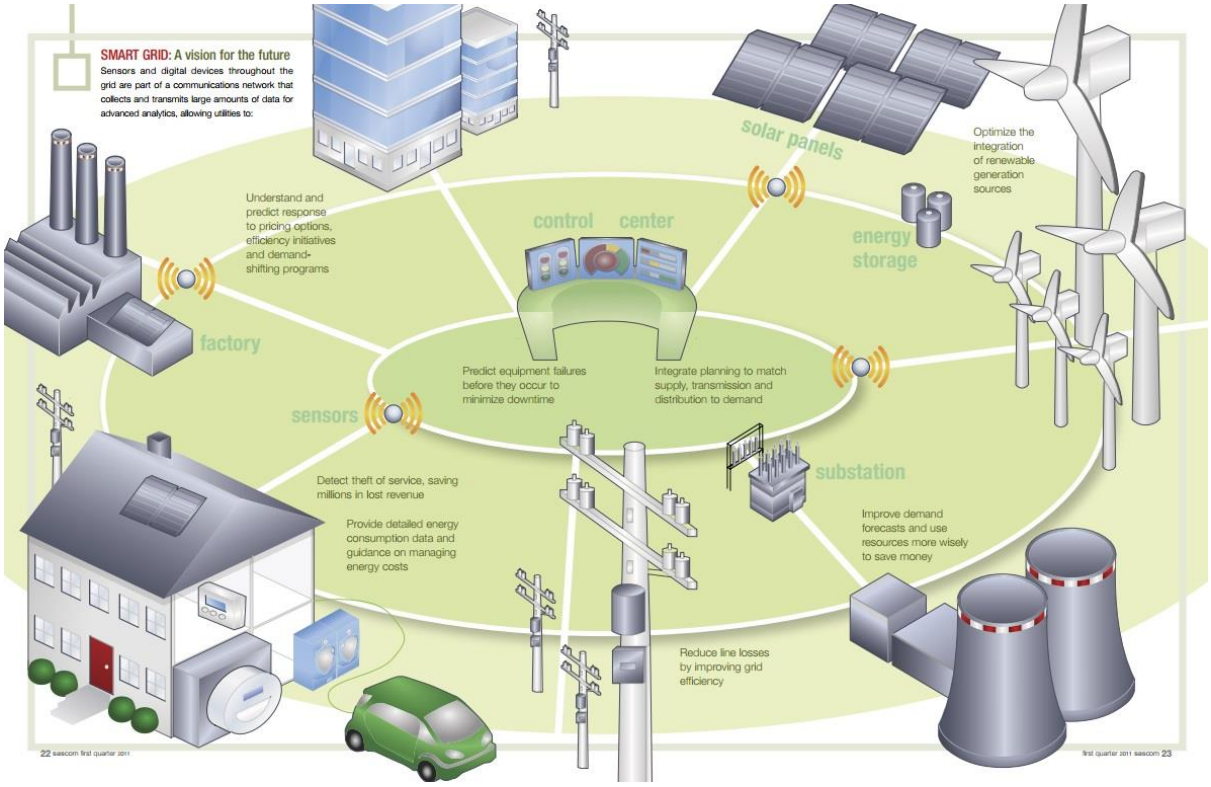
In the area of smart energy, i.e. the combination of the energy sector with sophisticated information and communication technology (ICT), smart homes and the internet of things will create the environment of the future. Smart energy will lay the groundwork for overall monitoring and controlling appliances in response to energy prices. While working independently, electrical appliances can work autonomous and more efficiently. Smart energy is the crucial prerequisite making the transition from fossil fuel and nuclear energy to solar energy and efficient energy as they integrate different forms of energy sources in one ecosystem[421].

In a modern distributed energy management system, energy suppliers use household data to forecast consumption behaviour in order to co-ordinate energy consumption in building blocks, as well as regards the sale and procurement of energy. With dynamic pricing, the entire energy system in smart home networks can be optimised as regards electricity usage. Thus, data storage and data exchange elements are key to this development, and technologically complex systems have to be developed further in accordance with energy management and marketplace systems, respectively. For example, a washing machine might start to work when there is a surplus in energy capacity available and the electricity prices are at its lowest levels.

[420] Süßel, A. (2014), Beacon Kompendium (1/5) – Am Anfang steht die Technik, https://www.mobile-zeitgeist.com/beacon-kompendium-am-anfang-steht-die-technik/ ; Süßel, A. (2014), Beacon Kompendium (2/5) – Die rechtliche Fragestellungen, https://www.mobile-zeitgeist.com/beacon-kompendium-25-die-rechtliche-fragestellungen/

[421] http://www.digitale-technologien.de/DT/Redaktion/EN/Dossiers/smart_home_projekte.html?cms_docId=330170

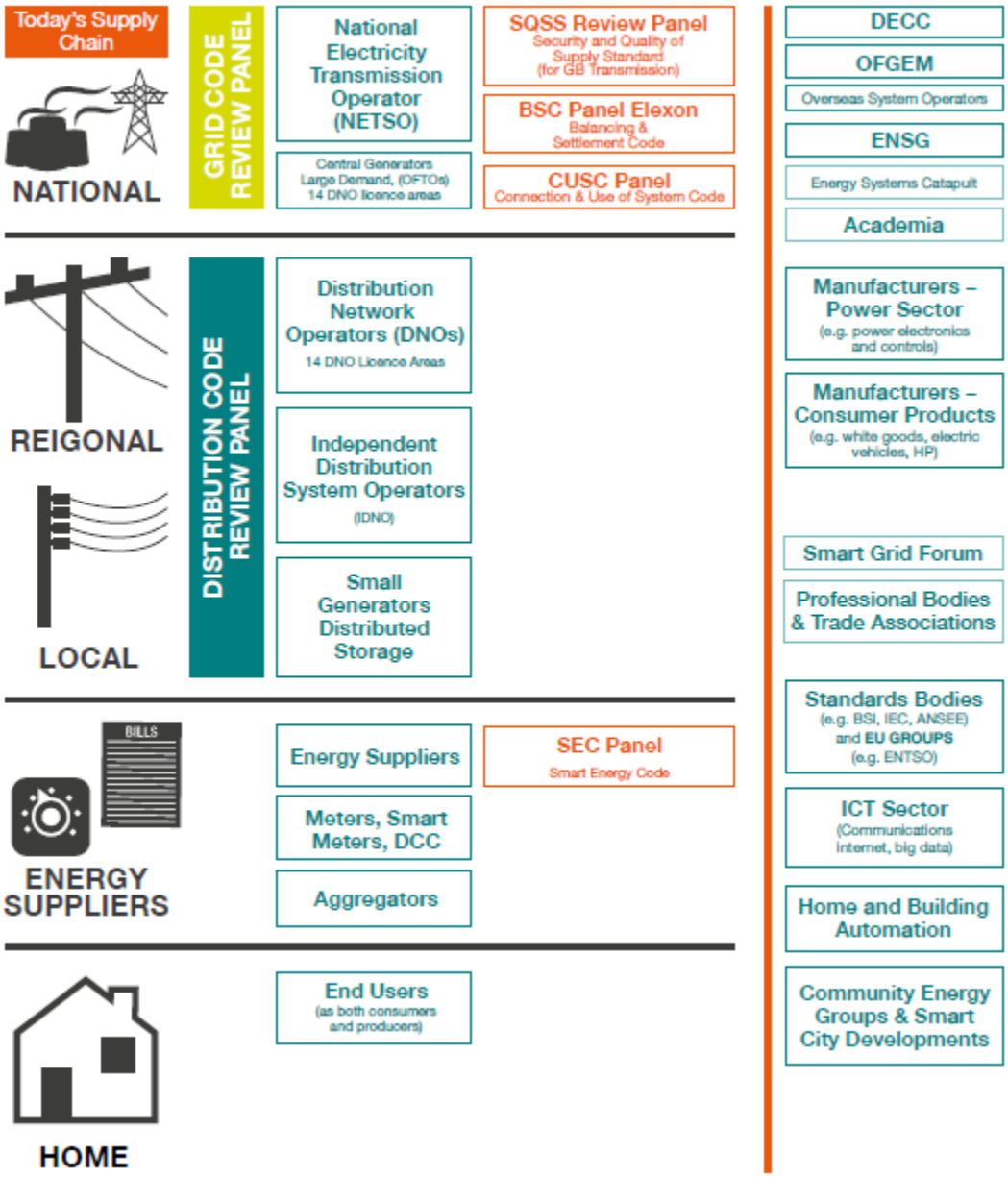
Figure 44: Energy sector Smart Grid and Smart Meter applications



Source: SASCOM Magazine (2011), First Quarter Issue, pp. 22-23.

As the figure above illustrates, smart meter will be the basis for smart grid intelligent energy systems of the near future. Intelligent energy networks connect energy suppliers, the demand side and energy storages enabling the exchange of data (information). From an economic perspective, there is a strong preference to reach a market equilibrium where matching supply and demand more efficiently is likely to reduce the volatility in energy capacities, thus reducing the costs for energy storage. This can only be achieved with real-time processing of energy systems data of millions of energy customers in order to be able to deliver feedback via price information for companies and consumers. The following figure illustrates the different bodies involved in the operation of the UK energy sector.

Figure 45: Different bodies involved in the operation of the energy system



Source: IET (2014), Britain's Power System: The case for a System Architect.

Consequently, these systems place high demands on connectivity, data exchange standards with several stakeholders and also on usability, user friendliness, and consumer data protection. This means new approaches must be developed for building automation and home networking for smart residential or industrial buildings in a flexible way. Many leading companies explore innovative concepts to implement prototypes based on application scenarios or have already introduced their business model. With respect to the energy sector we will focus on the case of British Gas and SAS as we will show how a leading utility is dealing with the challenges and opportunities in the field of smart energy.

Business model and actors

British Gas is a UK-based utility of the energy sector (electricity and gas supplier) being part of the Centrica Group. The main business consists of residential energy supply and services and business energy supply and services to about 15 million homes and businesses across the UK. Moreover, energy supply, services, connected home, distributed energy and energy marketing and sales are in the focus of the current Centrica Group growth strategy, expecting to invest an additional GBP 1.5 billion of operating and capital resources over the next five years.[422]

Table 30: British Gas business areas

Residential energy supply	The supply of gas and electricity to residential customers in the UK
Residential services	Installation, repair and maintenance of domestic central heating, plumbing and drains, gas appliances and kitchen appliances, including the provision of fixed-fee maintenance/breakdown service and insurance contracts in the UK
Business energy supply and services	The supply of gas and electricity and provision of energy-related services to business customers in the UK

Source: Centrica Group (2016), Annual Report 2015, p.36.

In 2015, British Gas realised a turnover of GBP 12.4 billion (GBP 12.9 bn in 2014) with around 28,000 employees. British Gas wants to be at the frontier in finding ways to analyse big data based on systems considered to be 'smart' in terms of generating insights in consumer patterns and business efficiencies. Smart CRM systems in combination with smart meters and smart grids generate huge amounts of data and have the potential for more customer-friendly services and cost-efficient products. Recently, British Gas started to explore how data analytics can process big data from smart meters[423], smart thermostats, smart boilers and different kind of sensors delivering the data via the Internet.

British Gas[424] is putting emphasis on data analytics software from SAS business analytics capable to allow them to track and visualise and finally predict energy usage and consumption behaviour. In this context, British Gas' activities cover the following steps of the data value chain:

[422] Centrica Group. 2016. Annual Report 2015.

[423] https://www.britishgas.co.uk/content/dam/british-gas/documents/smart-metering-customer-guide.pdf?cid=dplkcstgde

[424] Latest activities and achievements in the British Gas business unit "Connected Home" according to the Centrica Group Annual Report 2015: Acquisition of AlertMe in March 2015; sold over 300,000 smart thermostats in the UK; launched the next generation of the app "Hive Active"; sold nearly 200,000 smart thermostats in North America; launch Hive products outside of the UK and Ireland in 2016; launched a range of new connected home products (i.e. Hive Active Plug, Hive) in the UK in early 2016; launch Window or Door sensor and Hive Motion Sensor.

Figure 46: Data Value Chain

Source: Deloitte

As regards data generation, British Gas is using data sources such as their own gas and electricity meter readings, digital thermostat temperature data, connected boiler data[425], real-time energy consumption data, data from motion sensors, window sensors and door sensors. With respect to data transfer and data storage they have a partnership with Amazon Web Services providing a cloud solution that works as a scalable data platform also enabling data-based product and service differentiation over time.[426] When it comes to data processing and data analytics, they are using SAS analytics[427] and predictive analytics solutions, as well as an enterprise data warehouse (EDW)[428] along with machine learning which is applied to meter data. Data services need an access device connected to the router and allow for example for real-time mobile alerts. They are provided via apps developed by British Gas such as 'My Energy Live', 'Hive', 'Hive Active' and 'Hive Active Plug'.

British Gas is applying data science, data analytics and data engineering within its connected homes business unit. [429] The so-called insight & data team's activities comprise of techniques from market research, data standards, customer analytics, marketing optimisation and data strategy.[430] Within the steps of the data value chain the following software solutions, amongst others, are being used: [431]

[425] In March 2016, British Gas has launched a new boiler technology that can diagnose heating problems before they happen, allowing an engineer to fix them before residents wake up to a cold house or the shock of a cold shower. Boiler IQ is a small device that monitors the customers boiler using built-in sensors and sends diagnostic information to British Gas over the internet. If a fault is detected, a a text will be sent and prompted to book a visit from an engineer. In order to connect to the internet, Boiler IQ works with the Hive Hub, a small hub that connects to to the router and allows to control the heating and hot water from a smartphone. See http://home.bt.com/tech-gadgets/tech-news/british-gas-boiler-iq-heating-technology-detects-faults-alerts-homeowner-11364046062453

[426] http://de.slideshare.net/AmazonWebServices/british-gas-hive-scaling-for-the-connected-home

[427] http://www.sas.com/ro_ro/news/press-releases/2014/march/british-gas-analytics.html

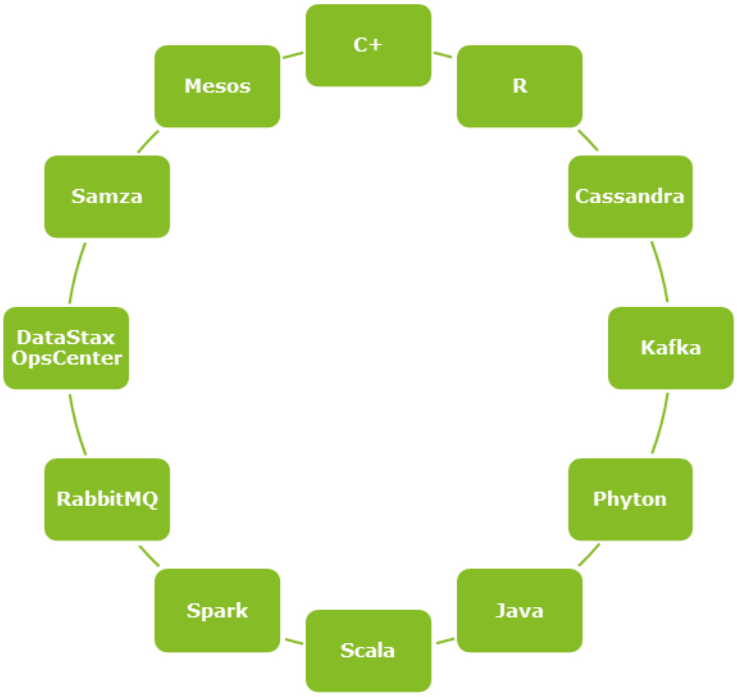
[428] Forrester Research. 2015. The Forrester Wave: Enterprise Data warehouse, Q4 2015, Cambridge, USA.

[429] See British Gas SlideShare, slide 13: http://de.slideshare.net/planetcassandra/bgch-cassandra-talk231014

[430] See British Gas website for more information with respect to the organisational structure, etc.

[431] See British Gas SlideShare, slide 13: http://de.slideshare.net/planetcassandra/bgch-cassandra-talk231014

Figure 47: Big Data Software solutions applied by British Gas



Source: Deloitte

After the data collection processes, the data (information) will be analysed. According to an article by Martin Courtney, "*all the information being analysed follows a standard pattern. Raw data is collected from the smart meter, on-grid sensor, industrial device, database, collecting point, or other asset before being transmitted over some form of telecommunications, radio-frequency identification (RFID) or wired/wireless network for ingestion onto a server or dedicated appliance which has the sole job of cleansing it–a job customarily performed in giant data warehouses, but now speeded-up significantly using Apache Hadoop clusters and/or in-memory databases (those that store data in some form of RAM rather than hard-disk) for example. After being cleansed of 'dirty' data-duplicate or incomplete records–the remaining information is sent, sometimes via the data warehouse, to the analytics engine, which runs a series of algorithms, the so-called 'secret sauce' designed to transform it into meaningful insight which can be deemed of some use to the business, and which can then be presented within third-party reporting or visualisation software*."[432]

In addition to the in-house integrated value chain they also cooperate with AWS Cloud as data platform provider, i.e. for the Hive app. Moreover, SAS solutions are used in the data analytics processes. According to SAS business analytics, the solutions implemented for British Gas are the following: [433]

- SAS Marketing analytic solutions: Offer the processes and technologies that allow marketers to plan, coordinate and evaluate the success of their marketing initiatives. By

[432] Courtney, M. 2014. How utilities are profiting from Big Data analytics. E&T Magazine 9(1).
[433] http://www.sas.com/ro_ro/news/press-releases/2014/march/british-gas-analytics.html

putting data in the hands of business users, marketing programs become more effective and the organisation more efficient in execution.

- SAS Visual Analytics: Enables organisations to easily map out and understand analytic insights and share those with employees and customers across the business. It delivers rapid in-memory analysis for quicker analysis, and interactive dashboards for reporting in-depth data visualisation.

Finally, BritishGas is cooperating with AMT-SYBEX, a company part of Capita Plc, using their Affinity Marketflow Solution (formerly DTS) to link with all other participants in the UK energy retail market.[434] According to AMT-SYBEX, "*the UK energy retail market requires participants to be able to gain and lose customers. The mechanism which enables this requires participants to manage in excess of 20 million complex data flows per annum for both electricity and gas. British Gas decided that they require a strategic data flow management tool to marshal all their industry related data flows for their residential, business and metering operations. Providing a significantly higher level of control of their data flows has enabled British Gas to gain increased end-to-end control of their business processes. In addition the solution provides significant reporting capability against data flows providing a series of KPI's to assist internal and agent management*."

AMT-SYBEX is offering their network data management product to all energy suppliers and thus enables demand forecasting, energy optimisation and commercial service scheduling capabilities based on their customers' data (energy suppliers and their customers), as well as other data. The solution "Affinity Networkflow"[435], a scheduling and optimisation platform, is using demand forecasting results and is fed by data from the wholesale energy market, forecasted wind speed and temperature, sunrise and sunset times, as well as historical demand data and already existing forecast data from energy suppliers. The company is able to manage the communication with, and storage of result data from smart meters or other operational data sources of energy suppliers (i.e. collection, validation, management, and dissemination of readings and events).

Among others, the network data management product is able to determine[436]

- Network capacity
- Future demand
- Optimisation of commercial services schedules that can be met with available resources
- Cost effective charge and discharge strategies.

Via a user interface, all scheduled services, optimised battery energy levels, demand forecasting, historical energy demand and service information can be viewed, admission is lim-

[434] http://www.amt-sybex.com/case-studies/british-gas/
[435] The platform has been selected for meter data management by ScottishPower and British Gas for their UK Smart Meter roll-outs, http://www.amt-sybex.com/energy-storage-why-networkflow/.
[436] http://www.amt-sybex.com/energy-storage-the-product/

ited to the registered customers, i.e. the energy suppliers like British Gas. AMT-SYBEX is not offering data from this business relations to third parties.

AMT-SYBEX claims to be the "only network energy storage optimisation system tested and working at scale in Europe and is currently the only fully localised stacked service offering in the UK"[437] Their database is able to manage portfolio of smart meter data of up to 10m customers[438] simultaneously and is further scalable. End to end processing for 10 million meter points is less than 36 minutes, metres can be half-hourly read and data processed and stored accordingly.[439] In this highly automated environment the data sharing between customers (energy providers and their customers' meters) and service providers (AMT-SYBEX, but also third-party service providers like e.g. connected home product providers) is crucial.

Service example: Intelligent energy management systems

The example intelligent energy management system IEMSy[440] is a data system to manage and optimise utility consumptions' in cities and municipalities for costs reduction, energy saving and climate impact reduction in Portugal and other European countries.[441]

The intelligent energy management system allows energy users to manage, generate, view and print performance reports, including:

- Characterization of buildings and equipment
- Use of energy and water resources
- Management of energy production and waste
- Consumption history
- Energy costs.

IEMSY application areas include public buildings, water and energy supply, grid transformers, waste collection, etc.

In early 2017, for example, 154 cities and municipalities were using IEMSy. 586 699 electronic invoices were issued, 10 491 buildings were managed and 3 325 vehicles. The total invoiced volume summed up to 206 263 936 € and the total energy managed to 1 656 212 390 kWh.[442]

[437] http://www.amt-sybex.com/energy-storage-why-networkflow/

[438] For comparison, there were 27.0 million households and 2.45 million enterprises in the UK in 2015 (Office of National Statistics UK).l

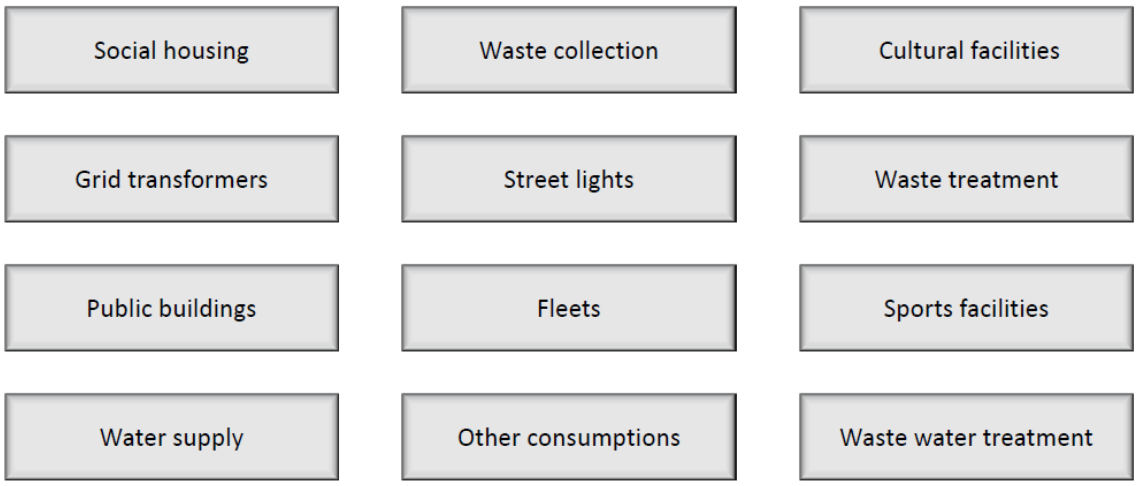
[439] http://www.amt-sybex.com/case-studies/affinity-meterflow-benchmark/#sthash.ARyBvD2O.dpuf

[440] Information for this chapter is gathered from interviews, website and the IoT Workshop Brussels, June 6th, 2017.

[441] The example was presented by Paula Peiró, Rui Pedro Henriques, Marcos Nogueira, IrRADIARE, Science for Evolution in Brussels, June 6th, 2017, during the IoT Workshop in the course of this study.

[442] See presentation "The transformative effect of access and re-use of data for smart industries - IEMSy's Case", Paula Peiró, Rui Pedro Henriques, Marcos Nogueira, IrRADIARE, Science for Evolution in Brussels, June 6th, 2017, slide presentation.

Figure 48: IEMSY application areas



Source: IrRADIARE

Data is generated and (re-)used from the field of utilities (mostly energy); public sector's consumption (local public authorities). Added value data is generated from additional knowledge extracted from invoices and consumption profiles. Other information needed is gathered from data about premises, geography, as well as buildings and vehicles utilization.

Data is collected by the smart metering provider (high sampling metering of energy consumption, minimum every 15 minutes, (typically energy or other utility distributor). Data is, then, gathered and shared by the utility provider with the consumer or with entities acting on the behalf of the utility provider. Third party data analysts may operate on behalf of the consumer.

Open data of energy and utilities consumption forms the basis of innovative energy services. The company names difficulties and obstacles for innovation especially in the field of standardization (absence of common (standardized) data schema). Another difficulty for further data innovations lies in the lack of best practices for data owner (i.e. the energy consumer) attribution of data utilization rights and in missing open data best practice enforced in the public sector. To foster a European single market for data driven innovation in utilities, the company calls for[443]

- Standardized data schemes throughout the energy sector
- Data access authorization mechanism regulated at European level on basis of best practices, considering consent of data owner balanced with data security and privacy protection issues
- Enforcement of open access to public sector utility consumptions

[443] See presentation "The transformative effect of access and re-use of data for smart industries - IEMSy's Case", Paula Peiró, Rui Pedro Henriques, Marcos Nogueira, IrRADIARE, Science for Evolution in Brussels, June 6th, 2017, slide presentation.

As experts do not expect standardization emerging from the energy market, they plea for market driven standards to established per sector.

Service example: Energy management and prediction provider

Since 2004, Energy & meteo systems[444] (established from a university project) is working as an international energy management and prediction provider. The German SME offers power predictions and a "Virtual Power Plant", contributing to the efficiency of integrating renewable energies into power grids and energy markets. The company claims to predict approximately 25% of the world-wide installed wind energy power. It also offers predictions for solar power, combined with a projection of the current power supply. Their services are based on different data from the energy markets, weather forecasts, and energy exchanges. Data access and re-use is based on private contracts with private companies and public authorities (e.g. Meteorological services). Protection of sensitive customer information (i.e. of energy providers) is self-evident. The company is not active in the private consumer market (smart meters) as there seems to be no willingness to pay for such services at the consumer side today.

In their "Virtual Power Plant", the company integrates fluctuating, decentralized power sources into the energy grid and provide customers with energy exchange information. Customers are grid operators and power traders from Europe, America, Asia, Africa and Australia.

The company established the first intelligent wind farm for Statkraft (Norway) in Germany in 2012 and participated in the 2016 balancing energy market using their product Virtual Power Plant and their own developed power prediction tools. Statkraft is Europe's largest generator of renewable energy.

With the help of Energy & meteo systems generated, processed and analysed data, Statkraft´s pilot wind farm was the first one directly marketed and continuously remotely regulated. Real-time information on its electricity production is collected and power generation can be adjusted according to market demands, simultaneously matching predictions. Thus, wind energy can be efficiently marketed.

The company stresses that only high-quality, precise, real-time data allows for flexible and demand-oriented products and services. From the view of service providers like Meteo regulation on requirements for energy providers to offer real-time data as a service to third parties is essential. This would lead to enhanced service quality and innovations.

Another example of Energy & meteo systems activities is "ORKA 2 – Optimisation of Ensemble Forecasts with Regenerative Inputs for Short-term Forecasts applied to the Example of Grid Security Calculations and Current Carrying Capacity Forecasts".[445] The company is working with the German Weather Service (DWD) and the network operators 50Hertz Transmis-

[444] Information used in this chapter is generated from expert interviews and website information https://www.energymeteo.com/about_us/company.php

[445] https://www.energymeteo.com/projects/orka_2.php

sion GmbH (transmission grid) and TEN Thüringer Energienetze (distribution grid) to improve network node predictions and the integration of forecasts into grid operations.

The nexus between data ownership, access to and (re-) use of data and data portability

In view of the above mentioned services and considering also the discussions about consumer profiles revealed by smart meter data the question of data ownership, access to and (re-) use of data and data portability are of major importance. Overall, the sensibility of consumer protection authorities towards the topic could be expected to be very pronounced but this is only the case in some countries of the EU, e.g. in Germany.[446] This results not just from the sheer increase in data volumes being retained by individual suppliers but also the need for interaction between different data types and sources. Data portability, i.e. the ability to (re-) use data across interoperable applications, is of major importance from the users` view. Only if generated energy data can be used for applications by different service providers the consumer is able to switch between service offers. Thus data portability is a concept to avoid lock-in effects. The common technical standards in the UK energy system which are required by law facilitate the transfer from one energy supplier to another and from one additional service offer (e.g. smart home service supplier) to another. Market mechanisms alone would not incentivise energy suppliers enough to develop machine-readable and interoperable data formats.

Experts on EU level like ENISA (European Union Agency for Network and Information Security)[447] also dealt with the question of data protection and IT-security in smart metering and opted for a concept of smart grid chain of trust. Countries that already roll-out smart metering like UK and Germany have been following these guidelines in principle.[448]

In the UK the issue of data protection and IT-security is widely acknowledged but not discussed at a prominent level. There is a large range of FAQ sites and consumer websites on the topic.[449] Apparently the main issues have been solved before the nationwide roll-out to

[446] See websites of privacy activists like https://www.datenschutzbeauftragter-info.de/smart-grid-zertifizierung-schutz-fuer-intelligente-stromnetze/ or the Data protection authority association (Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Düsseldorfer Kreis) (2012): Orientierungshilfe datenschutzgerechtes Smart Metering.

[447] ENISA (2014): Smart Grid Security Certification in Europe, The report describes the need for harmonised European smart grid certification practices which cover the complete smart grid supply chain and take trust in the solutions by more data protection and security into consideration.

[448] According to sector experts, the Netherlands had to postpone their roll-out of smart meters because of consumer concerns. They now refer to the UK case as a blue print for data protection and privacy in this field.

[449] Consumer protection authority Citizens Advice https://www.citizensadvice.org.uk/consumer/energy/energy-supply/, supplier British Gas https://www.britishgas.co.uk/smarter-living/control-energy/smart-meters/story-behind-the-smart-revolution.html, regulation authority Ofgem https://www.ofgem.gov.uk/information-consumers/domestic-consumers/making-enquiry-or-complaint; Smart Energy GB information website https://www.smartenergygb.org/en/the-bigger-picture/about-the-rollout.

the satisfaction of the consumer ("consumer as the data owner"). Consumer authorities claim to work on defending the existing rules rather than demand revisions.

The overall data protection law[450] serves as a blanket regulation for the use of smart meter data. Special regulations are laid down in the smart metering Data Access and Privacy Framework which regulate the license contents for energy suppliers[451]. Main features include

- Energy suppliers are always liable concerning the right use of customer data which is laid down in the general license conditions. In the UK the terms and conditions of energy suppliers must comply with regulation. If a supplier changes the variety of data read or the allowed frequency of readings by their terms & conditions they breach their license conditions and are answerable to the regulator Ofgem.[452]
- Customers (business and private) are the owners of their data and may decide how often their data is processed to the energy supplier. By default, data will be sent one time a day. There are opt-in options for e.g. monthly readings or readings every 30 minutes up to real-time readings. However, a complete opt-out is possible, too. The energy supplier (or another service provider who has a contractual relationship with the energy user) may use the data of the smart meter readings for billing and in aggregated anonymised form for analytics.
- The data can be read by the consumer as well and technically "stays" in the LAN (local area network) of the home. The consumer i.e. the owner of the data can decide whether to use smart home applications from other providers, also from outside the UK (e.g. Apple, Google) and allow them to read their meter. However, by default, only the energy supplier may (re-) use the data. Suppliers will also not be able to use energy consumption data for marketing purposes unless they have explicit consent[453].

Experts do not expect major protests against the nationwide roll-out of smart metering for the future.[454] This seems especially due to the fact that

- Data protection and security issues are clearly addressed on the level of terms & conditions between business and private customers and their energy suppliers (customers have to agree to data transfer to third parties)[455]

[450] Data protection act, http://www.legislation.gov.uk/ukpga/1998/29/contents.

[451] For details see Modification to the standard conditions of electricity and gas supply licenses, electricity distribution licenses and gas transporter licenses (smart meters), https://www.gov.uk/government/publications/smart-metering-licence-conditions-for-consumer-engagement-strategy-data-access-and-privacy-monitoring-and-evaluation-and-security-risk-assessments-and-audits-in-the-period-before-the-dcc-provides-services.

[452] Office of Gas and Electricity Markets, https://www.ofgem.gov.uk/

[453] There is data shared or sold through platforms such as AMT Sybex or AWS. They serve as a mere subcontractor for a specific service and are bound by contractual agreements with British Gas (or other service providers).

[454] For a brief description of the roll-out see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/236488/Non_Domestic_Leaflet_v_02.pdf

- The benefit of data analysis in smart metering and smart grids relies on vast amounts of automatically generated data, i.e. “big data” gathered by all stakeholders in the supply chain (the more data is collected, stored and processed the more reliable the overall system becomes and the more beneficial the results are both for service providers and for consumers). Smart metering achieves a win-win situation for consumers and suppliers.
- The data is highly aggregated and anonymised. Personalised data is only used for billing purposes and as a tool for the respective customer to control energy expenditures. This means, AMT-SYBEX is only a service provider of British Gas and subject to own limits determined by the British Gas license.
- Anonymised data can be used for analysis, also for research.
- Within the network, data is encrypted and telecommunications service provider cannot access them. Every energy supplier is using their own data base. Companies like AMT-SYBEX are only a service provider bound to contracts with the energy supplier. They do not use or (re-) use data without explicit permission (given via contractual clauses).

There is no doubt that these new digital services provide marketing and sales statistics for British Gas on customer profiles, pricing behaviour, sensitivity to special deals allowing for a new era of individualised product and service provision and optimisation, as well as faster response-rates as regards changes in usage patterns, etc. but today we could not find any significant attempt to stop the process because of privacy or liability issues.

The corresponding big data applications in the energy sector aim at: [456]

- Helping to transform utilities into smart data-driven companies.
- Laying the foundation for the next generation of smart energy generation, distribution and consumption.
- Adding new devices to smart grids and enabling the re-invention of the core business of utilities.
- Allowing data analytics software to track, visualise and predict smart grid operations, as well as electricity consumption behaviour.

When it comes to smart meter, they collect information about how much gas and electricity is used, but do not store other personal information that could identify the customer, such as the name, address or bank account. All information about energy usage is strongly protected. Therefore, private and business consumers accept the terms & conditions of British

[455] For British Gas T&C see https://www.britishgas.co.uk/products-and-services/gas-and-electricity/our-energy-tariffs/standard/terms.html. Clause 14 addresses data transfer: “You allow us to collect information from your smart meter for as long as we supply your gas or electricity. We'll only use the information from your smart meter to do certain things (for example, to send you a bill or take part in a government-approved trial) or for other reasons we’ve listed in clause 10. We won’t use it to sell you products or services from British Gas or our partners, unless you've given us permission to do so.” Clause 10 further refers to how data is given to third-parties (service providers of British Gas) to perform smart meter services.

[456] http://www.power-technology.com/features/feature-smart-thinking-big-data-energy-industry/

Gas which are based on the license by Ofgem and the implications for the storage and processing of energy data. British Gas will only use aggregated data for statistics and will only use it in ways complying with the licences. In this context, AMT-SYBEX is only a service provider to British Gas, bound to contractual clauses not to use any data for own business purposes.

The law, which is explained in the UK Energy Data guide for smart meters[457], puts strict controls on consumer data, data access and data sharing issues.[458] This means that companies can forward and use their customer's data only anonymised. For analysing smart meter data by AMT-SYBEX algorithms and for forecasting demand and the according service offerings this method seems sufficient. In principle, any service provider can approach the consumer directly with service offers and ask to access meter readings for special purposes. This limits complaints about the existing regulations within the industry.

The UK Energy Data guide for smart meters[459] explains the handling of data which helps building trust and user acceptance: "*it's your data – you choose what you want to do with it and you can change your mind about how much you share, and how often, at any time. So, you can choose:*

- *how often your smart meter sends data to your gas and electricity supplier (monthly is minimum, daily or half-hourly are optional)*
- *whether to share data about your energy use with other organisations, like price comparison sites*
- *if your supplier can use your meter readings for sales and marketing purposes*"

The so-called Data Communications Company (DCC), which organises the overall roll-out functions as another supervisor who "*provides the communications infrastructure that handles smart meter data. They make sure smart meters send the right information to ensure bills are accurate. They are regulated by Ofgem and will not themselves store any customer data*"[460], i.e. they run the Smart Metering Wide Area Network (WAN) for sending messages between energy suppliers and smart meters via the telecommunication network run by Arqiva and Telefonica but they are not involved in data processing solutions. As already mentioned customers have control over the data in their respective LAN and decide which and when data is shared.

Overall, the customer is the owner of the data and will decide whether to share it with the energy supplier (British Gas). The energy supplier is bound by the license to share the data only for defined purposes laid down in the T&C. The most important issue is that of access to

[457] http://www.energy-uk.org.uk/policy/smart-meters.html
[458] The energy regulator also issued a consultation in 2014 (Ofgem consultation: Extending the existing smart meter framework for data access and privacy to Smart-Type Meters and Advanced Meters).
[459] The guide (June 2013) has been developed and agreed between Energy UK, its members, and Consumer Futures (now transferred to Citizens Advice).
[460] https://www.smartenergygb.org/en/the-bigger-picture/about-the-rollout/roles-and-responsibilities/data-communications-company#sid

the added value generated through analytics and the (re-) use of data which is given to British Gas and partly to consumers.

Access to and (re-) use of data is ensured by an interoperable open application programming interface (API) for users of connected home products and services and they may be given access by the consumer on basis of a contract to receive the data of energy consumption and behaviour in real-time. This API solution also guarantees data interoperability.

Potential contractual barriers

- Consumer is owner of the data, but in practice mixture of data ownership between energy suppliers and service providers' services and customers: by signing the T&C customers agree to the transfer of anonymised data without limits, transfer of personal data is limited to British Gas.
- Access to data given to British Gas and partly to consumers: personalised data is only accessed by British Gas for billing purposes and by the respective consumer for using service offerings (information on energy consumption etc.). All parties involved (British Gas, their customers, third-party service providers) may use aggregated data for forecasting and planning.
- (re-) use of data: anonymised data can be (re-) used by third parties that have a contract with British Gas, e.g. AMT-SYBEX for forecasting solutions and contributions to government projects (e.g. in the field of smart grid).
- Suppliers of connected home products: British Gas is allowed (on basis of T&C) to transfer data to suppliers of connected home products so that they can offer their services to consumers. Consumers decide whether they close a contract with the connected home service provider.
- Energy consumers (real-time consumption data): via a user interfaces consumers can access their data (e.g. historical energy demand and service information).
- Data may not be used by third-parties without prior consent: if the data contains address information or similar personal information prior consent is required. Highly aggregated and anonymised data may be used for business purposes.
- Risk and liability: British Gas holds responsible as the company is the license holder. This means for example to be liable for any issues concerning the processing or use of data or for faults in a meter or fittings unless the customer has provided his own meter. The customer has to take reasonable care to make sure that the meter becomes not damaged or interfered with. They have to pay for repairs. Customers have to report any irregularities as regards the smart meter immediately. Liabilities concerning their respective service solutions are with the service providers offering data storage, transfer, or processing (liability based on contracts).

Potential non-contractual barriers

- **Technical interoperability** remains to be an issue, prevented by different technical subsystems of the energy system (not always possible to merge all kinds of data): the issue of technical interoperability is addressed by working groups on national level and international level. From our point of view, on UK level the interoperability of the

smart meter roll-out seems to be a minor problem today as the nationwide project already reached a very advanced state.[461] That is partly due to the fact that the government centralised the organisation of the roll-out at Ofgem (till March 2011) and later at the Department for Energy and Climate Change (DECC) which is directly responsible for managing the implementation of the smart meter programme. Technical interoperability is a pre-condition for data portability, i.e. the transfer of data from one service provider to another.

- **Cost aspects:** In the field of smart energy solutions several providers of information on solar and wind energy supply are entering the market successfully. Their business model is to compile electricity supply and demand data for companies who deal with electricity at electricity capacity auctions. A core prerequisite for their service is weather data and input data from customers (energy suppliers) on their wind parks or solar plants. Weather data is provided mainly by national/scientific meteorological service institutions which are often (partly) publicly funded. Tariff systems differ from organisation to organisation. Some offer services free of charge (e.g. US) but most charge per data unit and offer bulk tariffs or flat rates for heavy users (e.g. Germany, UK, Netherlands etc.). Input costs for service providers differ accordingly. A world leading service supplier of renewable energy supply forecasts puts the costs comparatively low compared to personnel costs and IT costs. Skilled personnel is acquired mainly from universities and has to be trained regularly. In addition, the company emphasized in one of our expert interviews the need for high quality data and is willing to pay a higher price for pre-checked data because they save on costs related to preparation. Free data is frequently not offered in a sufficient quality. Another cost factor is compliance with smart energy regulation but this is considered a burden other companies face in their sectors, too. Contract management and legal advice for drafting contracts with customers form a key activity. Standard setting and developing are a core business activity as well and help to maintain market leadership in power supply forecast services. Costs related to legal uncertainty are negligible because raw data in the energy sector is non-critical in terms of security or privacy.

As already mentioned, this example is based on data services for business customers. A market for private consumer energy data has not really emerged yet and experts do not expect this to happen soon. The reason for this is the lack of the willingness to pay on the side of the private consumers who expect only minor savings. Their electricity bills already are comparatively low and form not a major expenditure in a private household. This is why companies already active in the field of smart energy for businesses do not engage in the smart meter solution market. Costs for legal advice or opportunity costs based on existing policies are not relevant. In fact, private consumer data is available for every service provider who is

[461] Rolling out 53 million gas and electricity meters to all homes and small businesses in Great Britain by the end of 2020, most households will use a smart meter. 233,300 gas and 306,800 electricity meters were installed by the large energy suppliers in the first quarter of 2016 (Department of Energy & Climate Change, Smart Meters, Quarterly Report to end March 2016, Great Britain)

accepted by the private customer and smart meter APIs have been standardised in most European countries.

Access and (re-) use of data: Boundaries and mitigation actions

Technical standards as regards the systems energy suppliers use can differ between countries and regions.[462] Energy providers need to put effort into making barrier-free flow of data work in the European Union to realise smart grid technologies and they have to offer open APIs to smart meters for value-added services. In UK, access for service providers to smart meters is already put into practice. If service providers for home automation approach customers with their services from outside their country they can decide if they want to accept their T&C.

Difficulties currently arise within an energy system consisting of technical subsystems. It is not always possible for energy suppliers to merge all kind of data, i.e. there is a lack of opportunities to link data gathered about the consumers, including where they are located, which problems they have with energy services they use, etc. These problems are addressed on an operational level within the roll-out programmes.

Moreover, there are limitations as regards the access to and (re-) use of energy suppliers' data within the European Union. The privacy of the data must be ensured by digital service providers, i.e. data may not be used for aggregation and third-party usage without prior consent of the consumer. To mitigate this challenge, the digital software provider may provide different types of services to its clients. Giving consent to data aggregation and usage of digital services offered to third parties is done by the energy suppliers through accepting the software providers terms and conditions passed on to consumers. Thus, it is crucial to establish transparency for the consumers with respect to the data processes and what the software provider does with the data.

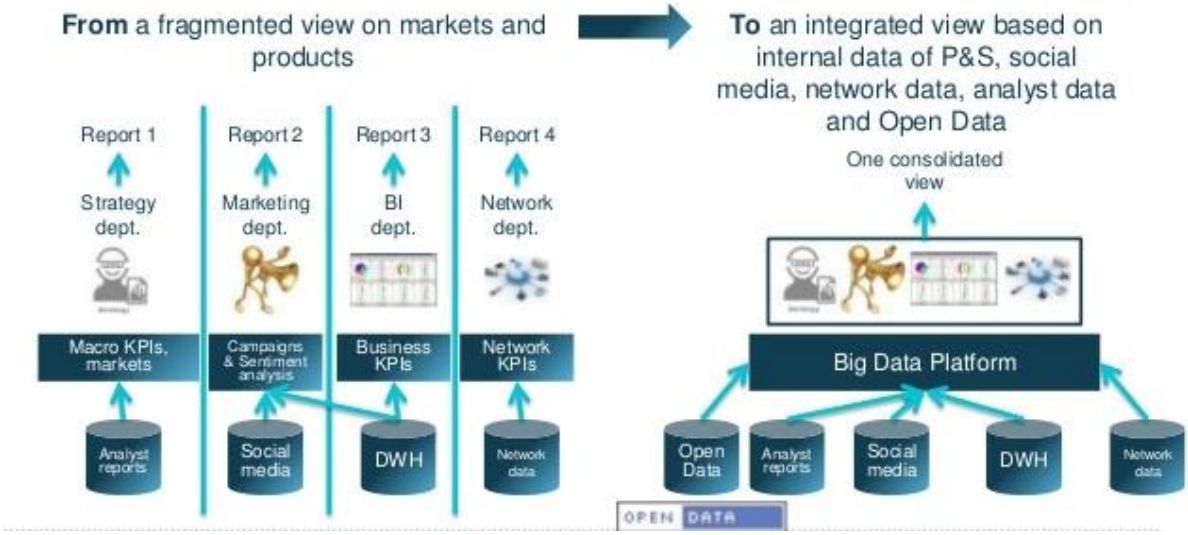
[462]Nationaler IT-Gipfel. 2015. Stakeholder Peer Review – Deutschland intelligent vernetzt: Status- und Fortschrittsbericht.

Telecommunication: Orange and Telefonica

Context: The initial situation

About 15 years ago, telephony services were the main source of revenue for fixed and mobile telecommunication operators such as Orange Telecom and Telefonica. This situation has progressively changed to broadband services as the main source of revenues for fixed line operators and the same phenomenon is taking place in mobile. Today, as telecommunication operators launch new services, they maintain the existing ones in their commercial plans (commoditisation of previous features) while also offering more and more complementary and sometimes innovative services such as content delivery networks, cloud computing capacities and big data technology solutions. As telecommunication providers process massive volumes of data in the course of their network operations, they have large-scale solutions for data management and experience in mobilising significant resources. Thus, providing data hosting, storing and processing services by acting as a multi-industry data hub across various industries, telecom operators such as Orange Telecom and Telefonica can play a crucial role in managing the free exchange of data in Europe in Europe.

Figure 49 : Data and the telecommunications sector



Source: Telefonica. http://image.slidesharecdn.com/benjamins-tefdig-bigdatav1-130924162654-phpapp02/95/big-data-from-hype-to-reality-7-638.jpg?cb=1380041316

As the figure above illustrates, telecommunication operators currently make the step from a fragmented view on markets and products to an integrated view on data-based businesses. Telecommunication systems place high demands on connectivity, data exchange standards, consumer protection (transparency and privacy concerns), data protection (personal data), data security (non-personal data) and usability when it comes to business clients. Because of natural monopoly characteristics such as the subadditivity of the cost function resulting from the telecommunications infrastructure, there is a sector-specific regulation of this network sector in place monitoring and regulating the activities of the leading incumbent in most member states. Because there is currently an EU review process of the relevant directives concerning the electronic communications regulation framework and because of the above

mentioned shift from a fragmented to an integrated view of the telecommunication providers, new approaches must be developed for networking opportunities as regards the data sharing and accessing in Europe. Many leading telecommunications companies explore innovative concepts based on application scenarios or have introduced business models such as over-the-top services. We will focus on the cases of Orange Telecom and Telefonica as we will show how these telecommunication utilities are dealing with the challenges and opportunities that lie ahead.

Business models and actors

The added value in telecommunications basically results from two models of value creation. The first model increases efficiency and optimises business processes of telecommunication providers internally, such that the performance of the telecommunications infrastructure is increased significantly due to more and better information resulting in high quality standards. The second model of value creation is about optimising value creation processes for business clients in order to increase positive externalities.

Analytics solutions, intelligent algorithms, machine learning and artificial intelligence are dynamic and require a real-time free flow of data. These innovative areas can be supported by telecommunication operators. For example, mapping services can be supported in creating user profiles by identifying movement patterns based on geo data, i.e. Mobility Insights of Telefonica[463]. This particular service enables them to leverage their data on consumer behaviour, properly anonymised and aggregated, in order to deliver value added services on mobility to traffic agencies, retailers and other companies interested in this data. In such cases, benefits from the free flow of data are based on more and better information as regards requirement planning and controlling as well as opening the playing field for innovative business models.

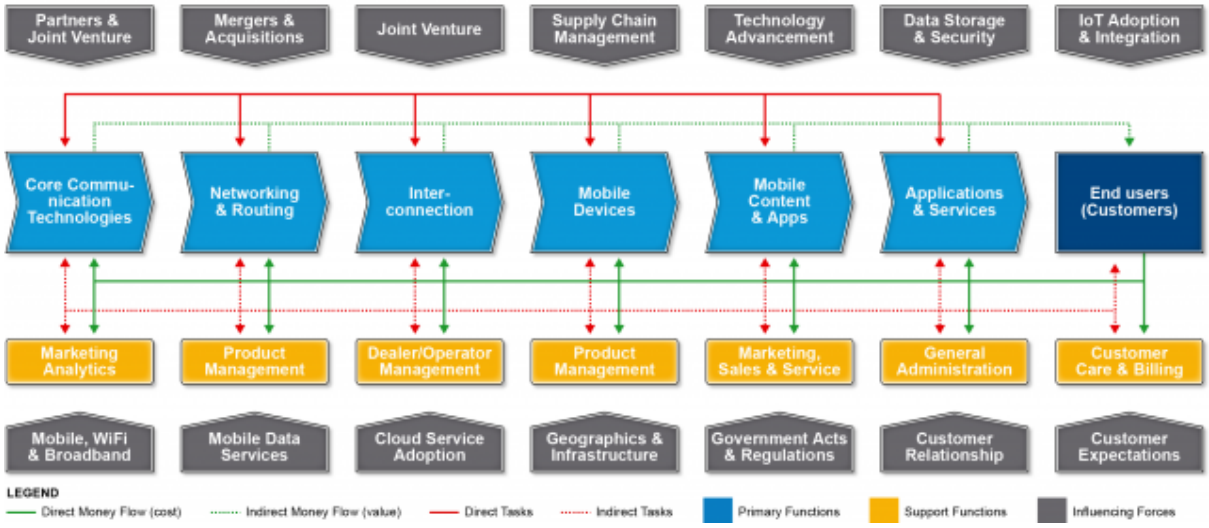
The French telecommunication operator Orange Telecom[464] "*assists companies in analysing data, and enriching it, by allowing them to cross-match it with data from third parties and to develop services from the analysis of this data allowing companies to actually change their performance and their customer relationships. For example, the development of market data services to better target marketing strategies; processing information in real time or near real time to facilitate and increase the speed of decision-making in organizations (fast data).*"[465]

Orange Telecom provides services to their customers, which support them to *"manage their information system in the Big Data era and therefore to put in place the architecture and cloud services that will help them store their data and analyse it with the computational power required. Big Data is, moreover, closely linked to the development of another strategic*

[463] Telefonica. https://blog.telefonica.de/2016/04/deutschland-in-bewegung-telefonica-nutzt-erkenntnisse-durch-advanced-data-analytics/
[464] Orange Telecom. http://www.orange-business.com/en/network
[465] Orange Telecom. http://www.orange.com/en/Press-and-medias/Mobile-World-Congress/Contents/Orange-Fast-Facts-in-2016

issue for Orange: The Internet of Things implying a 'big data/fast data/cloud' trio to become one of the factors that will make the market for the Internet of Things develop."[466]

Figure 50: Value chain in telecommunications



Source: http://www.leadingpractice.com/wp-content/uploads/Business-Model-Reference-Content-BML1-Telecommunication-01-640x303.png

The ability to aggregate data, to process it, to make it accessible and to allow for interactions with several stakeholders, i.e. for augmented reality, fully opens the scope of services to business customers. In line with this new business for telecommunication operators such as Orange Telecom[467] and Telefonica[468] is the requirement to be able to cover the complete data value chain including advanced data analytics.[469] Telecommunication operators are generally fast integrators with regards to big data and data analytics adoption. Data transfer and data storage are typical areas where telecommunication operators consider collaborations with content delivery network operators such as Akamai[470] or providers of cloud solutions such as Level3[471], to work as scalable data platforms enabling data-based product and service differentiation over time and to compensate for peak-load. In addition to the in-house integrated value chain, telecommunication providers also cooperate with other sectors' companies, i.e. *"Orange Business Services is providing a single, easily-provisioned SIM card that provides data connectivity for the [*fleet management*] solution, together with value*

[466] Orange Telecom. http://www.orange.com/en/Press-and-medias/Mobile-World-Congress/Contents/Orange-Fast-Facts-in-2016

[467] Orange Telecom data-related business services examples: 'Live Objects' (connecting smart objects/devices with business applications), 'Fleet Performance' (data services and equipment for vehicle fleet management applications).

[468] Telefonica data-related business services examples: 'Mobility Insights' (B2B service providing access to mobility and geo data), 'DAP' (B2B data aggregation and anonymisation services).

[469] See http://www.rcrwireless.com/20160222/big-data-analytics/telefonica-to-deploy-big-data-analytics-centers-by-the-end-of-2016-tag5

See http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/Smart-Data-Business.pdf?__blob=publicationFile&v=6

[470] See https://www.akamai.com/

[471] See http://www.level3.com/en/

added services, including service management and access to a portal for SIM management. The Orange SIM provides users with reliable connectivity and cost-effective cross-border roaming."[472]

Data ownership, access to and (re-) use of data, data portability and interoperability

Telecommunication providers are generally leading in terms of data processing techniques. They are gathering massive quantities of data on their electronic communications services in combination with mobility data of their users from their cellular networks, which have to be managed properly in order to have adequate internal processes and to optimise their own performance also improving customers' satisfaction, and to deliver new, innovative services. As mentioned above, telecommunications providers typically manage data services fully in-house. Thus, telecommunication operators develop value added services on top of their own data, either for internal purposes or for improving services to business clients. Providing intelligence services using data from their networks, the data typically used within telecommunication operators businesses therefore comprises of internal network data, sensor data and social media data.

The processing of personal data in telecommunications within the European Union was until recently mainly covered by the Directive 95/46/EC, which is enhanced and updated by the new General Data Protection Regulation[473], which recently entered into force. This regulation makes sure that Member States are forbidden to restrict or even to prohibit the free flow of personal data between Member States, i.e. by means of technical or legal barriers implemented at national level. The new regulation imposes quite stringent duties and obligations on both actors, on the controller as well as on the processor of the data. The controller is the one who determines purposes and means of the processing of personal data and the processor is the one who processes personal data on behalf of the controller. Given the above, the fact that personal data and non-personal data can be rapidly transferred by the telecommunications provider from one datacentre to another and customers have usually no control or knowledge over the exact location of the provided resources, the location independence concept understandably stimulate customers' concerns on data protection (personal data) and data security (non-personal data) compliance. Thus, it will take some time until there is evidence on data processing practices and enforcement practices under the new regulations.

Data portability according to the EU General Data Protection Regulation goes beyond the right to obtain a copy of the (personal) data, since it requires controllers to transmit the data directly to another controller at the request of the data subject, and can be compared to number portability in telecommunications in switching between mobile providers. To use

[472] Orange Telecom. Orange Business Services Partners with Konetik to Drive Forward the New Wave of Fleet Management: http://newswire.telecomramblings.com/2016/04/orange-business-services-partners-with-konetik-to-drive-forward-the-new-wave-of-fleet-management/

[473] EU Regulation 2016/679.

professional networks as an example, it entitles a LinkedIn user to ask LinkedIn to transfer the personal data directly to a service of a telecommunications provider and vice versa, instead of downloading the data from LinkedIn and upload it again to the service of a telecommunications provider. As regards non-personal data or anonymised and aggregated data the data portability issues are subject to individual contracts between the companies respectively.

The current e-Privacy Directive 2002/58/EC is restricting the usage of massive volumes of geo and traffic data of their users for marketing purposes and requires the agreement of the users for the application of tracking-cookies on their websites, etc. Since technological progress is quite fast in this particular sector, and other tracking technologies generating consumer data are not covered (i.e. fingerprinting, pixels, etc.), there is an ongoing review of the e-Privacy Directive concerning the respect for private life and personal data in electronic communications and repealing Directive 2002/58/EC 'Privacy and Electronic Communications Regulation'. It is up to the results of this process that are expected to have a huge impact on the telecommunications sector as well as for the over-the-top (OTT) services and their data-driven business models.

Confidential and personal data are prominent in telecommunications services. The telecommunications sector is more regulated in terms of data than other sectors. Also in this sector, using the concept of ownership is less relevant than the use of data, access to data and exploitation of data. Setting ownership rules means shaping the market in one specific direction but the solutions should rather focus on contractual issues in a multilateral or bilateral setting, otherwise there is a risk of market failure. Competition law can offer adequate answers to issues related to business models. Geographical restrictions need to be urgently tackled to enable more efficient use of resources and more flexibility.

Potential contractual and non-contractual barriers

Potential contractual barriers

Telecommunication operators' resources are usually offered to customers from different locations and data related to their businesses can easily and quickly be transferred from one datacentre to another one. Therefore, if particularly business-sensitive data are to be processed, for example in the cloud, customers should consider whether to specify the location where their data will be processed. By contracting out to the telecommunication providers' fundamental computing resources, customer's business becomes very dependent on the correct performance. Thus, service level agreements (SLAs), liability and indemnity clauses play a fundamental role. Detailed SLAs, in which the telecommunication providers' levels of performance are accurately regulated, coupled with contractual clauses that clearly allocate, on the one side, general parties duties and obligations, and, on the other side, parties' liabilities and responsibilities will be adequate for a good relationship.

Given the specific services delivered to business customers, individual agreements can vary substantially depending on the aggregation procedures and granularity levels of the relevant data and assigned property rights and are therefore difficult to evaluate at this stage. Potential existing exclusive rights regarding data shall be examined as well. If data are traded as

such, they are treated as goods and not as data-related services. In such cases, data are objects defined by their use and it has to be clarified whether certain data are subject to property rights. In Germany, the objects of rights are often identified with goods and a good is the sum of its possible uses. Thus, data property rights can be seen as a bundle of rights/possible uses assigned to the rights holder. Given the categories of property rights (use, benefits of the use, changing type and transfer of the property) the agreements as regards possessing information, using information and destroying information have to be identified. These categories can be directly translated into categories of data property.

Liability issues can be regulated within the telecommunications operators' terms and conditions as well as on an individual contractual basis depending on the service offered. Thus, legal aspects of associated risks are difficult to assess on a general basis. Since data portability issues with respect to non-personal data or anonymised and aggregated data are subject to individual contracts B2B it cannot be identified whether there are potential contractual barriers resulting from these issues because the interviewees were not allowed to provide information on such matters.

Potential non-contractual barriers

With the General Data Protection Regulation (Regulation (EU) 2016/679) technical or other barriers as regards the processing of personal data should not exist and otherwise being enforced by the corresponding regulatory authorities. In particular, besides data protection (privacy) and consumer protection (transparency) there is a data security protection regulation in place concerning non-personal data (all other data) in most Member States. Data security regulations are also of fundamental importance for the sector-specific telecommunications regulations. Moreover, interoperability is also regulated by national regulatory authorities. Since other potential barriers as regards the free movement of data in telecommunications face strict sector-specific regulation as well due to high EU standards and national requirements, other potential barriers for the European data economy cannot be identified, yet. Data portability regimes such as the one implemented by the new European General Data Protection Regulation concerning personal data in combination with various national data protection regulations in line with EU-wide settings have the legal reach to prevent most non-contractual barriers as regards personal data in the telecommunications sector.

Health

The generation, use and exchange of data as well as the use of new technologies plays an increasingly important role in the healthcare sector. Whether it is in hospital settings, nursing homes or in private homes – a range of technologies are used to connect different aspects of the "health ecosystem".[474] The possibilities of technological advances and big data also lead to the emergence of new business models, trying to capture the potential benefits presented by the advance of digitisation. The **main types of data** which are relevant to the health sector, are:

- Patient data (including personal information or health records);
- Hospital internal data (including data about patient flows or the storage of assets);
- Research data (e.g. academic studies on, for example, treatment diseases); and
- Behavioural data from sensors and apps (e.g. physical constitution, nutrition and other health-related habits).

In addition to this classification based on data content, the distinction between open and proprietary or closed data is especially relevant in the health sector: A large share of health datasets is produced and maintained by private insurers or pharmaceutical companies, which may not share it with other actors for privacy or economic reasons. Therefore, open health datasets are a relatively new phenomenon, mostly promoted through governments and civil society organisations.[475]

In line with this variety of data types, a diverse set of **stakeholders** is involved in the data value chain in the health care sector. In addition to sector-typical stakeholders like hospitals, therapists or doctors and insurances, new stakeholders entered the field based on the ongoing digitisation, such as app providers and analytics companies. In this context, some stakeholders are experimenting with new business models based on data, including:

- Open data competitions[476];
- Partnerships between research groups and analytics companies;[477] or

[474] Pappas, H.P. (2016), Welcome note to the Intelligent Health Pavilion at HIMSS 2016, in Intelligent Health Pavilion Handbook, available at http://ihassociation.org/2016-iha-handbook/

[475] See http://openhealthdata.org/.

[476] In open data competitions, a reward is promised by one or a number of sponsors to those developers that solve a specified problem (or a set of problems) based on a dataset provided online. These (recurring) tournaments, like the *Data Science Bowl* of *Booz Allen Hamilton* are administered through portals like *kaggle.com*. Recent competitions include a search for optimised strategies for lung cancer detection, involving a total volume of USD 1 million in prize money, attracting more than 1200 competing teams so far., see https://www.kaggle.com/c/data-science-bowl-2017. Other examples include the *Health Datapalooza* (http://www.academyhealth.org/healthdatapalooza), rewarding developers with similar prizes, or much smaller competitions organised by the NHS England. (https://www.england.nhs.uk/ourwork/tsd/data-info/open-data/).

- Safe spaces for collaboration on data[478].

Table 31: Stakeholders potentially involved in the data value chain in health

	Not data driven business models/ companies	Data driven business models/ companies
Data producer	• Hospitals • Insurance companies • Doctors/therapists • Other healthcare facilities • Public administrations	• Online platforms • Apps • Wearables • Manufacturers of RTLS systems
Data user	• Hospitals • Insurance companies • Doctors/therapists • Other healthcare facilities • Public administrations • Universities (specialised institutes)	• Data analytics companies • Specific healthcare management enterprises which are working together with users who produced the data • Manufacturers of RTLS systems

Source: Deloitte.

The smart use of data and new technologies have the potential to reduce costs and/or generate revenue for providers of services as well as to bring advantages for patients, other citizens (e.g. users of health apps) or society as a whole. In terms of optimising health management, researchers can mine data to evaluate the effectiveness of treatments or identify patterns. Furthermore, big (open as well as closed) data may be used to:

- Predict infection risk;
- Measure health quality;
- Measure proactive patient health engagement;
- Analyse population health; and
- Analyse patient population and understand the patient journey.[479]

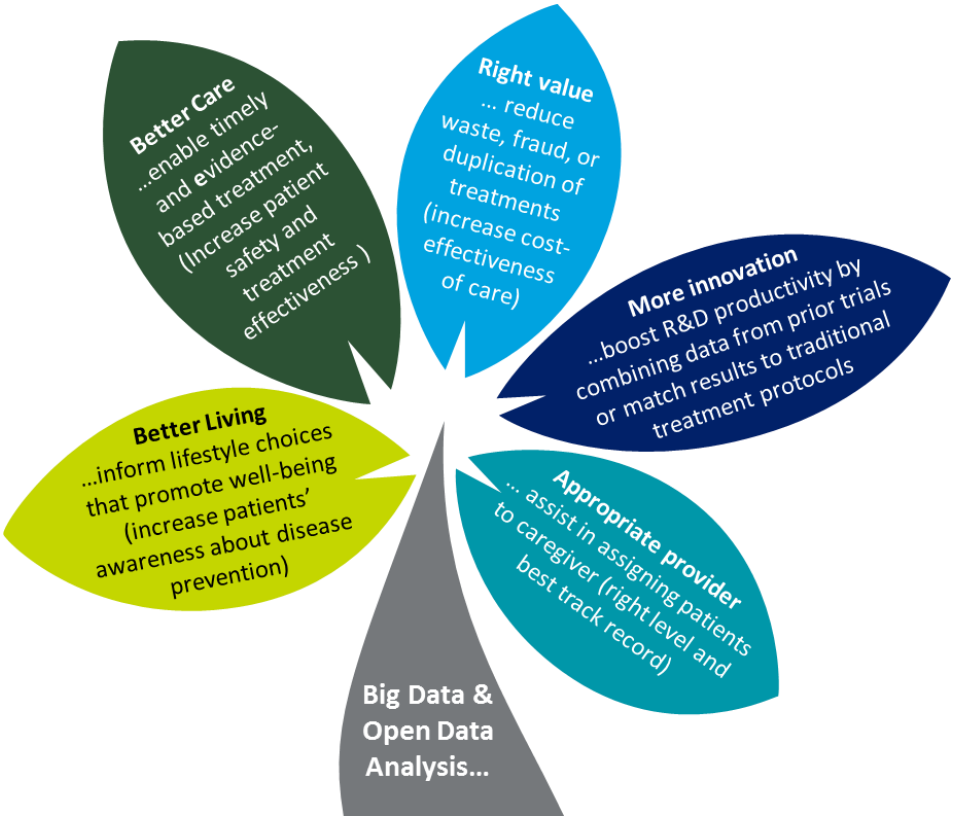
An overview of potential merits of data use in the healthcare sector is provided in the following figure.

[477] The Structural Genomics Consortium is an example for these collaborations between public research institutions, pharmaceutical companies and public as well as private donors. Established in 2004, it united the universities of Oxford, Toronto and the *Karolinska Institutet Stockholm* with *GlaxoSmithKline*, *Novartis* and *Merck*. Additional funding and expertise was provided by the *Wellcome Trust*, government institutions and smaller foundations. Together they sought to model "the three-dimensional shape of thousands of human proteins with potential relevance for drug discovery", see Perkmann, M. and Schildt, H. (2015): Open data partnerships between firms and universities: The role of boundary organizations, in: *Research Policy* 44 (5), p. 1133–1143.

[478] Several initiatives in the development aid sector aim at generating open data, fostering exchanges and collaboration. The *World Health Organisation* (WHO) set up the *Global Health Data Collaborative*, where member countries work together with development agencies, donors and academics to strengthen health information systems. Likewise, the *OpenHIE* network aims at fostering exchanges of healthcare data between countries. In both cases, improved availability of data and interoperability of systems and software is expected to improve patients' treatments.

[479] McKinsey (2013): The 'big data' revolution in healthcare.

Figure 51: Potential merits and new value pathways of big data use in the healthcare sector



Source: based on McKinsey[480], graphical representation by Deloitte.

In the following sub-sections, we analyse existing business models and potential barriers in relation to two different facets of the health sector: the hospital context (representing more traditional data generators), and apps and wearables (representing newer data generators). In addition, a short excursion about the situation in the U.S. illustrates examples and experiences with barriers in an advanced digital health market. At the end we provide a summary of our main findings in relation to the health sector.

Real-Time Location Services (RTLS) used for patient and asset tracking

Context: The use of RTLS in the hospital context

Hospitals nowadays are under pressure to deliver high quality and cost-efficient services. New technologies, such as Real-Time Location Systems (RTLS), can help by increasing efficiency and quality at the same time.[481]

Intelligent Hospital: Example of an intelligent operating room (OR)

Based on the Intelligent Health Pavilion presented at the 2015 HIMSS conference *Healthcare IT News* painted a picture of what a truly connected hospital can look like.[482]

[480] McKinsey (2013): The 'big data' revolution in healthcare.
[481] Cf. Müller, M. (2011), Echtzeitlokalisierungssysteme für Krankenhäuser – welche Technologie passt? Ergebnisse einer Untersuchung des Fraunhofer-Instituts für Integrierte Schaltungen (IIS), *Krankenhaus-IT 3/2011*.

In this scenario, an OR contains several screens, displaying key data for the on-going procedure. This includes predictive analytics data on that specific procedure, such as forecasted outcomes. The patient and all staff members wear badges with which they can identify themselves electronically. These are scanned when entering the room.

In addition, staff members wear hands-free devices that can receive communications in the OR. Surgeons that are not on the spot can watch the procedure through real-time cameras and offer feedback via video screens.

Supplies are tracked as nurses log every unit used by scanning electronic badges. This way, usage can be monitored and expired supplies can be flagged automatically so that they are not used any longer.

Devices linked to the patient's vitals monitor anaesthesia. This way, it can be ensured that sedation is given in the right amount. Provision of drugs is monitored using devices, directly feeding this information into the patients' electronic health records (EHR).

RTLS are automatic systems, which can identify and locate objects or persons equipped with a tagging device. In the hospital context, this concerns e.g. medical equipment or patients.[483] The tags communicate their location via a network. Signals may be transmitted via different technologies, e.g. radio-frequency identification (RFID)[484] or Wi-Fi. The network communicates the data to a software interface. That way, users can see the location of the different tags graphically and can e.g. search for the location of specific items or persons.[485] An example of a graphic representation is presented in the figure below.

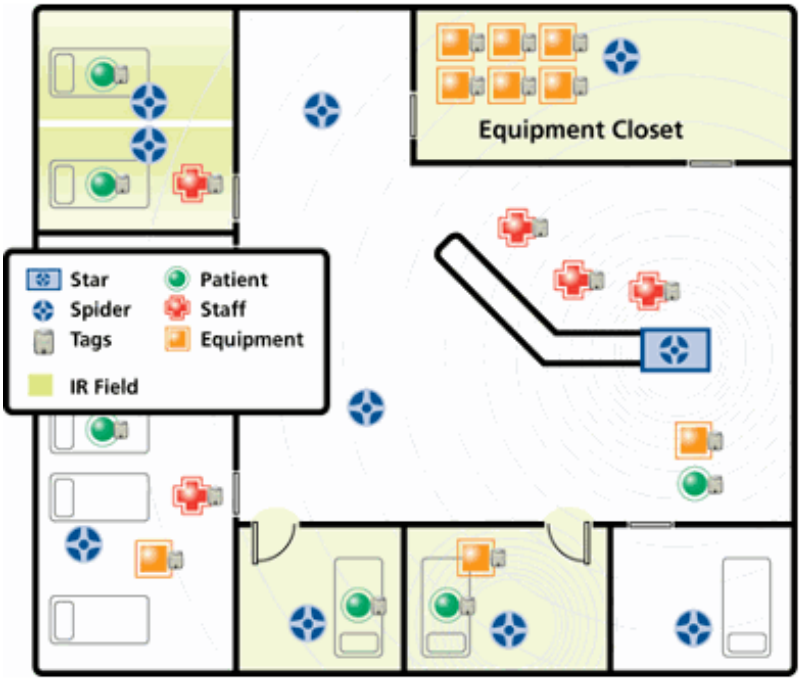
[482] Powderly, H. (2015): Intelligent hospital, home on display: The Intelligent Hospital Association features a suite of 'intelligent' demonstrations at HIMSS15, Healthcare IT News (http://www.healthcareitnews.com/news/intelligent-hospital-home-display).

[483] It is e.g. also possible to monitor staff, but this is outside the scope of this case study, which focuses on asset and patient tracking.

[484] In this case, it is only possible to locate objects if they pass a reading device.

[485] Fisher, J.A. and Monahan, T. (2012), Evaluation of real-time location systems in their hospital contexts, *International Journal of medical Informatics 81(2012)*, 705-712.

Figure 52: Example of RTLS use in a hospital (graphic representation of tags)



Source: Secure Edge Networks[486]

Inventory and tracking systems can help hospitals to keep an overview of where equipment, staff members and patients are located to organise their services.[487] More precisely, RTLS for the purpose of patient and asset tracking can fulfil the following **immediate functions**[488]:

- Identification and location of assets including e.g. expensive and mission critical equipment (e.g. infusion pumps, ultrasound scanners, and patient monitors), wheelchairs, or drug supplies:
  - Tracking of lost or misplaced equipment and information on the status of equipment (e.g. available, in use, to be repaired, etc.) to help staff to carry out their tasks efficiently, reducing search time and costs;
  - Tracking equipment to prevent theft;

[486] http://www.securedgenetworks.com/blog/Benefits-of-Real-Time-Location-System-on-Hospital-Wireless-Networks

[487] Sopensky, E. (2016), *The RFID-Enabled Intelligent Hospital*, in Intelligent Health Pavilion Handbook, available at http://ihassociation.org/2016-iha-handbook/; Katainen, Mirja (2008), Real-time location over standard Wi-Fi networks, *HighTech Finland*, available at: http://www.hightechfinland.com/direct.aspx?area=htf&prm1=661&prm2=article.

[488] Cf. e.g.: Vecchione, A. (2014), Hospitals are finding ROI from RFID – 'The time-savings justify the cost of the chips', *Healthcare IT News* (http://www.healthcareitnews.com/news/hospitals-find-roi-rfid-deployment); Katainen, M. (2008), Real-time location over standard Wi-Fi networks, *HighTech Finland*, available at: http://www.hightechfinland.com/direct.aspx?area=htf&prm1=661&prm2=article ; Pierson, A. (2010), Location made easy, *HighTech Finland*, available at: http://www.hightechfinland.com/direct.aspx?area=htf&prm1=894&prm2=article; Fisher, J.A. and Monahan, T. (2012), Evaluation of real-time location systems in their hospital contexts, *International Journal of medical Informatics 81(2012)*, 705-712; Sopensky, E. (2016), *The RFID-Enabled Intelligent Hospital*, in Intelligent Health Pavilion Handbook, available at http://ihassociation.org/2016-iha-handbook/.

    - Management of inventory, including e.g. optimising the distribution of equipment among different departments, organising maintenance and replacement;
- Identification and location of patients:
    - Identifying patients' whereabouts e.g. if a medical procedure is to be started or to inform relatives of the status of a surgery;
    - Verifying the identity of patients before the start of medical procedures;
    - Protection of persons with dementia; and
    - Protection of babies from being stolen.

These functions lead to an increase in efficiency and cost saving as well as better patient care and patient safety[489] including by ensuring the safety of medical devices.[490]

In addition, such systems can fulfil **long-term functions**, notably via the data generated by its day-to-day use. This data can later on be analysed with a view to optimising procedures. For example, the actual use of medical equipment could be analysed to predict whether more or less equipment is needed in the future.

In the sections below, we explain a typical business model in relation to patient and asset tracking, actors involved, and discuss potential contractual and non-contractual barriers.

Business model: A typical service offering

Systems for asset and patient tracking in the hospital context are typically offered by firms that specialise in the health care sector, to be able to cater to the specific needs of hospitals.

The RTLS provider we interviewed develops relevant hardware as well as software necessary for the RTLS, specifically suited for the hospital environment. They also offer the practical implementation of the system, as well as supporting measures such as training. Once the system is in place, they offer technical support to their users e.g. in case something is not working properly. However, the security of the systems has to be ensured by the user, as the RTLS is integrated into the users' IT systems.

Other RTLS providers may work with partners: for example, it is possible that a company rather focuses on the production of hardware and software and that the installation is carried out by businesses specialised in networking and security integration.

The hospital that we interviewed chose their RTLS provider based on a public procurement procedure. In addition to the price, they took into account the technical solution, flexibility and also the geographic location of the provider. They considered that it would be most convenient to have a provider in the region, as interchanges would be easiest. The system was installed five years ago and is used for patient and asset tracking.

[489] Katainen, Mirja (2008), Real-time location over standard Wi-Fi networks, *HighTech Finland*, available at: http://www.hightechfinland.com/direct.aspx?area=htf&prm1=661&prm2=article; Fisher, J.A. and Monahan, T. (2012), Evaluation of real-time location systems in their hospital contexts, *International Journal of medical Informatics 81(2012)*, 705-712.

[490] See: Polisena, J., Jutai, J. Chreyh, R. (2014), A proposed framework to improve the safety of medical devices in a Canadian hospital conext, *Dove Press Journal* (Medial Devices: Evidence and Research).

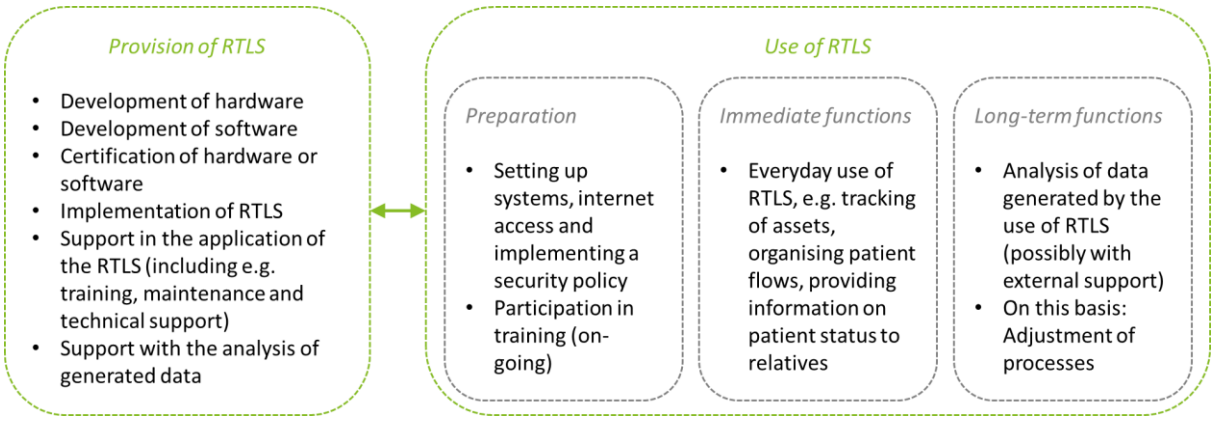
The hospital uses the **tracking of patients** first to locate them. Once a patient enters a room, his or her tag is registered with the system. That way, nurses can see where the patient is. This is important e.g. if the patient is in need of medicine but has been taken to x-ray. The hospital can also monitor when the OR is free, e.g. to organise cleaning. Furthermore, it is possible for visiting families to check the whereabouts of a patient. They see a map and need to know the code number of their relative. This service is highly appreciated by families and staff. Staff saves time, as families do not ask as many questions about the status of procedures.

The **tracking of assets** is mainly used to locate equipment. This is considered very helpful, as the hospital is very big and the staff spends a lot of time searching for objects. This includes, for example, wheelchairs, which are sometimes hidden by patients to use them further. Controlling where the assets saves a lot of time.

The hospital interviewed as part of this case study has also been starting to **analyse the data generated by the RTLS**. For example, they are studying the flow of patients in chirurgical rooms to optimise their use. The hospital plans further analyses as well as an integration of the RTLS with the hospital's business intelligence application.

The figure below portrays the different steps involved at the providers' and users' side. These may be carried out by various actors, as explained in the following section.

Figure 53: Exemplary display of the steps involved in the provision and use of RTLS



Source: Deloitte

Actors

In the example discussed with the interviewed RTLS service provider, there are two main parties involved: the RTLS provider and the client. As indicated above, the RTLS provider develops software and hardware components and offers a wide service package to the client, including installation of the RTLS, training, technical support and support with data analytics.

However, it is thinkable that additional parties are involved, depending on the situation:

- On the providers' side:
  - Vendor of raw material and specific parts of the hardware;
  - Certifier of hardware and software;
  - Cooperation with analytics company if this service is not offered by the provider;

- On the users' side:
  - Internet provider (relevant for RTLS that function over Wi-Fi);
  - Provider of hardware, including e.g. computers;
  - Support in relation to the IT structure and security policy;
  - Provider of data storage solutions such as clouds (not common yet); and
  - Support with analysing the data and optimising processes (e.g. consultants), although the analytics part may be offered by the RTLS provider.

In addition, third parties may be interested in the information generated by the RTLS. For example, tracking data of patients may bring valuable information for future hospital designs.[491] In the example analysed as part of this case study, the data is not shared with any third parties.

Potential contractual barriers

Data ownership

In the example analysed as part of this case study, the hospital is the owner of all data generated via the RTLS. The data is generated and stored there. The question of ownership is **clearly defined** in this case and neither of the interviewees see any issues in this regard at the moment.

However, the interviewed RTLS provider indicated that there could be difficulties in the future: at the moment, the data is stored on the servers of the hospital. In the future, it is thinkable that data would be stored in a cloud. In this case, the question of ownership and access would need to be clarified between the hospital and the cloud provider.

Security, access and (re-) use

The hospital is responsible for defining a **security policy to prevent unauthorised access**. This includes security of hardware and software as well as access policies. The interviewees explained that there are different access levels defined for the data generated by the RTLS, with some aspects only being accessible to management staff. For example, a nurse responsible to assign wheelchairs, cannot access patient data. According to the hospital, the access restrictions are as strict as for clinical information. Of course, the hospital has to comply with the relevant data protection law.

The RTLS provider may **access and use** the data generated by the system for two reasons:

- To check whether the system is working properly; and
- To support the client with analyses of the data.

In both cases, all data is only shared in anonymised form, so that it is not possibly to identify any patients or staff. The RTLS provider may either work with the data in the system of the hospital or in their own system. In any case, the RTLS provider needs to follow the security and access rules of the client.

[491] See: http://www.securedgenetworks.com/blog/Benefits-of-Real-Time-Location-System-on-Hospital-Wireless-Networks

The hospital does not share the data with any other parties. Accordingly, this is an example of the **closed data category**, in which the data is only used by the data controller.

A factor that may potentially affect the **use** of the data generated by the RTLS is **data quality**. A study carried out in the US found that many RTLS systems were in fact not able to deliver accurate results leading e.g. to tags not being found or tags registered in the wrong place.[492] Such issues would also lead to weak data quality, which may hinder the usefulness of analyses and potentially discourage hospitals from analysing such data. This was, however, not confirmed by the hospital interviewed as part of this case study. The interviewee indicated that the RTLS is reliable and accurate and that the information gathered is very helpful to understand the processes. The challenge lies rather in finding suitable solutions to the identified problems.

Liability

According to the interviewees, questions in relation to liability have not posed any challenges so far.

In general terms, the RTLS provider works towards **minimising incidents by ensuring a high quality of their products**. This includes the provision of technical support to solve any issues as soon as possible.

As concerns **potential errors** of the system, these do not lead to liability questions. For example, RTLS does not cause problems in relation to patient identification but rather solves such problems. If a hospital puts a wrong tag on a client, this can be recognised via the RTLS system. In general, patient identification works very well. There could be errors with locating items. However, inaccuracies in this regard do not lead to cases of damages, especially as the system is only complementary. It is still possible to check manually for the location of an item or a person, which is why no serious issues would occur.

On this basis, the interviewed RTLS provider did not experience a single case in which the client informed them of a mistake happening based on their system that could entail damages. On this basis, they do not have a specific policy on liability in their contracts. They agree with the clients that the system has to be working 90% of the time.

Potential non-contractual barriers

Technical barriers

Based on our interviews and desk research, technical barriers seem to be the most serious concerns from the perspective of providers and users.

One aspect concerns **interoperability**, both between the RTLS and a hospital's IT system as well as within different systems of one hospital.

First, there are **no common standards in relation to the IT systems hospitals use**; this may differ between countries and regions. On this basis, the RTLS provider needs to put efforts

[492] The study notes, however, that some of systems examined were in a pilot phase. Fisher, J.A. and Monahan, T. (2012), Evaluation of real-time location systems in their hospital contexts, *International Journal of medical Informatics 81(2012)*, 705-712.

into making the RTLS work in the hospitals. This requires additional resources and costs. The severity of such issues may depend on the type of technology used. For example, there are solutions of RTLS working with standard Wi-Fi networks instead of RFID. Such a solution was installed e.g. at Herentals Hospital in Belgium. In that case, it was necessary to integrate the new RTLS with the existing Wi-Fi network and SAP system, which could be achieved without major issues.[493] Although it is usually possible to achieve interoperability between the RTLS and the hospitals' IT systems, the interviewed RTLS provider argued that it would be useful if standards were more aligned.

The hospital confirmed that interoperability is challenging but manageable. The interviewee explained that the new RTLS system had to be integrated with the Health Information Management System of the hospital. This system is an in-house software developed on demand and it contains e.g. the Electronic Health Records. Although this was challenging, it could be achieved without major issues.

A related, potential barrier identified in other studies concern fears about possible interference between RTLS-transmitters and other radio-emitting devices used for diagnostics or treatment.[494] However, interferences should not occur in practice due to the provisions of the *Radio Equipment Directive* (2014/53/EU).

According to the hospital, on-going challenges are rather based on management. Both the applications of RTLS provider and the hospital's IT systems are regularly improving. If such improvements are not coordinated properly, information may be stored in different formats and it may be more difficult to retrace it. However, normally it is possible to recover the relevant information. The interviewee argued that such issues are based on communication and fall under the responsibility of the hospital/staff.

Second, difficulties could also occur on the side of the hospital. One difficulty that currently arises is that **even within one hospital different IT systems may not be interoperable**. On this basis, it is not possible for the hospital to synthesize data. For example, according to the interviewed RTLS provider it could be possible in theory to gather comprehensive information about the patients, including where they are located, which symptoms they have, who is treating them etc. However, this is not the case yet, because such data (stemming e.g. from RTLS and EHR) can often not be connected. Indeed, it was also argued by a US study that interoperability between IT systems used in the healthcare sector is a challenge based on proprietary platforms and interfaces. On this basis, the study found that hospitals were reluctant to invest in RTLS, as it was no clear how it would work with other IT sys-

[493] Katainen, Mirja (2008), Real-time location over standard Wi-Fi networks, *HighTech Finland*, available at: http://www.hightechfinland.com/direct.aspx?area=htf&prm1=661&prm2=article

[494] van der Togt R, et al. (2008): Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment. *JAMA, 299 (24), 2884-2890. doi:10.1001/jama.299.24.2884*

tems.[495] The interviewed hospital indicated that it is planned for the future to connect the information from tagging oncology patients with their EHR.

Another potential issue is **technical uncertainty** based on variety of offers and lack of transparency. A study carried out in the US between 2008 and 2010 found out that many hospitals in the US were unsure about the usefulness of RTLS and about which technology would be the most suitable based on the variety of offers. On this basis, they preferred waiting until the different technologies were developed further, leading e.g. to a clear superior. Indeed, as mentioned above the study also found that many of vendors' claims as concerns the accuracy of their systems could not be upheld.[496]

Other barriers

A precondition for the successful application of RTLS and the exploitation of the generated data is **effective change management**, i.e. including the design of processes for the implementation of the new system.

This has been identified as a barrier in a US study on RTLS. For example, in one hospital that had implemented RTLS for asset tracking, the administration had not defined responsibilities for placing tags on equipment, entering the information into the database and monitoring the database. On this basis, there were only few tags in use and a lack of awareness among staff. In some cases, staff was reluctant to use the new system, as they were not aware of the benefits or because they believed falsely that the system was used to monitor their performance.[497] Such barriers obstruct both the immediate and long-term functions of such systems.

The interviewed RTLS service provider also raised this aspect. It was underlined, that change management is an important aspect of the service offering of this specific RTLS provider. For this purpose, they work closely with their clients including e.g. to deliver training. The hospital did not report any challenges in this respect. While training is of course indispensable, the implementation happened smoothly and the staff in general supports the RTLS as it makes their work easier.

[495] Fisher, J.A. and Monahan, T. (2012), Evaluation of real-time location systems in their hospital contexts, *International Journal of medical Informatics 81(2012)*, 705-712.
[496] Fisher, J.A. and Monahan, T. (2012), Evaluation of real-time location systems in their hospital contexts, *International Journal of medical Informatics 81(2012)*, 705-712.
[497] Fisher, J.A. and Monahan, T. (2012), Evaluation of real-time location systems in their hospital contexts, *International Journal of medical Informatics 81(2012)*, 705-712. See also: Cf. Müller, M. (2011), Echtzeitlokalisierungssysteme für Krankenhäuser – welche Technologie passt? Ergebnisse einer Untersuchung des Fraunhofer-Instituts für Integrierte Schaltungen (IIS), *Krankenhaus-IT 3/2011*.

Mobile health: Apps and wearables in the health sector

Context

The idea of apps and wearables in the health sector

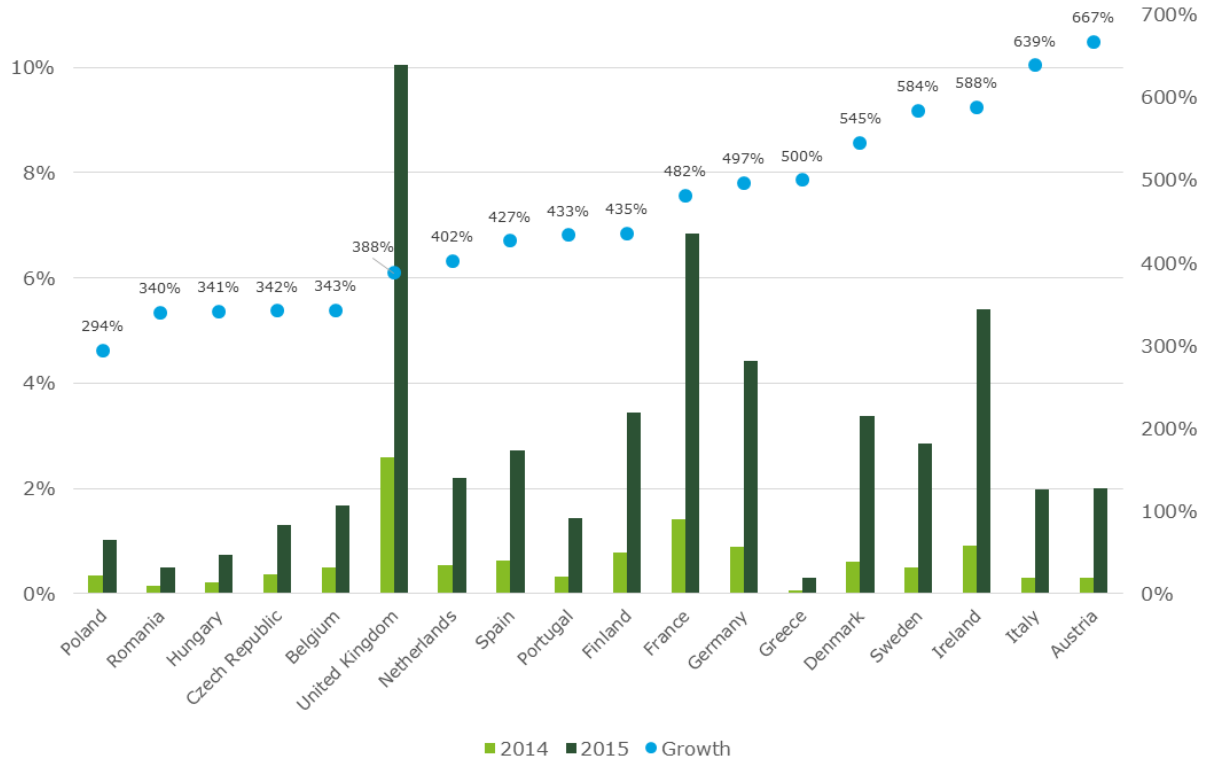
In essence, apps and wearables in the health sector are a low threshold, ad hoc means of self-monitoring and communication between a healthcare provider and a (potential) patient. The industry is generally referred to as mobile Health (mHealth). Typical examples of wearables are: Smart watches, glasses, scales, thermometers, blood pressure monitors, heart rate monitors, alarm clocks. Examples for of applications are:

- **Whitings**: Offers products such as activity and sleep tracking watches, wireless blood pressure monitors, sleep sensors, smart scales, compatible through an open API;
- **Runtastic**: Offers different trackers and smart scales as well as integration of their apps with other smartwatches and synchronisation with other apps;

A recent study conducted by IDC and Open Evidence on behalf of the European Commission indicates that wearables are becoming increasingly popular in Europe: Although the share of Europeans owning such devices is still rather small, adoption rates are growing at a fast pace. Depending on the Member State, between 2014 and 2015 alone, the share of the population owning a wearable device at least tripled – in exceptional cases like Austria or Italy even increased by more than six-hundred percent.[498] Figure 51 summarizes this development for 18 selected Member States.

[498] IDC and Open Evidence (09.06.2016): European Data Market (SMART 2013/0063). D8 — Second Interim Report. Statistical Annex. https://a2528ba5-a-c3c32646-s-sites.googlegroups.com/a/open-evidence.com/download/repository/EDM_D8_Statistical%20Annex.pdf?attachauth=ANoY7crEDv9XIIfoKK6zBN2evNHADcHfWQQyYRRHfovwLdzzV4pwnKop970VIIRgOhkayOzmPKwsjPnpk5283cUSNrPlzvZu4kFMWOPOu3djODmcVtWEjL2l_WAfwPoOK5KbmxKcToqF8PLcWEGMxsm45UKF6C_lftZzzIizrw3fY7AINVfmZeMSfGawlLLVqdEuTtPnR5ui1kwyT1vOqyaNrGdPfG-TcaNSqrpDjMY5bG9m19cwoKZAX17dwX95kqk7kzIwQxQI&attredirects=2

Figure 54: Percentage of citizen owning a wearable device and (n=18 Member States)



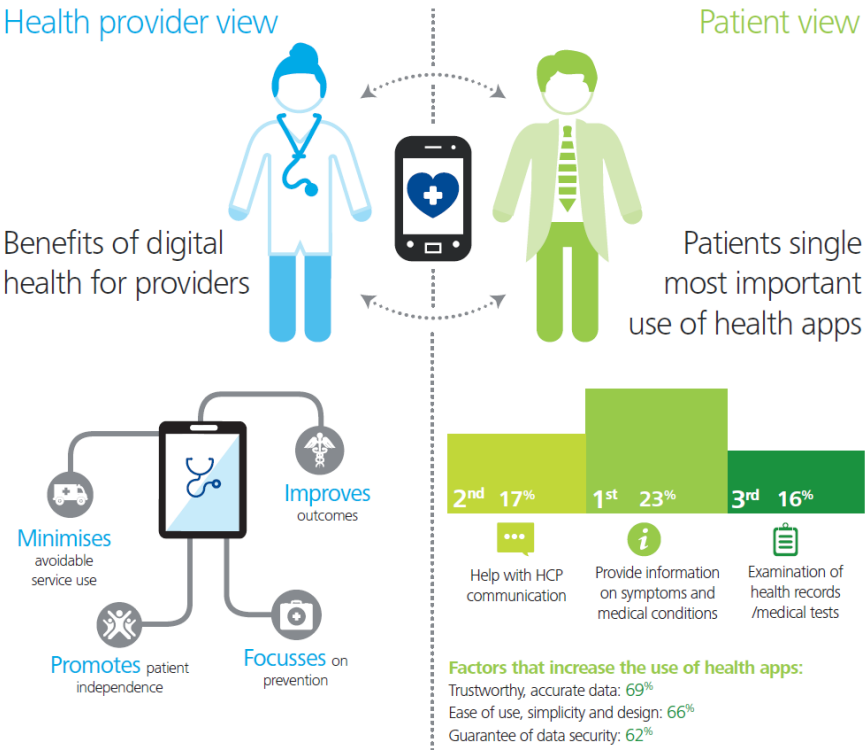
Source: data collected by IDC/Open Evidence, graphical representation by Deloitte

Interestingly, the study also reveals that the number of citizens basing their decisions on data is increasing in a very similar fashion. Thus, while the actual user base of commercially available wearables is still small, to users they represent more than just gadgets and affect their behaviour.

Indeed, according to a 2015 Deloitte study[499], the provision of information on symptoms and medical conditions, the communication with healthcare professionals, and the examination of health records are the three most important use patterns for health apps by patients. By contrast, healthcare providers such as doctors, hospitals, and insurance companies can make use of already existing information (instead of gathering the information themselves) in order to provide their services to patients. This is expected to minimise avoidable service, improve the service quality – in other words to increase the effectiveness and efficiency.

[499] Deloitte (2015): Connected health. How digital technology is transforming health and social care. See: http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf

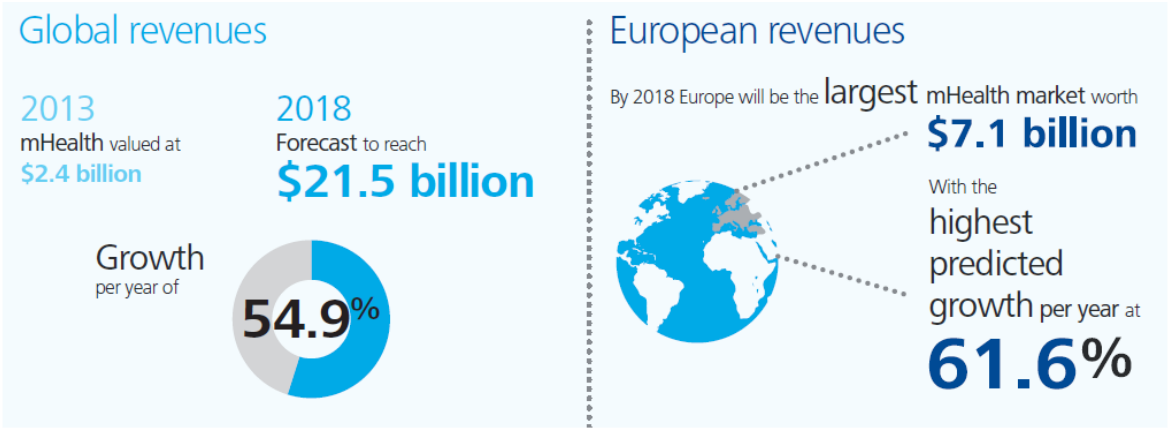
Figure 55: Potential benefits of mHealth for service providers and patients



Source: Deloitte (2015)

The Deloitte 2015 study has estimated the global mHealth market to grow to 21.5 billion USD in 2018 with the EU market growing to 7.1 billion USD.

Figure 56: The global and EU mHealth market development



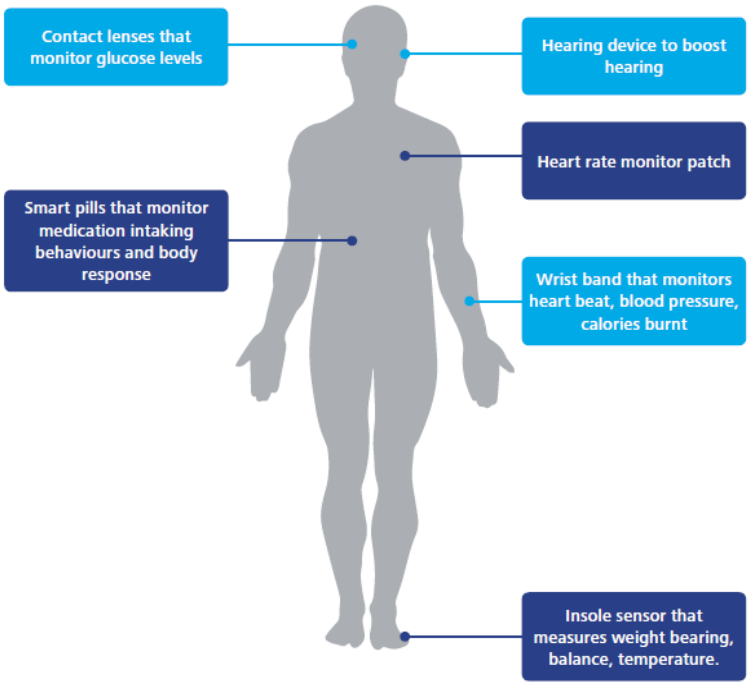
Source: Deloitte (2015).

In addition, according to the European Economic and Social Committee, mHealth could in 2017 potentially save a total of EUR 99 billion in healthcare costs in the EU.[500] Boston Con-

[500] European Economic and Social Committee (2014): TEN/551 EU Framework on "mHealth" and "health applications and wellbeing apps".

sulting Group has estimated that mHealth could reduce the number of doctor visits in the EU by 330 million a year.[501]

The growth of the mHealth market is and will be driven in the future by three factors[502]:



Digitalisation: Through the increasing prevalence of smart devices and by developing and making use of modern applications, digital technology enables the efficient provision and use of previously analogue services by means of smart phones, tablets, and other wearables such as e.g. smart glasses and watches.

Health awareness: Today, citizens are much more aware of individual and societal health issues than in recent years. This leads, on the one hand, to an increased demand for effective, high quality, personalised services (top-down logic, precision medicine) while, on the other hand, citizens make increasingly use of the possibility to shape and impact on the available services by providing health data on their own (bottom-up logic). According to a 2014 PwC study, 77% of US consumers want wearables to exercise smarter, 75% to collect and track medical information, and 67% to eat better.[503]

Societal ageing: This general societal macro-trend is not only impacting on the health market but on all facets of social life (e.g. communication, employment, education). With citizens becoming increasingly old, however, the health sector is facing particular challenges with regard to e.g. its organisation, finance, and service quality and continuity. Market operators see mHealth as a means to cope with such current and future challenges.

[501] Boston Consulting Group (2015): Five priorities for achieving the Digital Single Market. Commissioned by ETNO. See: https://etno.eu/datas/publications/studies/FINAL_BCG-Five-Priorities-Europes-Digital-Single-Market-Oct-2015.pdf

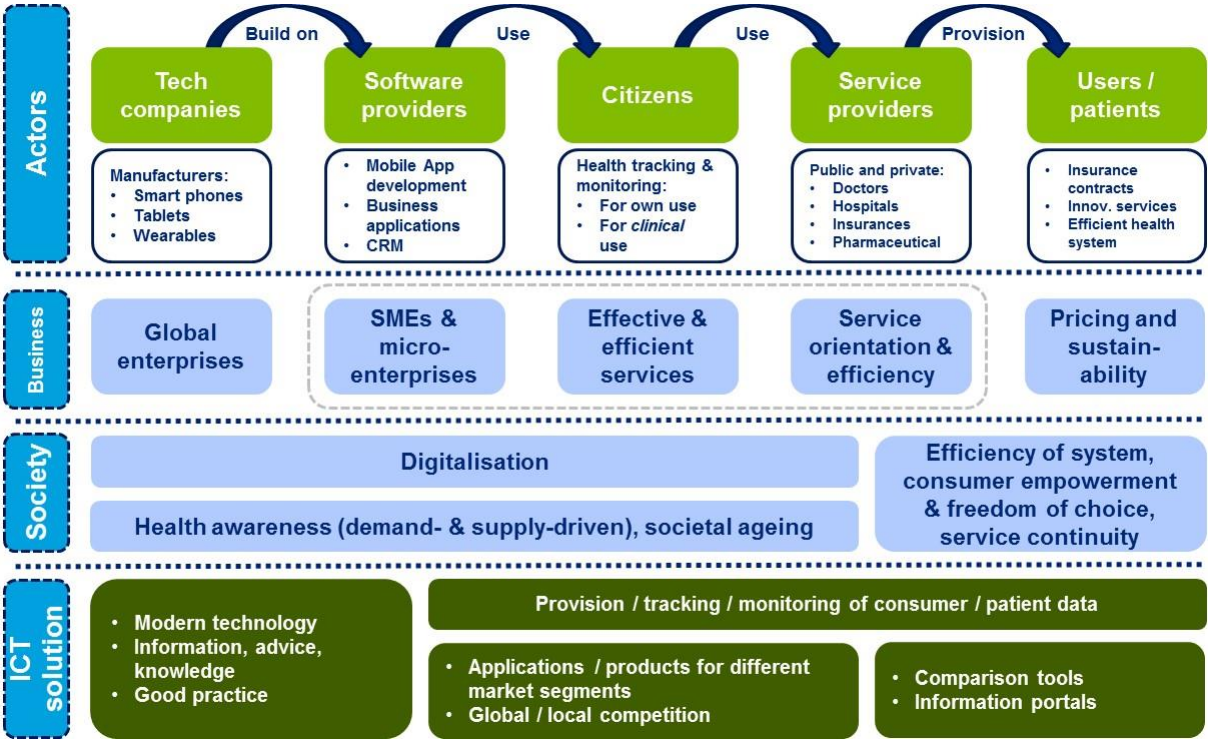
[502] Deloitte (2015): Connected health. How digital technology is transforming health and social care, p.9. See: http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf

[503] PwC Health Research Institute (2014): Health wearables. Early days. See: https://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/pwc-hri-wearable-devices.pdf

Actors, challenges, and technical solutions in the value chain

The following figure presents an overview of the actors involved within the mHealth value chain, as well as the current challenges for businesses and society that mHealth is expected to contribute to overcoming.

Figure 57: Business and societal challenges and their ICT solution in the mHealth value chain



Source: Deloitte based on the model developed by Poppe et al. (2013)[504].

The figure above outlines our understanding of the actors involved in the mHealth value chain, as well as their business models and the societal challenges these models are responding to by means of ICT solutions. The value chain ranges from device manufacturers via software and app developers to the user / consumer, who enables service providers through the use of her/his data to offer them efficient, individual, targeted products and services (rather than having to use scattergun approaches).

As stakeholders along the value chain (incl. global enterprises, as well as SMEs and micro-enterprises) build on the products and services of each other, the use and exchange of data is key to providing citizens / consumers / users / patients with added value to cope with societal challenges.

While most of the service offerings today are based on the bottom-up logic of users tracking and monitoring their own health for individual purposes, the data generated throughout this process can and increasingly will be used to tackle societal challenges such as public health and finance under the condition of societal ageing and growth.

[504] Poppe, KJ, Wolfert, S, Verdouw, C Verwaart, T (2013), Information and communication technology as a driver for change in agri-food chains, *Eurochoices*, vol. 12, issue 1.

Types of data generated and used by different actors

Looking at the types of data provided by and exchanged between businesses, three main types of actors can be distinguished. These actors provide and make use of different types of data (see the table below).

Table 32: Main types of actors along the data value chain and their respective contributions to it

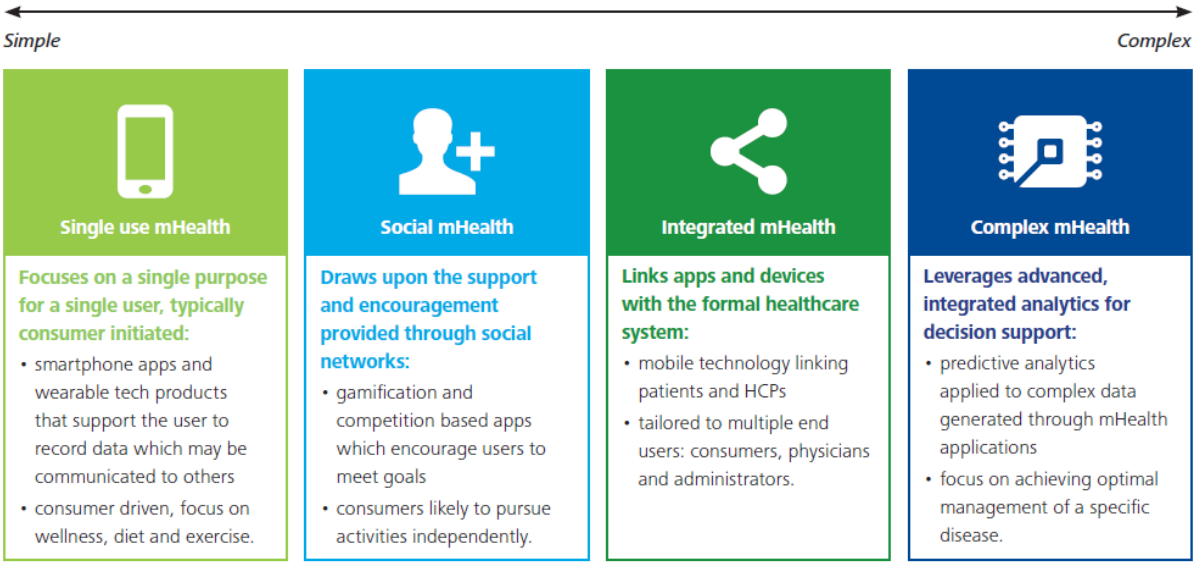
Actor	Contribution to the data value chain
Citizens / users / patients	• Provide individual, personal data by making use of mHealth applications on smart devices; • Data can be used by themselves to track and monitor health parameters in order to take informed decisions on issues such as exercise, fitness, sport, nutrition etc.; and • Patients can track the development of their disease such as diabetes, blood pressure, cardiac frequency, weight, minerals, vitamins etc.
Providers of mHealth solutions	• Develop and provide smart applications that can be used by citizens / users / patients to track and monitor individual parameters; and • Data is collected and aggregated in anonymous fashion and can be used to provide products and services for third-parties; • Examples: App developers in the B2C market, software providers in the B2B market (e.g. in relation to CRM software)
Third-party users of mHealth data	• Make use of the data provided by citizens / users / patients and aggregated by providers of mHealth solutions in order to improve the quality and the efficiency of their current products and services (short-term perspective) • Use data for research and development of new products and services (rather long-term perspective) • Examples: Insurance companies that provide tailored contracts to their clients, e.g. based on their fitness level or pharmaceutical companies that can more effectively track where any by whom their products are used and if they are used correctly.

Source: Deloitte.

These different types of actors along the data value chain, as well as their respective data contributions are closely connected – necessitating standardisation and/or interoperability along the value chain in order to provide added value to consumers and/or other businesses.[505] This is also reflected in the differentiation between **single use** and **complex mHealth**.

[505] A concise overview on the technical aspects and infrastructure involved data exchanges in typical business models involving fitness wearables and mHealth applications is presented by de Arriba-Pérez et al (2016): *Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios*, In: *Sensors*, *16* (9), 1538. http://doi.org/10.3390/s16091538

Figure 58: Range of simple to complex mHealth business opportunities

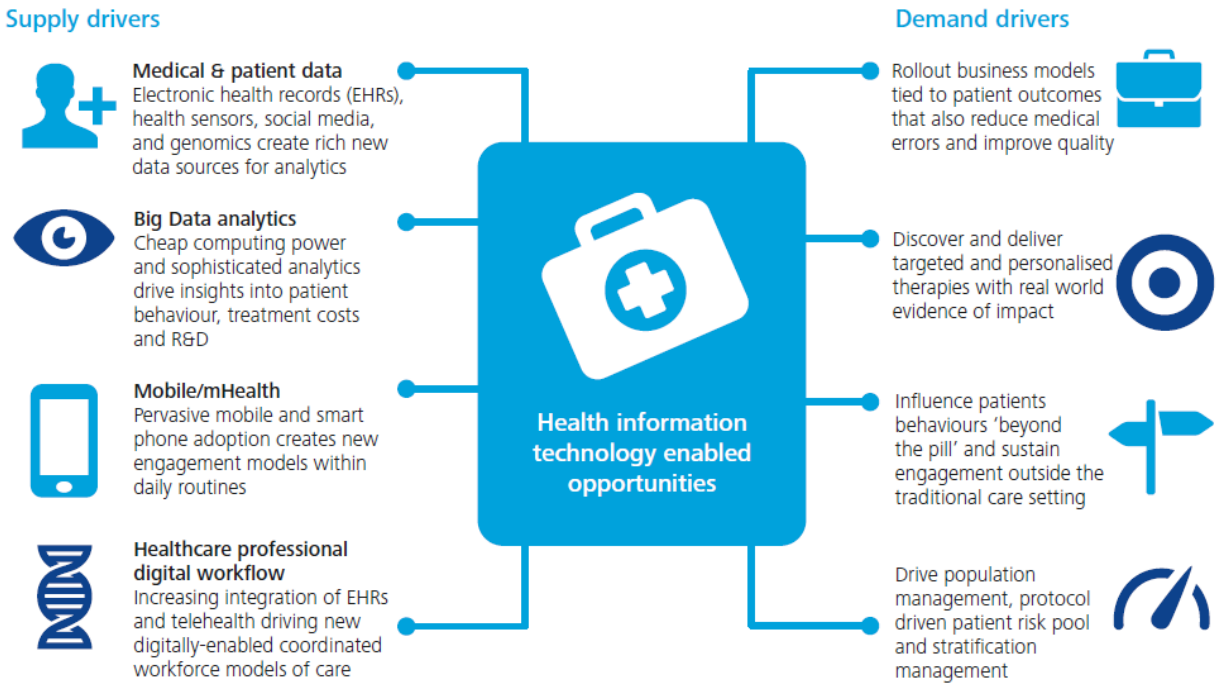


Source: Deloitte (2015).

Business model and actors: A typical service offering

In more general terms, digitalisation has enabled the development of a large number of different types of new, innovative business models circulating around supply and demand drivers. An overview of different types of business models is briefly presented in the graph below.

Figure 59: Business models in the mHealth market



Source: Deloitte (2014).[506]

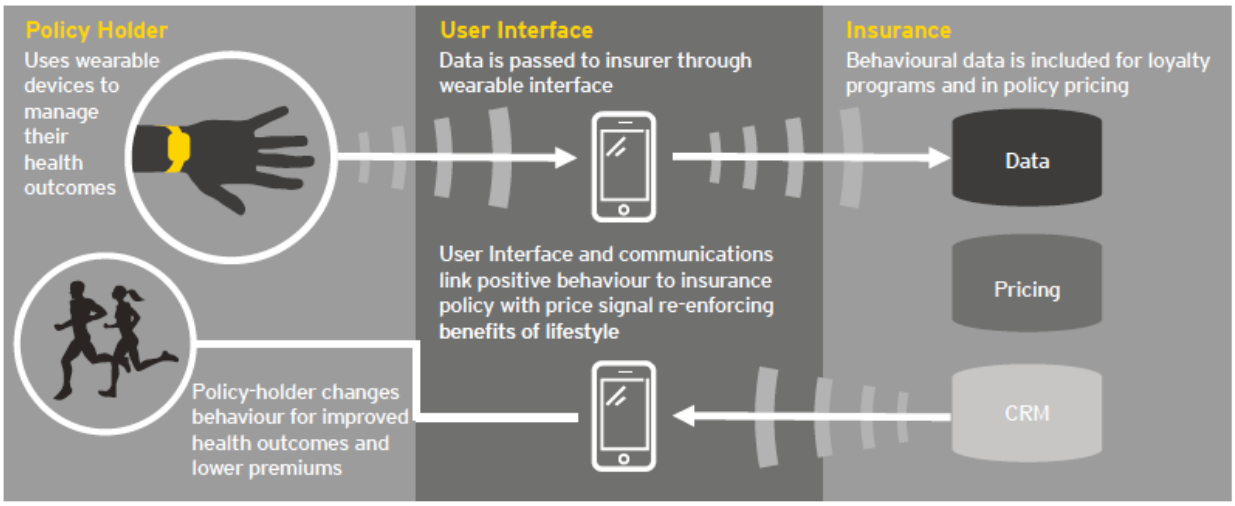
[506] Deloitte (2014): Healthcare and life sciences. Predictions 2020. A bold future? See: http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-healthcare-and-life-sciences-predictions-2020.pdf

As already indicated above, we are focussing on the mHealth market as part of this case study. More specifically, the case study covers the nexus between / the value chain of fitness apps for consumers and insurance companies.

Although numerous other examples could have been chosen for this case study, we have decided to use this example due to its straight forward use case and potential applicability in everyday life. Use cases in the area of e.g. disease treatment would have eventually been more interesting to analyse from an ethical and substantial perspective: However, the business potential and broad applicability of the issues identified and analysed as part of the value chain between fitness apps, consumers, and insurance companies have given this example the edge.

The figure below displays the basic relationship between consumers (insurance policy holders), user interface (the insurance and/or fitness app), and the insurance company that is making use of aggregated and individual data to develop targeted pricing models based on the health and behaviour of its customers.

Figure 60: Interaction between users and insurance companies in the mHealth market



Source: EY (2016).[507]

Typically, the insurance policy holder purchases two items: (1) The wearable itself; and (2) the application by means of which the health outcomes can be managed. While the former can often be associated with relatively high costs of around 100 Euro to 300 Euro depending on the device, the latter is almost always a low cost, low threshold online download.

Once downloaded, the application typically offers a set of functionalities that can be used without further payment in order to "tease" the customer. Full functionality, or extra functionality can be opened up either by "achieving" it (buzzword: gamification) or by additional payments – either monetary or in the form of personal data.

There are, however, clear boundaries with regard to the access to and (re-) use of customers' data within the EU. The privacy of the data must be ensured by service providers, i.e. data must not be used for aggregation nor by third parties without prior consent of the customer.

[507] EY (2016): PAYL. Wearable trends. How will real-time client activity and health data change your insurance business? See: http://www.ey.com/Publication/vwLUAssets/EY-wearable-trends/$FILE/EY-wearable-trends.pdf

While not all applications allow for the use of collected data for sales purposes to third parties, this is from a principle perspective possible with all applications, either at aggregated level or at the level of individual, anonymised data. In its privacy policy, *Runtastic*, for example, indicates that it "does not pass on personally identifiable information to third parties, except as required by law or with the explicit consent of the user" while "health data will never be shared with advertisers or similar agencies."[508] Although such an explicit statement cannot be found in, for instance, *Whitings'* privacy policy the company indicates that it "undertakes not to sell personal data without customers' prior agreement" and if so, only in anonymised fashion.[509]

In case data is shared with third parties such as insurance companies, it is used to develop targeted service offerings and pricing models for customers based on the big data analysis of customers' health data as part of CRM-processes. The reasoning behind this is that more and healthier customers can be attracted towards an insurance company in case lower premiums have to be paid at the individual level without having to restrict that service offering and its quality. Moreover, insurance customers using such apps are generally expected to be younger than average and to enjoy a healthier lifestyle and are thus – in particular from a cost perspective – more attractive towards insurance companies than, for instance, older citizens with chronic diseases.[510]

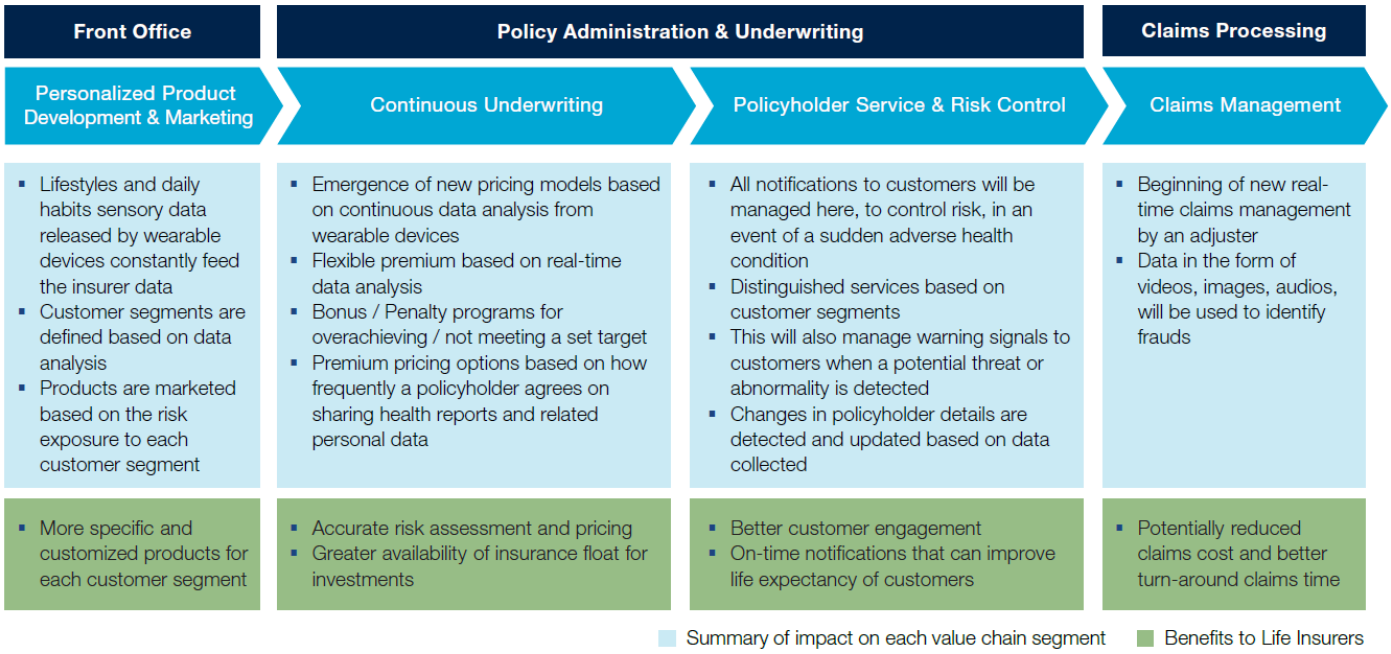
An overview of the benefits of such a business model for insurance companies is presented in the table below.

[508] See: https://www.runtastic.com/en/privacy-policy

[509] See: http://www.withings.com/eu/de/legal/privacy#a15

[510] Typically, the applications include a feedback functionality that e.g. uses positive reinforcement to engage with the app user / insurance customer in order to improve their health behaviour.

Figure 61: The nexus between the wearable ecosystem and the insurance value chain



Source: Capgemini (2015).[511]

Typically, mHealth applications and services are provided as "free" to consumers with providers compensating through other revenue sources such as data trading. Usually, consumers are not necessarily informed or unaware of how their data is being used (and by whom) and monetised. According to the Boston Consulting group, "unlike services based on direct remuneration, application-based services that are based on consumers handing over personal data are not subject to most consumer protection rules."[512]

Potential contractual barriers

This section provides a brief analysis of potential contractual barriers, businesses in the mHealth value chain may face. The section first discusses contractual barriers related to data ownership, access to, and (re-) use of data. Then, risk and liability are discussed briefly. Finally, the section includes a high-level assessment of the potential economic impact of such barriers.

Data ownership, access to, and (re-) use of data

Within the mHealth market, the ownership of data lies in principle with its generator, i.e. the user, customer, or insurance policy holder. Wearables and applications typically collect personal information such as

- **Identity data:** First and last name, home or other physical address, including street name and name of city or town, email address, birth dates, photos;

[511] Capgemini (2015): Wearable Devices and their applicability in the life insurance industry. See: https://www.capgemini.com/resource-file-access/resource/pdf/wearable_devices_and_their_applicability_in_the_life_insurance_industry.pdf

[512] Boston Consulting Group (2015): Five priorities for achieving the Digital Single Market. Commissioned by ETNO. See: https://etno.eu/datas/publications/studies/FINAL_BCG-Five-Priorities-Europes-Digital-Single-Market-Oct-2015.pdf

- **Body metrics data:** Gender, age, weight, height, pulse rates, blood pressure etc.;
- **Activity data:** Miscellaneous workout data, such as length and type of workouts; and
- **Environmental data:** GPS and other geo-location data, e.g. based on running routes of customers.

This is usually stated clearly as part of the service providers' Terms & Conditions. Therefore, data can only be processed and e.g. shared with third parties with the explicit consent of the data owner, i.e. the customer.

Depending on the service provider, access to data is ensured. *Whitings*, for instance, guarantees the easy access to and amendment of personal data (i.e. changes, additions, deletions, updates of data) while also offering the possibility to remove data by completely deleting ones' account.

Case example: Data ownership in fitness apps:

A 2014 examination of four different fitness apps (Fitbit, Jawbone, Nike+, and Basis) by researchers Greig Paul and James Irvine (University of Strathclyde) on privacy implications of wearable health devices[513] found that only "in the case of Basis, the privacy policy asserted ownership of data gathered from users, as their \sole and exclusive property. None of the other four services reviewed made a claim to user data in this manner, although Fitbit reserved the right to \use and commercially exploit" all data submitted by users to their service, with no right to privacy.

In addition, the analysis found that in all four cases, user data would be stored outside the European Union. The Terms & Conditions of Nike+, for instance, stated that they would not transfer user data outside the Nike group, unless necessary for a service provider (like shipping or payment processing).

The data collected is typically used by app providers for different purposes in relation to:

- Presentation of collected data in a user-friendly way to the customer (e.g. by means of diagrams and dashboards): This is typically the main benefit for and reasons for customers to use the applications;
- Targeted service and product offerings for existing customers based on their data (e.g. workout preferences, age, location etc.);
- Improvement of product or service e.g. based on the general take up of specific services by users, as well as the reasons not to make use of a product or service based on customers feedback;
- Analysis of aggregated data of (specific sub-groups of) customers, e.g. with a view to raise awareness of health issues, as well as scientific research and development in the area of health;
- Aggregation and sharing of data with third parties such as insurance companies based on the prior consent of data owners, i.e. the customers.

[513] Paul, Greig and James Irvine (2014): Privacy implications of wearable health devices. See: https://pure.strath.ac.uk/portal/files/38340137/Paul_Irvine_SIN14_privacy_implications_of_wearable_health_devices.pdf

Unless data owners are giving their consent and alienate their ownership and/or access rights as part of the use of services (e.g. by agreeing to certain Terms & Conditions), data cannot be shared with third parties (e.g. insurance companies). In turn, this means that in the area of mHealth, data ownership is not considered as an issue *per se* but is dependent on the individual preferences of the data owners. These preferences are determined by different factors:

- *The awareness and will of the customer:* Is the customer aware of and fine with alienating the ownership of the data? This is a personal choice by the customer that is made based by each individual based on the information available and the level of courtesy given by the customer. In this regard, transparency and clarity of Terms & Conditions, as well as the products and services themselves are crucial;
- *The parties involved:* With which types of companies / institutions along the value chain is the data shared? This resembles very closely with the first question concerning the individual awareness and preferences of the customers. For instance, the customer might be fine to share data with public authorities for general statistical purposes but not with private entities (or vice versa).
- *The purpose of the data sharing:* What should be done with the shared data? This heavily depends on the benefits companies and customers receive from sharing data. In the insurance example, companies determine "data's' value […] on their potential to be used for the greater good, such as disease prevention [while…] from a commercial standpoint, marketers want these data to gain insight into individual preferences as a means of offering personally targeted products."[514] Customers, on the flipside, provide their data and would, potentially, receive a remuneration in the form of lowered insurance premiums.[515]

Thus, ownership, access to, and (re-) use of data in the mHealth market should not be treated as issues isolated from the individual data owners. Instead, data owners should much rather be given the freedom of choice in individual situations based on a sufficient level of information presented in a user-friendly way to make an informed decision with a view to their individual preferences and benefits from data sharing.

Turning the argumentation around, however, may lead to the adverse (economic) effects for insurance policy holders that (1) do not provide their data; (2) belong to a more risk-prone group of society (e.g. in relation to certain jobs, elderly); and /or (3) are generally less healthy than others (e.g. insurance policy holders that have a chronic disease).

While insurance policy holders that provide their data to the insurance company may reap the benefit of lowered premiums, the stock of overall costs for *all* insurance customers can be expected to remain fairly equal, at least from a medium term perspective. This means that the insurance premiums of customers that do not provide their data to the company or

[514] Langley, Matthew R. (2015): Hide your health: Addressing the new privacy problem of consumer wearables. In: Georgetown Law Journal. See: http://georgetownlawjournal.org/files/2015/08/Langley-Final.pdf

[515] In this sense, the mHealth market differs from other market as, for instance, precision agriculture in which farmers typically do not receive a direct / indirect remuneration for the alienation of their data.

are less healthy need to increase quasi automatically in order to keep the necessary level of finance of the insurance company.

This means that the voluntary provision of health-related data by *some* insurance customers may have direct, detrimental effects on *other* insurance customers.

While this could generally be seen as an improvement of the economic efficiency of the insurance market, ethical questions around the appropriate level and costs for insurance are of similar importance and are less easy to grasp within the framework of this analysis.

Thus, the sharing of data is a problem of collective action, whereas it is rational for a healthy individual to share data in order to secure economic benefits in the form of lowered premiums while others insurance policy holders suffer economic detriment from information they cannot impact on themselves.

A potential solution to such a problem could evolve around a regulatory regime that governs the terms and conditions of adaptations of premiums of insurance policy holders that do not share data with their insurance provider.

Risk and liability

So far, academic literature around risk and liability issues in relation to wearables and the respective data is scarce – at least with a specific focus on the EU.

Most importantly, this is due to the still emerging nature of the market with businesses still trying to figure out how to capitalise on data sharing business models. A 2014 ITU study concludes, for example, that "mHealth is insufficiently widespread and, in the end, still in a very experimental phase."[516]

Albeit numerous applications are available on the market, personal fitness apps for instance do not necessarily capitalise on sharing data with third parties as this is seen as a potential harm to their customers and associated with a loss of consumer loyalty. Thus, in such cases, liability cannot per se be considered an issue if the data generated by the user is collected by the app developer but not shared with third-parties. This raises, however, questions in relation to the economic necessity of data sharing between businesses in general, as well as the value of data that is collected but not monetarised in order not to scare away large parts of a loyal customer base.

The mHealth market in the US is comparatively advanced, which will be discussed in more detail as part of section 0. Yet in an argument that may be transferred to the European context, Nicolas Terry and Lindsay Wiley come to the conclusion that existing doctrines of tort and privacy law may be adequate to address the "development, use, recommendation, and

[516] ITU (2014): Filling the Gap: Legal and Regulatory Challenges of Mobile Health (mHealth) in Europe. See: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/ITU%20mHealth%20Regulatory%20gaps%20Discussion%20Paper%20June2014.pdf

prescription of mobile health products".[517] Liability issues are considered as likely to occur in the future mHealth market.[518] Given that the market is still at a very early stage of development, professional practices (e.g. by healthcare professionals, third-party companies) have not yet emerged as take up and marketing of technology is still considerably low (given the potential). Right now, consumers "drive the processes of choosing and using mobile apps."[519] Thus, in the B2C context, it is essentially the consumers who get to choose what products and services to use and when – or to abstain from its use.

The authors proceed to argue that, as long as the extent of a product manufacturer's liability in relation to privacy and security breaches, is an open question, it is crucial to test apps and wearables for effectiveness against current established baselines in order to safeguard customers in the B2C and B2B context from potential harm and detriment.

While there is "little doubt that product liability models would apply to health information technology devices and their mobile extensions"[520], such tests and safeguards can be implemented as part of certification procedures "to ensure that apps do not pose potential harm to their users or have significant security and privacy vulnerabilities."[521]

In addition, the available literature emphasises the need for 'informed consent' as a precondition for liability involving the recommendation or curation of health apps, e.g. by insurance companies.

Thus, even though the argumentation of Terry and Wiley is based on the current legal regime in the US, important comparisons can be drawn to the EU. For instance, as also shown in relation to the precision agriculture market, the development, implementation and use of certification schemes and/or professional standards in order to avoid product liability issues in the B2B context might be a step forward without putting potential growth and innovation at risk through the adoption of a regulatory framework that might tackle current barriers while disregarding emerging issues that cannot be foreseen at this stage.

Similarly as in the US, the EU Product Liability Directive might also be applicable to mHealth devices in the EU B2B context. In addition, as step was made to establish sector specific rules with the *EU Medical Devices Directive*, described in the textbox below.

---

[517] Nicolas P. Terry and Lindsay F. Wiley (2016): Liability for mobile health and wearable technologies. In: Annals of Health Law (25), p. 62-95. See: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725450

[518] Especially so since for example the vast majority of fitness apps are not curated, sold or implemented by HIPAA[518] 'covered entities' but by technology companies and sold through app stores, as Terry and Wiley note. Therefore, insurance companies who might recommend the use of fitness and other health care apps face liability issues in case inaccurate data leads to incorrect prescription plans, healthcare recommendations, or price offerings. Similarly, they expect that "arguments will be made that fitness and wellness apps recommended either over-exercise or under-exercise, and it is unlikely to be long before some plaintiff alleges a new syndrome such as *exercise addiction*. Other quantified-self apps have faced such exposure"

[519] Ibid. p. 83.

[520] Nicolas P. Terry (2015): Mobile Health and Wearable Technologies: Systemic Liability. See: http://www.aaas.org/sites/default/files/Terry%20Mobile%20Health%20and%20Wearable%20Technologies%20Systemic%20Liability.pdf

[521] Ibid. p. 92.

The EU Medical Devices Directive:

The EU Medical Devices Directive[522] lays down procedures for evaluating conformity of medical devices with different essential requirements based on the risks that they may pose to patients, users, and if applicable, other persons.

According to its Art. 1, a medical device is defined as any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings […].

Under the EU Medical Devices Directive, there are four classes of products in relation to which different types of liability regimes apply, incl. e.g. a procedure for which the manufacturer is solely liable based on the low degree of vulnerability of the medical devices in question (class I).

According to ITU, "software designed for diagnostic and/or therapeutic purposes that may be downloaded to a mobile telephone meets or may meet the [preceding] definitions and, consequently, may lie within the scope of the Directive of 14 June 1993."[523]

Proposals for a replacement of the EU Medical Devices Directive have been submitted to the European Parliament and the Council in 2012 but have not yet been adopted.[524]

However, ITU for example argues that the "European institutional and legal landscape is too fragmented as it is largely dominated by individual Member State jurisdictions. Accordingly, operators are confronted by what appear essentially as national legal obligations (when they are not imposed on sub-national levels). No attempt at harmonization or consistency has yet been made in the systems – for example a system of mutual recognition for national approvals. All operators are thus quite cognizant of the need to harmonize rules on a Europe-wide, if not worldwide basis."[525]

ITU proceeds to propose already three principles for future consideration in the mHealth market, incl. an active cooperation among the States which remains a fundamental principle within the European Union, as well as the principle of reciprocity that the EU Member States have applied in the domain of protecting personal information.

[522] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1). See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF

[523] ITU (2014): Filling the Gap: Legal and Regulatory Challenges of Mobile Health (mHealth) in Europe. See: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/ITU%20mHealth%20Regulatory%20gaps%20Discussion%20Paper%20June2014.pdf

[524] See: http://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework/revision_de

[525] ITU (2014): Filling the Gap: Legal and Regulatory Challenges of Mobile Health (mHealth) in Europe. See: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/ITU%20mHealth%20Regulatory%20gaps%20Discussion%20Paper%20June2014.pdf

Conversely, the European Economic and Social Committee argued in 2014[526] that there is a need to:

- Regulate, by means of regulation, a) "mHealth", in line with the established definition of "healthcare"[527] and b) safety and wellbeing apps.
- Because it is not covered by current legislation, consideration should be given to the issue of cross-border healthcare.
- Aims: a) to give legal certainty to manufacturers; b) to provide guarantees for both professionals and users; c) prevent the marketing of ineffective or dangerous products.

In addition, EESC argues that risks posed by the use of mHealth solutions in relation to whether contractual or non-contractual liability could best be mitigated by applicable law under the Patients' Rights Directive[528], Art. 4(1)), as well as in relation to defective products under the Product Liability Directive (PLD)[529] under the principle of liability without fault.

The European Commission's public consultation on the Green Paper on Mobile Health[530] has revealed that "safety and performance requirements of lifestyle and wellbeing apps are not adequately covered by the current EU legal framework, according to a clear majority of respondents." In addition, respondents indicated that specific regulation on lifestyle and wellbeing apps would be needed to tackle the current legal vacuum, as well as guidance (soft-law), and quality labels or certification schemes to ensure the safety and performance of lifestyle and wellbeing apps.

Furthermore, the public consultation revealed that medical solutions typically pose a greater risk to patient safety and health than lifestyle solutions. According to the Commission, the logical conclusion is that medical interventions should be more strictly regulated than it is presently the case.[531] It was also emphasised that manufacturers need to have a clear understanding of their liability when designing mHealth solutions. This requires a clear legal framework with adequate guidelines to help manufacturers and developers assess easily with what rules they have to comply.

[526] European Economic and Social Committee (2014): TEN/551 EU Framework on "mHealth" and "health applications and wellbeing apps".
[527] See Article 3 a) of Directive 2011/24/EU on cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
[528] Directive 2011 /24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45). See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:en:PDF
[529] Directive 85/374/EEC on liability for defective products. See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN
[530] See: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-green-paper-mobile-health
[531] Mobile solutions, which have a medical purpose, fall within the scope of the medical devices directives, currently under review. See SWD accompanying the Green Paper on mHealth.

Potential non-contractual barriers

Already in 2012, ITU has emphasised that "a lack of interoperability is one of the greatest threats to achieving the improvements to healthcare and cost efficiency promised by emerging e-health systems."[532]

According to ITU, lack of interoperability is both:

- A technical barrier; and
- A market-driven barrier.

Other barriers can, for example, relate to sensing and data collection hardware to collect physiological and movement data, as well as the communication hardware and software to relay data, e.g. to a remote centre.[533] Such technical barriers are, however, not subject of this case study.

Technical barriers

As part of the European Commission's public consultation on the Green Paper on Mobile Health[534], stakeholders have supported the actions proposed in the eHealth Action Plan[535] and the need to foster the use of international standards (e.g. in cooperation with Continua/ ITU-T, IHE profiles, HL7, IEEE and SNOMED CT). In addition, stakeholders emphasised the need to develop an EU eHealth Interoperability framework while being divided however on whether it should be made mandatory by EU legislation, or not (i.e. open standards). Moreover, according to the results of the public consultation, there is a need to promote and further develop testing and certification schemes in order to enable suppliers to test the interoperability of their solution with others.

These findings are also largely supported by the European Economic and Social Committee that recommends to prioritise establishing a list of medical devices, ethical principles, and data protection and interoperability provisions.[536] This also includes the establishment of reliable and secure mechanisms for transferring medical data by means of medical devices as data volumes are doubling every 18 months, and growth at this pace means that standards are essential. According to the EESC, standards have different functions in different healthcare fields, but interoperability standards – implemented as part of the European In-

[532] ITU (2012): E-health Standards and Interoperability. ITU-T Technology Watch Report. April 2012. See: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000170001PDFE.pdf

[533] See: http://www.zwmb-stahn.de/uploads/1/4/6/4/14643218/_presentation_tiemann_wearabl_technology.pdf

[534] This relates to establishing the semantic and technical cross-border interoperability specifications and assets necessary for the eHealth Interoperability Framework, as well as to propose an EU interoperability testing, quality labelling and certification framework for eHealth systems.
See: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-green-paper-mobile-health

[535] See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0736&from=EN

[536] European Economic and Social Committee (2014): TEN/551 EU Framework on "mHealth" and "health applications and wellbeing apps".

teroperability Strategy – are the cornerstone of usable interfaces between disparate systems.

Technical barriers are also of importance in view of liability claims for defective products under the Product Liability Directive (PLD).[537] Here again, as argued in the precision agriculture case, businesses in the B2B context do not seem to accept the liability without fault conditions but much rather rely on product safety regimes (pre-market testing / certification schemes) that are based on interoperable solutions than contractual liability regimes.

Hence, interoperability between products and services can also be regarded as a means to preclude liability claims in the B2B context in case the end-consumer suffers damage.

Market driven barriers

With regard to market driven barriers, ITU argues that those arise from the economic competition inherently occurring among companies seeking to profit in emerging and extremely lucrative e-health industries, and the lack of incentives among healthcare delivery systems to adopt standards.

In essence, this means that incumbent market players provide non-interoperable solutions to their clients in order to leverage lock-in effects while the market is still a an early stage of development. This mechanism can be observed, for instance, with regard vendors that impose their standards on app developers in order to be able to sell them via large app stores.

However, as also argued in the precision agriculture case, interoperability improves customer experience[538] and is therefore crucial to the success of products on the market. It could be argued that, due to an increasing number of actors along the data value chain – especially SMEs and consumers – generally reluctant to commit themselves to only one service provider, businesses that do not provide for interoperable, vendor neutral description formats will – in the medium run – face challenges regarding their customer base and, most likely, be pushed out of the market (e.g. through competition or through acquisition by larger market players).

Excursion: Digitalisation in the US healthcare sector

Compared to the European Union, the ecosystem surrounding the use and exchange of data between healthcare actors is more developed in the U.S. market. Similarly, the quantity and quality of B2B data exchanges in health-related markets is also much higher, as the textbox below explains for the case of fitness apps.

US Federal Trade Commission study on health apps:

According to Federal Trade Commission (FTC) findings, health apps are in fact transmitting sensitive health information to third parties. On May 7, 2014, the FTC released a study of

[537] Directive 85/374/EEC on liability for defective products. See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31985L0374&from=EN

[538] This means that, for instance, newly purchased devices by a certain manufacturer can be used with already purchased hard- and software from other providers

twelve different health and fitness apps. The study found that those apps transmitted user data to seventy-six different third parties, including advertisers. The information transmitted varied all the way from device information to exercise routines, dietary habits, and symptom searches. In a few instances, even names and addresses were being transmitted.[539] The names of the apps under scrutiny were not disclosed.

The higher market maturity enables further insights into possible barriers for data exchanges in RTLS and wearable contexts. This section illustrates some notable differences in market environment and summarises the experiences from a larger evidence base.

The first notable difference between the two markets is that the exchange and use of data in the healthcare system has been actively promoted by the U.S. government. The explicit objective is to reduce the overall costs in the U.S. health care system, while improving treatments and enabling informed choices of patients.[540] The *Open Government Initiative* launched in 2009, led to the establishment of a nationwide platform containing health data in 2011.[541] Today, *healthdata.gov* grants access to more than 3,000 datasets containing information on the quality of clinical care providers, community health performance information and government spending data as well as a nationwide health service provider directory and databases of the latest medical and scientific knowledge.[542] Users of this data include a variety of public and private companies, including insurance providers or analytics companies, as well as scientific researchers.[543]

Data exchanges are also encouraged on the state level: Around 45% of U.S. hospitals are participating in regional and local Health Information Exchanges (HIE). For instance, around 80 hospitals in Indiana share their information on more than ten million patients. Datasets include clinical data, costs incurred per patient, as well as data on patient sentiment or pharmaceutical R&D processes. More than 18,000 physicians may access and use this data to improve treatments.[544]

Experiences with RTLS applications in U.S. hospitals

Another notable difference between the two regions are higher adoption rates of RTLS: North America is the largest market for this technology and most of the relevant companies are from the U.S.[545] For instance, a growing number of hospitals is using RFID technology to track inventory, patients and sometimes even staff performance. Several case studies (pre-

[539] Federal Trade Commission (2014): Spring Privacy Series: Consumer generated and controlled health data. See: http://www.ftc.gov/system/files/documents/public_events/195411/consumerhealth-data-webcast-slides.pdf#page_22.
[540] McKinsey (2013): The big-data revolution in US health care: Accelerating value and innovation.
[541] European countries appear to have been far more reluctant to promote exchanges of (public) health data, as Eugene Borukhovich and Katarzyna Rabczuk note in their assessment of the state of play in 2013; see http://openhealthdata.org/post/41348924369/open-health-data-international-snapshot#tumblr_notes
[542] https://www.healthdata.gov/content/about
[543] Example cases from the sectors healthcare, insurance and scientific research are provided by the Open Data 500 project, an initiative studying emerging business models and use cases using open government datasets; see http://www.opendata500.com/us/list/
[544] McKinsey (2013): The big-data revolution in US health care: Accelerating value and innovation.
[545] http://www.marketsandmarkets.com/Market-Reports/real-time-location-systems-market-1322.html

dominantly provided by RTLS providers) confirm that several benefits identified in section 0 materialise in practice.[546]

In a recent study, Robinson et al. reviewed the implementation and performance of RTLS-systems in U.S. hospitals. They identify three notable barriers. The first barrier encountered is related to the topic of **data ownership and (re-) use**, especially personal data of employees. Whereas the implementation of systems that track inventory and supplies was largely welcomed by staff, the tracking of staff movements, productivity and "customer service orientation" was answered with hostility.[547]

Second, **technical barriers** included reduced signal strength and possibly low data quality in certain buildings. Even though close-range RFID tracking proved successful, long-range methods using other technologies remain a challenge because of antenna technology and layout. While this could result in important inventory still not being found in critical situations, this has not been reported as a possible source for **liability** disputes so far. Interoperability, likewise, was not mentioned as a source of barriers. [548]

Other barriers inhibiting collection and exchange of data are related to the cost of setting up hardware and software, as well as staff training. This seems to affect mostly small to medium sized hospitals; case studies so far only provide examples of large and very large hospitals adopting the technology.

Wearables and the U.S. insurance market

The U.S. market has so far seen several attempts by insurance companies to launch special plans and programs for customers willing to share data in return for individualised treatments and financial gains.[549] Start-ups like New-York-based *Oscar* began experimenting with performance based rewards in 2014: Insurance holders were able to use *Misfit* wristbands to track a certain (increasing) number of steps over extended periods of time. In return, they were offered gift cards for online shops. Most insurers so far use wearables rather as a part of rewards programmes and not as a tool to compute highly personalised risk premiums. However, analysts expect this to change in the future.[550]

Traditional insurance companies tried to establish their own data platforms to collect and exchange patient data as early as 2012. These attempts saw mixed results: *Aetna's Carepass* platform aggregated customers' personal health information from various sources (without exchanging it with third parties), whereas *Kaiser Permanente's Interchange* open API aimed

[546] See for example http://resources.impinj.com/h/i/229784245-hospital-supply-management-case-study-university-of-tennessee-medical-center/76992; https://www.rfidjournal.com/purchase-access?type=Article&id=12728&r=%2Farticles%2Fview%3F12728

[547] Robinson J., Starr, J., Vasss, J. (2016): Implementation of Radio-Frequency Identification in Hospitals, http://bakercenter.utk.edu/wp-content/uploads/2016/04/Implementation-of-RFID-in-Hospitals.pdf

[548] Ibid.

[549] http://www.mobihealthnews.com/22779/how-kaisers-interchange-differs-from-aetnas-carepass/

[550] See https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#3f7876ef18bd

at utilising non-personal health related data.[551] While *Carepass* was discontinued in 2014, *Interchange* still exists to assist and encourage users' healthy life choices. The company claims that information regarding nutrition or activity provided through apps based on *Interchange* has improved cardio-vascular disease prevention and produced an estimated 1 billion USD in savings (e.g. via reduced numbers of doctor visits).[552].

Obstacles in practice: The case of Aetna's Carepass[553]

The U.S. insurance provider Aetna, selling traditional and consumer directed healthcare insurance plans, launched its *Carepass* mHealth platform in 2013. The service integrated data from wearables, health records and encouraged users to maintain a healthy lifestyle. The platform maintained collaborations with a large number of mHealth devices and software developers.[554] It targeted insurance holders at first and was later opened to the general public. Facing low user numbers and low returns on investment, the platform was decommissioned and partly integrated into other products by the end of 2014. No official reasons for the end of the service were disclosed.

Nevertheless, business analysts from the industry insider website *mobilehealthnews.com* offer some insights on the barriers the service faced. First, despite the efforts to collaborate with other companies, significant challenges for **interoperability** remained. As *Carepass* integrated statistics and measurements from other mHealth apps, their respective developers had a strong incentive to loosen those ties once they had reached a critical mass of users (in order not to cannibalise their own app). This uneasy truce was aggravated by the fact that *Aetna* lacked the weight of companies like *Apple* or *Google*: Their later platforms were deeply integrated into the operating systems of users' smartphones and wearables.

At the same time, the company was reluctant to integrate their platform into the existing healthcare infrastructure due to possible regulatory burdens. Therefore, users faced significant obstacles to transfer and integrate data from *Carepass* into their *Electronic Health Record*. Given this parallel infrastructure, potentials for insights through **(re-) use of data** were never realised. The platform was mainly aggregating the data from different sources but did not provide more insights through analytics to customers.

Finally, besides questions of usability and added value, the collective action problem discussed in the previous section on **data ownership** was identified as one of the biggest challenges. Privacy concerns may have deterred many possible users, fearing higher future premiums if they would not meet goals negotiated as part of their health care plans today.

Increasingly, U.S. employers offering health care coverage or wellness programs are interested in wearables as part of their collaboration with insurers: One wellness program pro-

[551] http://www.mobihealthnews.com/22779/how-kaisers-interchange-differs-from-aetnas-carepass/
[552] McKinsey (2013): The big-data revolution in US health care: Accelerating value and innovation.
[553] http://www.mobihealthnews.com/36172/10-reasons-why-aetna-carepass-failed
[554] Partners included like *MapMyFitness*, *LoseIt*, *RunKeeper*, *Fooducate*, *Jawbone*, *Fitbit*, *fatsecret*, *Withings*, *breathresearch* (MyBreath), *Zipongo*, *BodyMedia*, *Active*, *Goodchime!*, *MoxieFit*, *Passage*, *FitSync*, *FitBug*, *BettrLife*, *Thryve*, *SparkPeople*, *HealthSpark*, *NetPulse*, *Earndit*, *FoodEssentials*, *Personal.com*, *Healthline*, *GoodRx*, *GymPact*, *Pilljogger*, *mHealthCoach*, *Care4Today*, and *meQuilibrium*, see: http://www.mobihealthnews.com/35976/exclusive-aetna-to-shut-down-carepass-by-year-end

vider reports that up to 50% of their corporate customers use trackers. However, due to privacy concerns, most companies choose to make wearables a purely optional feature of programs and entrust third parties to process data and administer benefits.[555] One recent example of such an initiative is the cooperation between IT-firm *Qualcomm* and insurer *UnitedHealthcare*, rewarding employees using wearables to monitor activity and exercise. On behalf of several employers, *UnitedHealthcare* already administers this and several similar programmes covering more than 10,000 employees.[556]

Returning to the points made in section 0, these adoption rates are able despite the fact that "the vast majority of health apps are not curated, sold or implemented by HIPAA[557] 'covered entities'; they are built by technology companies and sold through app stores. As a result, much of the fitness and health data collected by mobile apps and wearables have very thin legal protection."[558] According to the Nicolas Terry, the same holds true for mobile platform healthcare data aggregators and APIs such as those offered by *Apple* with its "*Health*" app. Therefore, institutional providers such as insurance companies who recommend the use of fitness and other health care apps might face liability issues in case the data collected is not accurate as it should ideally be – which could lead to incorrect prescription plans, healthcare recommendations, and price offerings.

Thus, in the future, "plaintiffs' attorneys no doubt will consider a plethora of product liability allegations against app developers, wearable manufacturers, and their distributors".[559] It is anticipated that "arguments will be made that fitness and wellness apps recommended either over-exercise or under-exercise, and it is unlikely to be long before some plaintiff alleges a new syndrome such as *exercise addiction*. Other quantified-self apps have faced such exposure."[560] Nevertheless, existing doctrines of privacy and tort law are argued to be adequate to ensure adequate remedies for damages incurred by consumers. In addition, the U.S. Food and Drug Administration (responsible for regulating medical devices) has reacted to the emerging market by providing guidance on minimum standards for digital health devices and applications.[561]

Main findings relating to the health sector

Overall, the two cases presented share two features: First, both cases describe emerging markets at a very early stage of development regarding business models and exchange relations. Even within the more mature U.S. market, applications and cooperation between

[555] https://www.wsj.com/articles/as-wearables-in-workplace-spread-so-do-legal-concerns-1457921550

[556] https://www.forbes.com/sites/brucejapsen/2016/03/01/unitedhealth-qualcomm-launch-wearable-device-coverage-plan/#559bdeea3a3f

[557] HIPAA stands for the US 1996 *Health Insurance Portability and Accountability Act. See:* http://www.hhs.gov/hipaa/

[558] Nicolas P. Terry (2016*): Regulatory disruption and arbitrage in healthcare data protection*. In: Yale Journal of Health Policy, Law, and Ethics, Vol. 17. p. 37. See: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2774471&download=yes

[559] Nicolas P. Terry and Lindsay F. Wiley (2016): Liability for mobile health and wearable technologies. In: Annals of Health Law (25), p. 87. See: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725450

[560] Ibid

[561] See: https://www.fda.gov/MedicalDevices/DigitalHealth/default.htm

hardware and software, as well as health care providers may be described as isolated and fragmented.

Second, personal and machine generated data are hard to separate in healthcare contexts. As a result, a number of barriers identified in this study are more related to privacy concerns: User consent and user acceptance of **ownership** structures around **transfers, uses and (re-) uses** of their data may be a very sector-specific barrier to free exchanges. The excurse to the U.S. market shows that the insurance market is especially affected by collective action problems associated with data collection and (re-) use. Here, users shy away from exchanges for fears of future disadvantages in social and economic terms. This is not the case in RTLS applications, which concern mostly non-behavioural data gathered in very specific, isolated situations.

The main barrier identified across both case studies concerns **interoperability**: Because of the early stage of development RTLS markets, systems have been very much tailored to specific, closed contexts (hospital IT-systems). Likewise, close cooperation between individual device manufacturers or data service providers and insurance companies appear to be the norm. As a result, proprietary platforms and data formats are common, possibly promoting the development of monopolies in specific applications. Stakeholders may not integrate systems of different manufacturers and are not aware of good practices or which application or system is suited for their present and future needs. Standards for data exchange interfaces, certification and testing are considered crucial by stakeholders in both contexts.

Standards for pre-market testing and enhanced interoperability are expected to affect **liability** questions (as a possible future barrier) as well. Exercise or treatment decisions based on faulty primary or interpreted data may result in compensation or medical malpractice law suits. On the one hand, defining standards for design and testing of products and services (e.g. as part of a new EU Medical Devices Directive) could prevent or reduce the occurrence of liability disputes. On the other hand, insights from the cases and academic literature suggest that liability questions may be adequately addressed through existing privacy and product liability regimes (e.g. the EU Product Liability Directive). In this regard, informed (and meaningful) user consent to terms and conditions is emphasized.

Annex 3 – Surveys' results

This Annex contains a summary of the data emerging from the two surveys carried out for this assignment and especially the general survey and the specific (or targeted) survey.

Analysis of the general survey

This annex provides an analysis of the general survey with companies conducted via computer-assisted telephone interviews. The survey was conducted by GDCC[562].

First, an overview of the survey's target group and its current response rate is presented, followed by an explanation of the structure and content as well as a discussion of the results.

The general survey was conducted from March-April 2017. As the web-based specific survey presented in the following chapter it is related to the use of data within and between businesses, covering the following main issues:

- Relevance of accessing/sharing data within the business model;
- Main barriers to accessing and/or sharing data;
- Costs related to accessing and/or sharing data; and
- Liability problems with accessing and/or sharing data.

The general survey and the specific survey are both based on the same questionnaire.

Basic information about the survey respondents

In total, the survey was filled in by 152 **respondents representing companies across several sectors and Member States**. Companies from 7 Member States (Austria, Belgium, Cyprus, Germany, Finland, France and UK) participated in the survey. Overall, 27% (41) of these companies operate in more than one country (see below).

Table 33: Share of companies operating in more than one country

Does your company operate in more than one country?		
Answer Options	**Response Percent**	**Response Count**
Yes	27,0%	41
No	72,4%	110
Answered Question		**152**

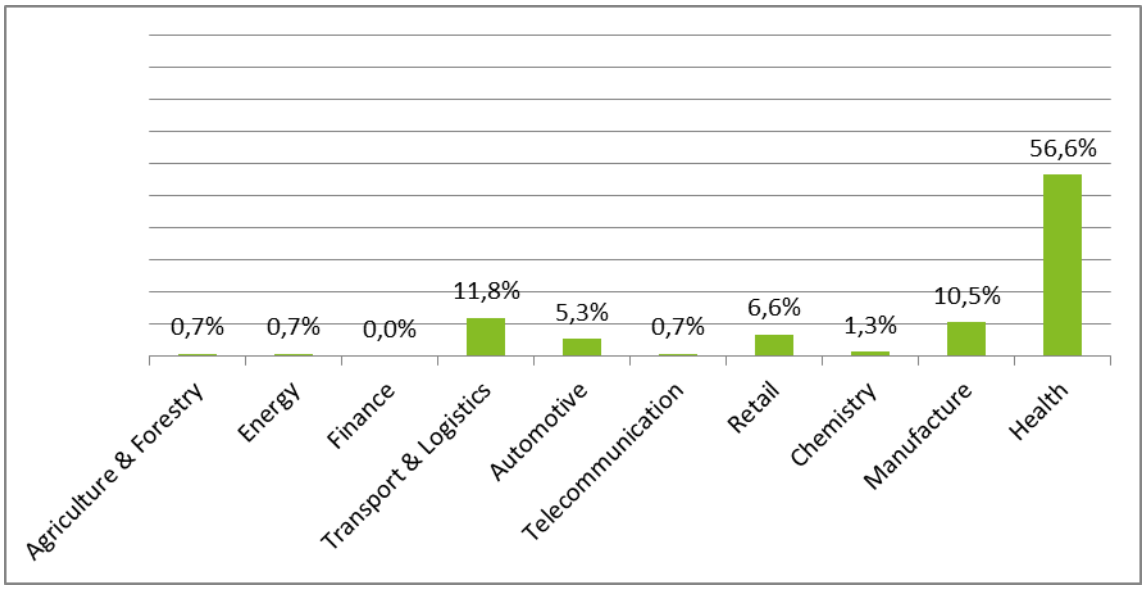
Source: Deloitte

The figure above provides an overview of the sectors in which the companies are situated. The majority of respondents, 56,6%, is active in the health sector. Moreover, 11,8% of respondents operate in Transport & Logistics and 10,5% in Manufacturing. The comparatively

[562] http://www.gdcc.com/nl/

large response rate form the health sector may be because these sectors are usually the main focus of the discourse about digitisation and assumed to experience the greatest problems as regards data access and (re-) use. Other sectors mentioned by participants are, amongst others, Retail and Automotive.

Figure 62: Sectors in which participating companies operate



Source: Deloitte

Data analytics companies account for 7,3% (11) of respondents, compared to 92,7 (140) that work at a company mainly offering non-data driven goods and services.

Table 34: Share of data analytics companies

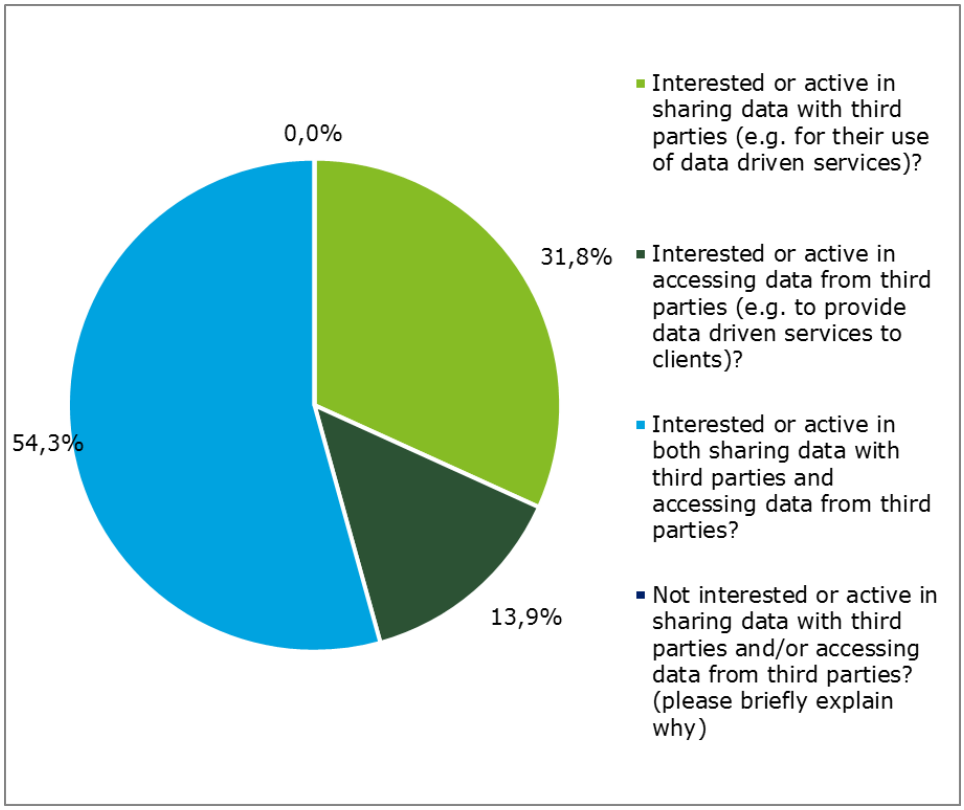
Is your company a data analytics company?		
Answer Options	**Response Percent**	**Response Count**
Yes	7,3	11
No	92,7	140
Answered Question		**151**

Source: Deloitte

Participants were also asked about the nature of their interest in data: whether they are interested in accessing data, sharing data, both, or not at all interested in data.

As demonstrated in the figure below, approximately a third of respondents (31,8%) is interested in sharing data with third parties while only 13,9% of companies are interested in both the access and sharing of data. A majority of 54,3% of respondents is interested or already active in both sharing and accessing data.

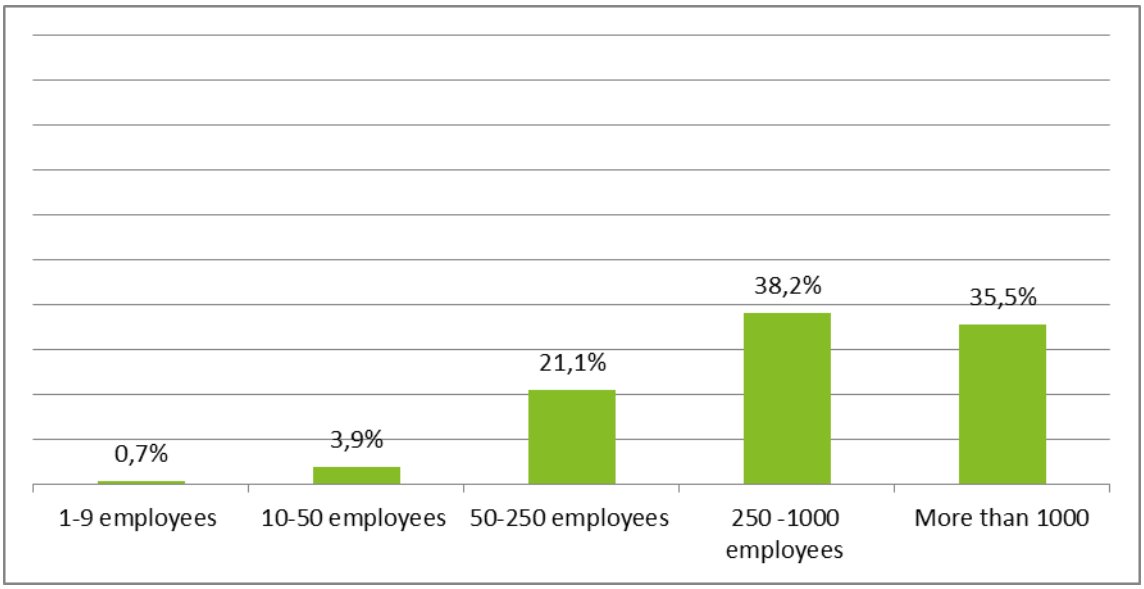
Figure 63: Company's interest in data (n=151)



Source: Deloitte

As concerns the size of the companies, small companies with less than 250 employees account for a quarter of the respondents as can be inferred from the figure below.

Figure 64: Company size (n=152)



Source: Deloitte

As regards growth rates, around 21,1% of the companies experienced a 10% growth annually either in people or revenue over the past 3 years, compared to 68% that did not experience such development.

Table 35: Share of companies with 10% growth

Has your company experienced a 10% growth annually either in people or in revenue in the past 3 years?		
Answer Options	**Response Percent**	**Response Count**
Yes	21,1%	32
No	68,4%	104
I do not know	9,9%	15
Answered Question		**152**

Source: Deloitte

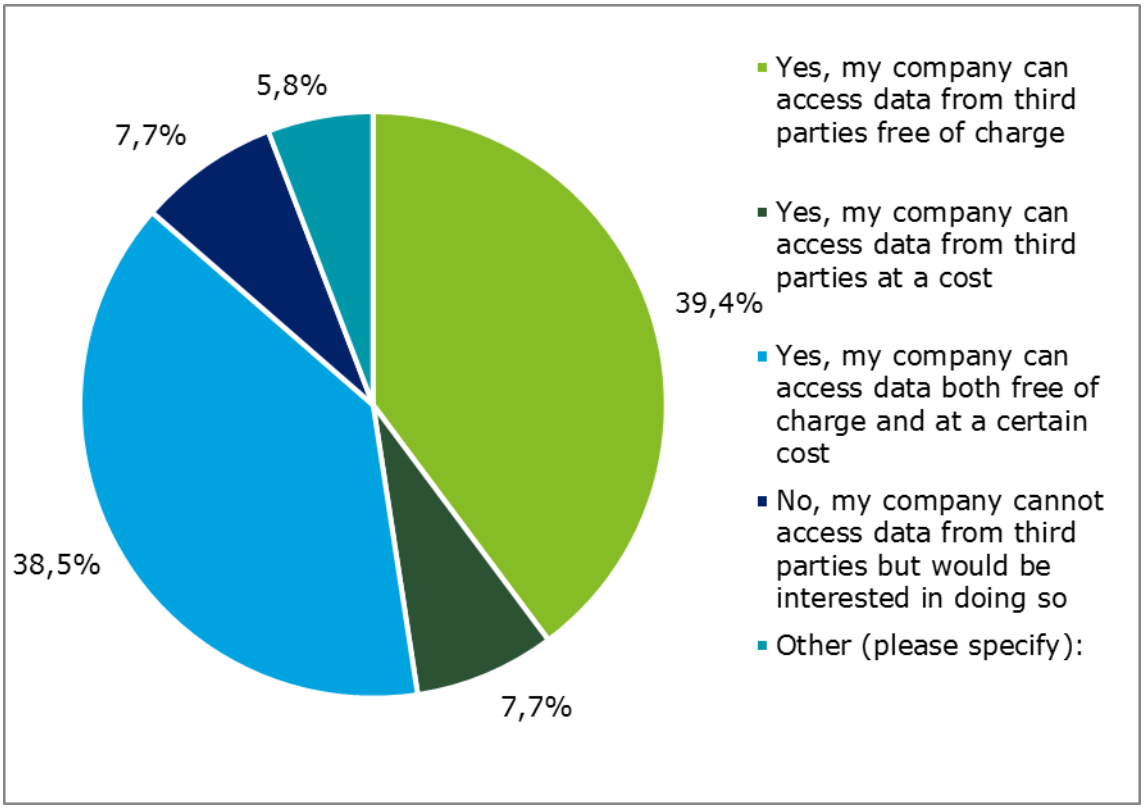
Data access

In the following, the results of questions concerning the **access to data** will be presented. The chapter contains results from respondents in total and from companies that **are interested or active in accessing data from third parties** and from companies that are **interested or active in both sharing data with third parties and accessing data from third parties**.

Relevance of accessing data within the business model

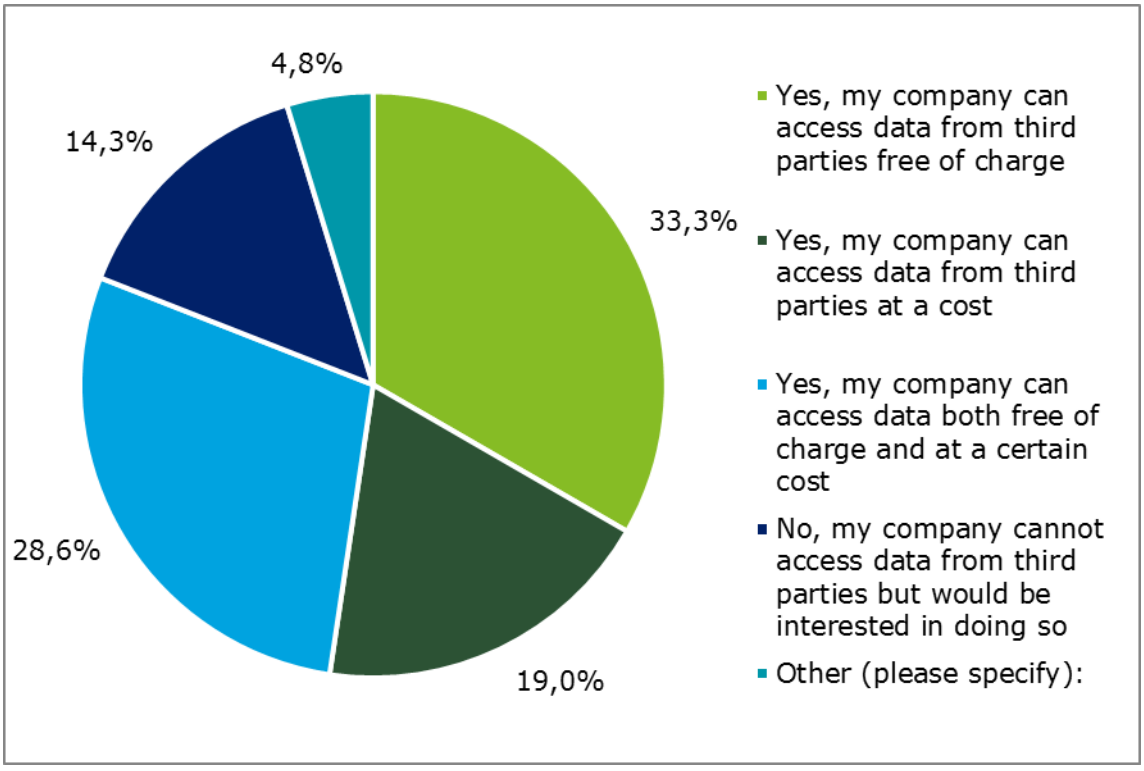
Participants were asked a set of questions relating to the relevance of accessing data. First, participants are asked whether they can access third party data or not. The figure below shows the share of respondents whose companies are only interested in data access. 39,4% of participants indicated that their company can access data from third parties free of charge. 7,7% pay for accessing data held by third parties. 38,5% can access data either for free or at a certain cost. 7,7% are **not able to access** the data they want to obtain – neither for free, nor at a cost.

Figure 65: Characteristics of access to data (total respondents, n=104)



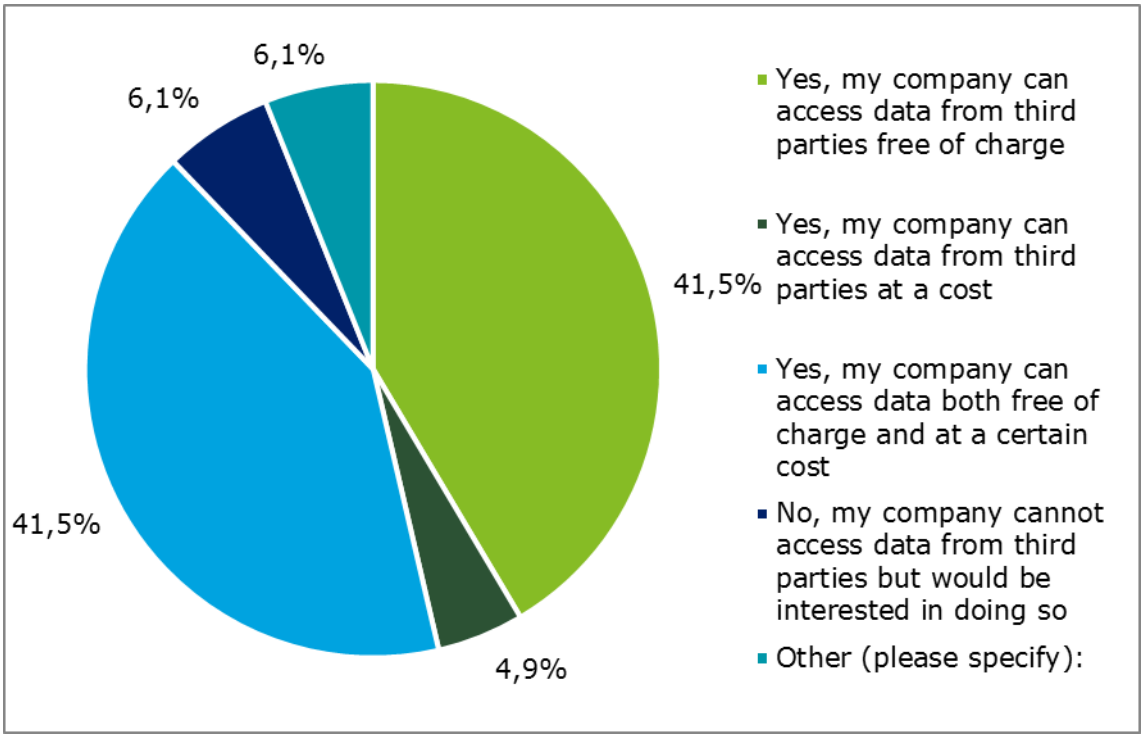
Source: Deloitte

Figure 66: Characteristics of access to data ([Interested or active in accessing data] data users=21)



Source: Deloitte

Figure 67: Characteristics of access to data [Interested or active in both sharing data with third parties and accessing data from third parties] data users and sharers; n=82)



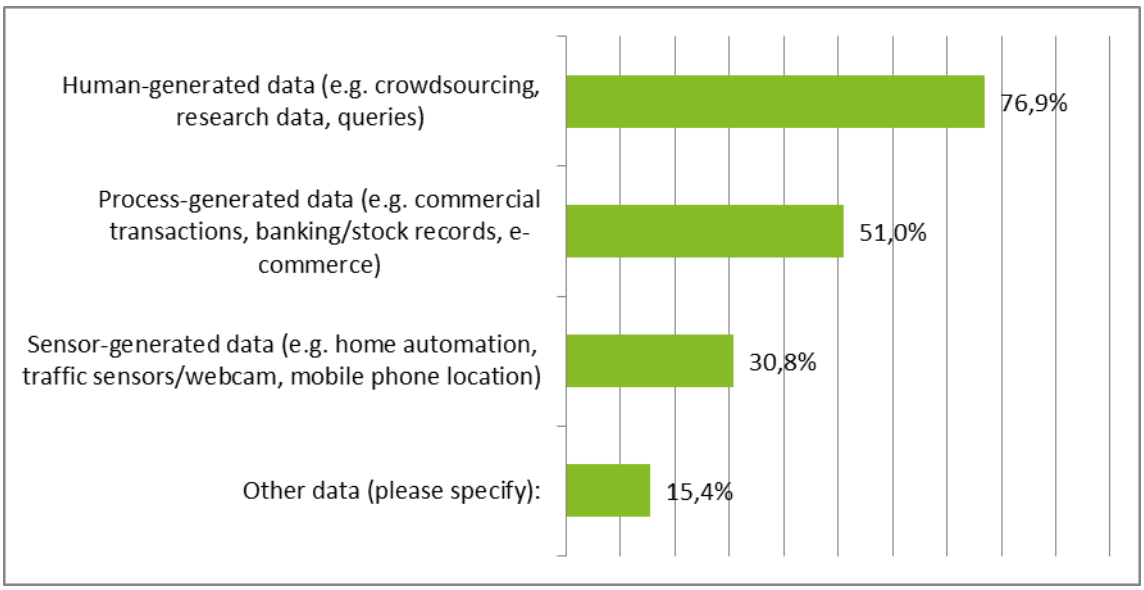
Source: Deloitte

As concerns the reasons why data access is needed in the particular company's business model, the companies mentioned the following points in open comments (mostly reflecting the health industry):

- Legal requirements (e.g. sharing with insurances)
- Billing the patients - cooperation with other hospitals, to exchange medical data for billing reasons
- For (national health and research) statistics. As a research institution we share data for free with other researchers.
- Improve processes internally
- Customer/patients satisfaction
- Improve treatment - sharing of patients records between hospitals and local doctors can be important for follow-up treatments
- Data sharing increases patient`s safety and reduces fraud

The figure below presents an overview of the data needed by companies. Taking into account that a majority of respondents is active in the health sector it seems plausible that around 76,9% need human-generated data. This data may originate, for example, from patients and treatments courses.

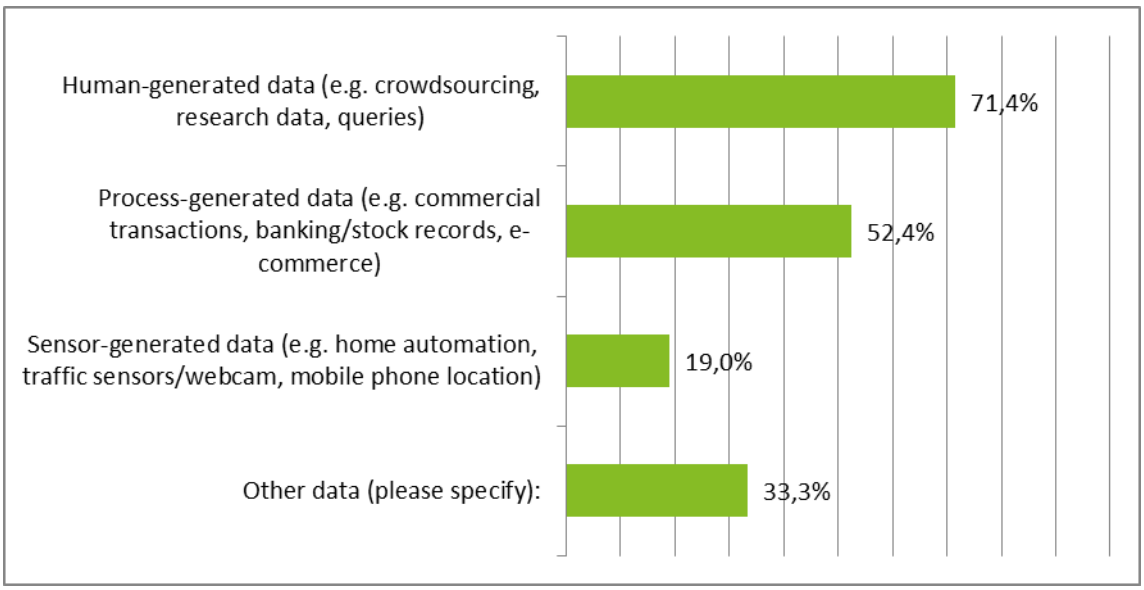
Figure 68: Categories of data to which access is needed, total (n=104)



Source: Deloitte

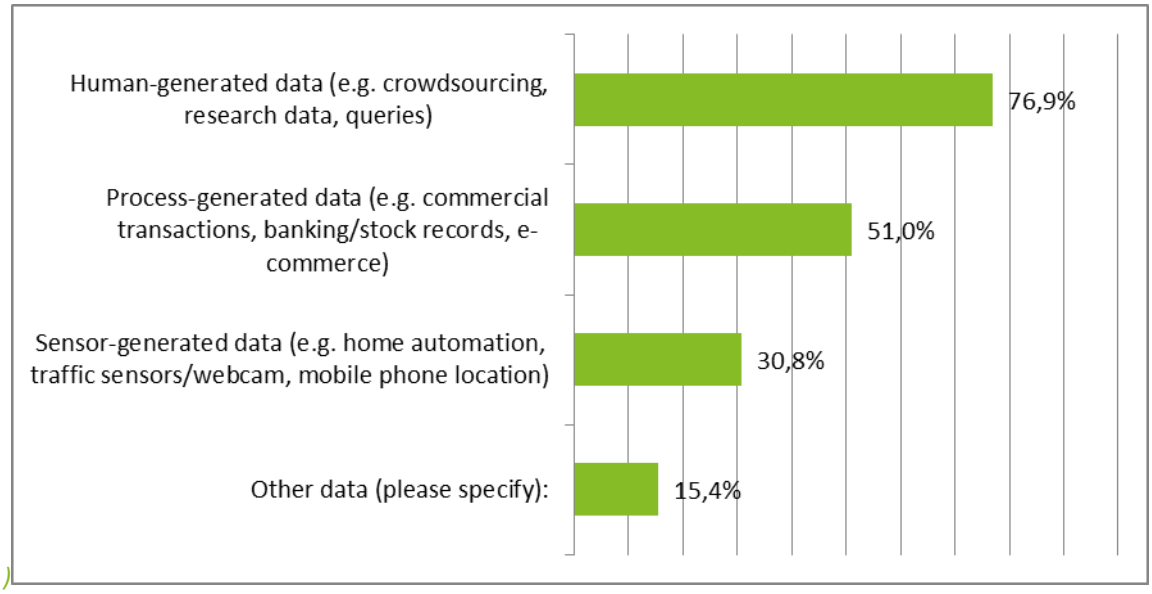
Companies which are data users or data users and sharers require mainly the same categories of data as can be inferred from the two figures below.

Figure 69: Categories of data to which access is needed, data users and sharers (n=48)



Source: Deloitte

Figure 70: Categories of data to which access is needed [Interested or active in accessing data from third parties], data users n=21



Source: Deloitte

When companies were asked which categories of data their company needed more specifically, the following examples were given:

- Course of disease and medical records
- Geolocation data
- Treatment information gained from medical equipment (sensors)
- Electronic shipping notes (in the logistics sector)

In general, accessing data from third parties is very important within the whole range of survey participants. The table below shows the importance of several reasons ranked by the total of respondents. To better segment and target existing markets and to compete in markets otherwise restricted seems to be less important to companies. **Improve existing products and services** and **increase productivity and internal efficiency** is important or even very important for most of the respondents.

Table 36: Importance of accessing third party data (total)

To what extent is accessing third party data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Better segment and target existing markets	47	12	12	15	11	6
Compete in markets otherwise restricted	49	11	8	19	9	7
Improve existing products and services	14	13	17	42	16	1
Deliver new products and services	35	12	10	30	13	3
Increase productivity and internal efficiency	12	9	15	40	25	2

Other	11	3	6	0	6	77
Answered Question						**104**

Source: Deloitte

A similar picture is drawn by the 21 respondents working at companies interested or already active in data accessing as well as sharing. However, this gives only a mixed picture as the number of respondents is quite limited.

Table 37: Importance of accessing third party data [Interested or active in accessing data from third parties], data users

To what extent is accessing third party data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Better segment and target existing markets	7	3	3	3	5	0
Compete in markets otherwise restricted	8	2	2	5	4	0
Improve existing products and services	2	5	4	7	3	0
Deliver new products and services	8	2	1	5	5	0
Increase productivity and internal efficiency	1	3	3	7	6	1
Other	0	2	0	0	1	18
Answered Question						**21**

Source: Deloitte

Looking at the 82 respondents interested or active in both sharing and accessing data from third parties, better segment and target existing markets and compete in markets otherwise restricted is also less important. For the most companies, improve existing products and services and increase productivity and internal efficiency is the most important reason for accessing third party data.

Table 38: Importance of accessing third party data [Interested or active in both sharing data with third parties and accessing data from third parties] data users and sharers

To what extent is accessing third party data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Better segment and target existing markets	40	9	9	12	6	6
Compete in markets otherwise restricted	41	9	6	14	5	7
Improve existing products and services	12	8	13	35	13	1
Deliver new products and services	27	10	9	25	8	3
Increase productivity and internal efficiency	11	6	12	33	19	1
Other	11	1	6	0	5	59
Answered Question						**82**

Source: Deloitte

Main barriers to accessing data

Many companies encounter barriers concerning the access to third party data. The table below provides insights about the extent to which data-related problems occur.

A significant proportion of respondents claims that technical difficulties between involved parties, for example to exchange data with different data formats, is a barrier or even a considerable barrier.

Table 39: Main barriers to accessing third party data (total)

What are the main barriers to accessing third party data?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considerable barrier**	**4 - Very important barrier**	**5 - Blocking factor**	**I do not know**
Data are not made available to my company	33	20	23	12	11	4
Data are too expensive to acquire	52	16	16	7	4	8
Uncertainty about who owns and what can be done with the data	35	22	25	16	3	2
Technical difficulties between the involved parties (e.g. different data formats)	19	29	29	18	7	1
Unequal bargaining power with the data holder	44	15	21	9	6	8
Uncertainty about liability of using data	34	18	28	14	6	3
Other	6	10	5	1	2	79
Answered Question						**104**

Source: Deloitte

Nevertheless, companies who are already data users or data users and sharers do not encounter severe barriers. The tables below provides insights about the extent to which data-related problems are a barrier to a smooth functioning for these companies interested in accessing or sharing data. 5 respondents claim that uncertainty about who owns and what can be done with the data is a very important barrier. Three mention uncertainty about liability of using data as a blocking factor.

In contrast, a majority of participants (11) only encounter small or no barriers related to uncertainty about data liability. Most respondents see availability of data (14), costs of data (11), uncertainty of ownership (13), technical difficulties (12), unequal bargaining power (13) as no or only a small barrier.

Table 40: Main barriers to accessing third party data [Interested or active in accessing data from third parties], data users

What are the main barriers to accessing third party data?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considerable barrier**	**4 - Very important barrier**	**5 - Blocking factor**	**I do not know**
Data are not made available to my company	10	4	6	0	1	0
Data are too expensive to acquire	7	4	5	3	1	1
Uncertainty about who owns and what can be done with the data	9	4	3	5	0	0
Technical difficulties between the involved parties (e.g. different data formats)	6	6	5	2	1	1
Unequal bargaining power with the data holder	9	4	5	1	1	1
Uncertainty about liability of using data	8	3	3	4	3	0
Other	0	1	1	0	0	19
Answered Question						**21**

Source: Deloitte

Looking at data users and sharers, a nearly half of participants (47,6%, 39) claim that data not being available is a considerable, very important or even blocking factor, 22% (18) think data are too expensive, 43%, 26 consider to be uncertain about who owns and what can be done with the data as at least a considerable barrier and 56,1%, 46 mention technical barriers. Unequal bargaining power is a considerable, very important or even blocking factor for 35,4%, 29 respondents and liability was mentioned by 46,3%, 38 companies as a considerable, very important or even blocking factor.

Table 41: Main barriers to accessing third party data, data users and sharers [Interested or active in both sharing data with third parties and accessing data from third parties], data users and sharers

What are the main barriers to accessing third party data?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considerable barrier**	**4 - Very important barrier**	**5 - Blocking factor**	**I do not know**

What are the main barriers to accessing third party data?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considera-ble barrier**	**4 - Very important barrier**	**5 - Block-ing factor**	**I do not know**
Data are not made availa-ble to my company	23	16	17	12	10	4
Data are too expensive to acquire	45	12	11	4	3	7
Uncertainty about who owns and what can be done with the data	26	18	22	11	3	2
Technical difficulties be-tween the involved parties (e.g. different data for-mats)	13	23	24	16	6	0
Unequal bargaining power with the data holder	35	11	16	8	5	7
Uncertainty about liability of using data	26	15	25	10	3	3
Other	6	9	4	1	2	60
Answered Question						**82**

Source: Deloitte

19 data users and 60 data users and sharers gave examples of other main barriers to sharing data with third parties. The main issues can be summarized as follows:

Data protection / Confidentiality:

- Confidentiality of data in the health sector (9)
- Problems to define what is private and what is public data. For example, a key that is used to open a car remotely, could be considered as access to a private database of the customer (example from automotive industry)

Legal requirements:

- Sector specific legal requirements (mentioned frequently (5) from respondents in the health sector)

Contracts:

- Contractual uncertainties

Costs:

- Uncertainty about the value of data the company wants to access or share

Technical:

- Not sufficient bandwidth (2)
- Technical and safety requirements (2)
- Quality of the data
- Different data formats

Costs related to accessing data

Another key factor of accessing third party data are the costs involved. The table below summarises the extent to which costs play a role for all respondents.

In general, all queried categories of costs are mostly ranked as moderate. However, the technical implementation (39) and requiring necessary skills cause high costs, followed by high administration and legal advice costs. 40,4%, 42 of respondents mentioned technical implementation as a high or very high cost factor.

Table 42: Costs of accessing third party data (total)

How would you describe the costs of accessing data for your business with respect to the following categories?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Buying data	21	22	23	14	7	16
Technical implementation (e.g. data preparation, interoperability)	5	12	41	39	3	3
Acquiring necessary skills (e.g. IT-trainings, human resources)	5	17	50	25	4	2
Administration costs (e.g. contract management, on boarding)	10	27	39	20	5	2
Legal advice	21	22	32	15	4	9
Other costs	8	11	11	1	4	68
Answered Question						**104**

Source: Deloitte

Companies interested in both data access and data sharing also encounter similar types of costs as displayed in the tables below. Acquiring skills and technical implementation induce the highest costs.

Table 43: Costs of accessing third party data [Interested or active in accessing data from third parties], data users (n=21)

How would you describe the costs of accessing data for your business with respect to the following categories?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Buying data	5	1	7	2	4	2
Technical implementation (e.g. data preparation, interoperability)	2	3	9	6	0	1
Acquiring necessary skills (e.g. IT-trainings, human resources)	4	3	9	5	0	0
Administration costs (e.g. contract management, on boarding)	2	9	4	4	2	0
Legal advice	5	3	6	4	1	2
Other costs	4	2	2	1	0	12
Answered Question						**21**

Source: Deloitte

Table 44: Costs of accessing third party data (Interested or active in both sharing data with third parties and accessing data from third parties)

How would you describe the costs of accessing data for your business with respect to the following categories?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Buying data	16	21	16	12	3	14
Technical implementation (e.g. data preparation, interoperability)	3	9	32	33	3	2
Acquiring necessary skills (e.g. IT-trainings, human resources)	1	14	41	20	4	2
Administration costs (e.g. contract management, on boarding)	8	18	35	16	3	2
Legal advice	16	19	26	11	3	7
Other costs	4	9	9	0	4	56
Answered Question						**82**

Source: Deloitte

Liability problems with accessing data

Companies can have diverse approaches towards data liability. The table below provides an overview of the extent to which survey participants interested in accessing data agreed (or disagreed) with several statements. It becomes obvious that there is no general consensus amongst the respondents how to handle data liability. About 54,8%, 57 examine liability assurances on a case by case basis (agree or completely agree). Most do accept data as provided (42,3%; 44) including potential errors. Contractual limitations towards people who continue to use the data are relevant for 49,0% of participants (51). Negotiations with individual data providers about additional liability assurance do not appear relevant for 51,9%, 54 respondents.

Table 45: Liability problems with third party data (n=104)

How do you approach liability problems with data you use? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
I examine on a case by case basis what liability assurances are attached to the data I use.	15	15	10	36	21	6
I accept data as provided, and accept that it may contain errors.	14	22	21	32	12	2
I contractually limit my liability towards people who use my data that I previously obtained from a third party.	10	16	20	34	17	6

I sometimes negotiate with individual data providers because I want additional liability assurance.	29	25	12	25	5	7
Other	8	3	7	1	1	83
Answered Question						**104**

Source: Deloitte

A look at data users and data users and sharers gives a similar impression on the relevance of liability problems in these companies.

As regards data users, about 52,4%, 11 examine liability assurances on a case by case basis (agree or completely agree). Most do accept data as provided (42,9%; 9) including potential errors. Contractual limitations towards people who continue to use the data are relevant for 52,4% of participants (11). Negotiations with individual data providers about additional liability assurance do not appear relevant for 42,9%, 9 respondents.

Table 46: Liability problems with third party data [Interested or active in accessing data from third parties], data users, n=21

How do you approach liability problems with data you use? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
I examine on a case by case basis what liability assurances are attached to the data I use.	3	3	3	6	5	1
I accept data as provided, and accept that it may contain errors.	2	4	6	7	2	0
I contractually limit my liability towards people who use my data that I previously obtained from a third party.	2	1	6	4	7	1
I sometimes negotiate with individual data providers because I want additional liability assurance.	4	5	5	5	1	1
Other	0	0	3	0	0	18
Answered Question						**21**

Source: Deloitte

As regards data users and sharers, about 56,1%, 46 examine liability assurances on a case by case basis (agree or completely agree). Most do accept data as provided (42,7%; 35) including potential errors. Contractual limitations towards people who continue to use the data are relevant for 48,8% of participants (40). Negotiations with individual data providers about additional liability assurance do not appear relevant for 54,9%, 45 respondents.

Table 47: Liability problems with third party data [Interested or active in both sharing data with third parties and accessing data from third parties], data users and sharers, n=82

How do you approach liability problems with data you use? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
I examine on a case by case basis what liability assurances are attached to the data I use.	12	12	7	30	16	5
I accept data as provided, and accept that it may contain errors.	12	18	15	25	10	2
I contractually limit my liability towards people who use my data that I previously obtained from a third party.	8	15	14	30	10	5
I sometimes negotiate with individual data providers because I want additional liability assurance.	25	20	7	20	4	6
Answered Question						**82**

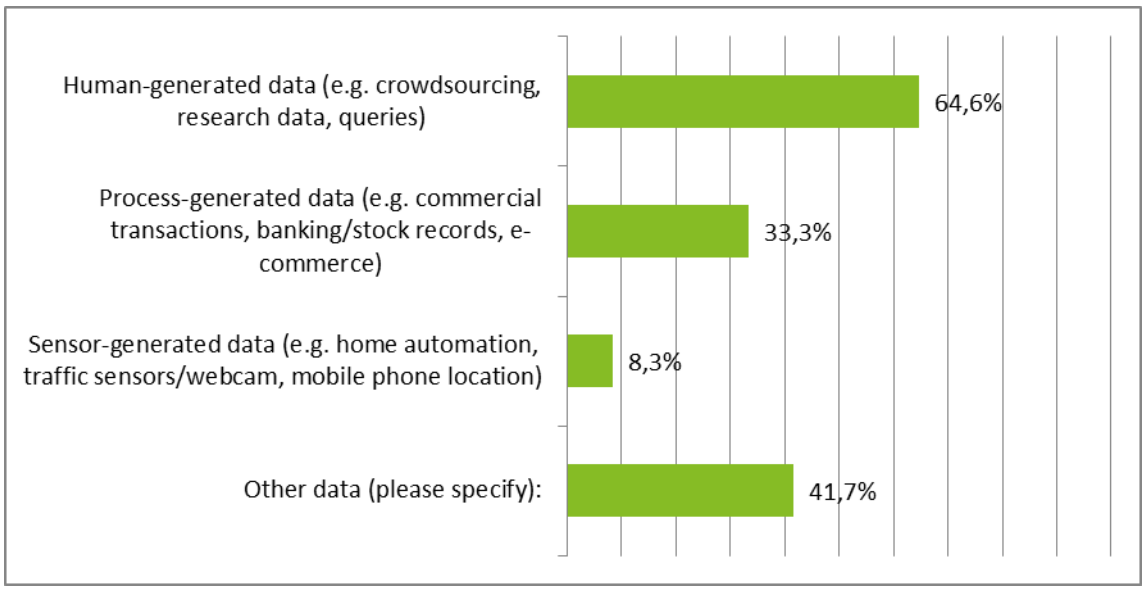
Source: Deloitte

Data sharing

Relevance of sharing data within the business model

With regard to the type of raw data generated by companies, 64,6% respondents who are interested or active in sharing data with third parties indicate that human-generated data like queries and research data is a part of their operation. 33,3% of respondents also generate data on processes (e.g. commercial transactions or banking records). Data from sensors (e.g. on location of devices) is produced by 8,3% of companies.

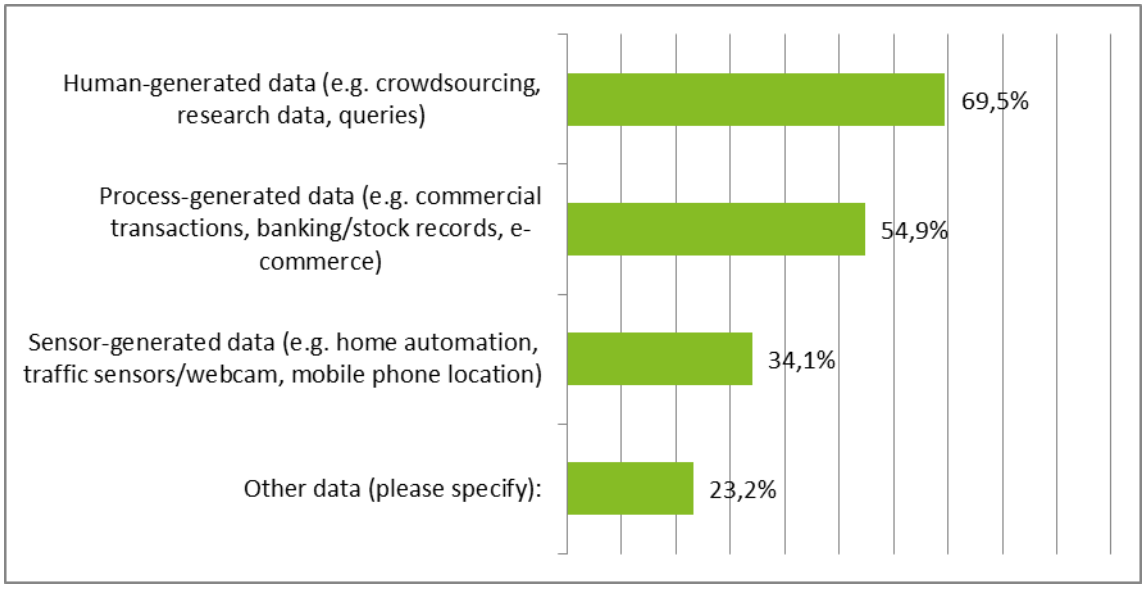
Figure 71: Categories of data shared (Interested or active in sharing data with third parties); n=48)



Source: Deloitte

With regard to the type of raw data generated by companies, 69,5% respondents who are data users and sharers indicate that human-generated data like queries and research data is a part of their operation. 54,9% of respondents also generate data on processes (e.g. commercial transactions or banking records). Data from sensors (e.g. on location of devices) is produced by 34,1% of companies.

Figure 72: Categories of data shared (Interested or active in both sharing data with third parties and accessing data from third parties); n=82)

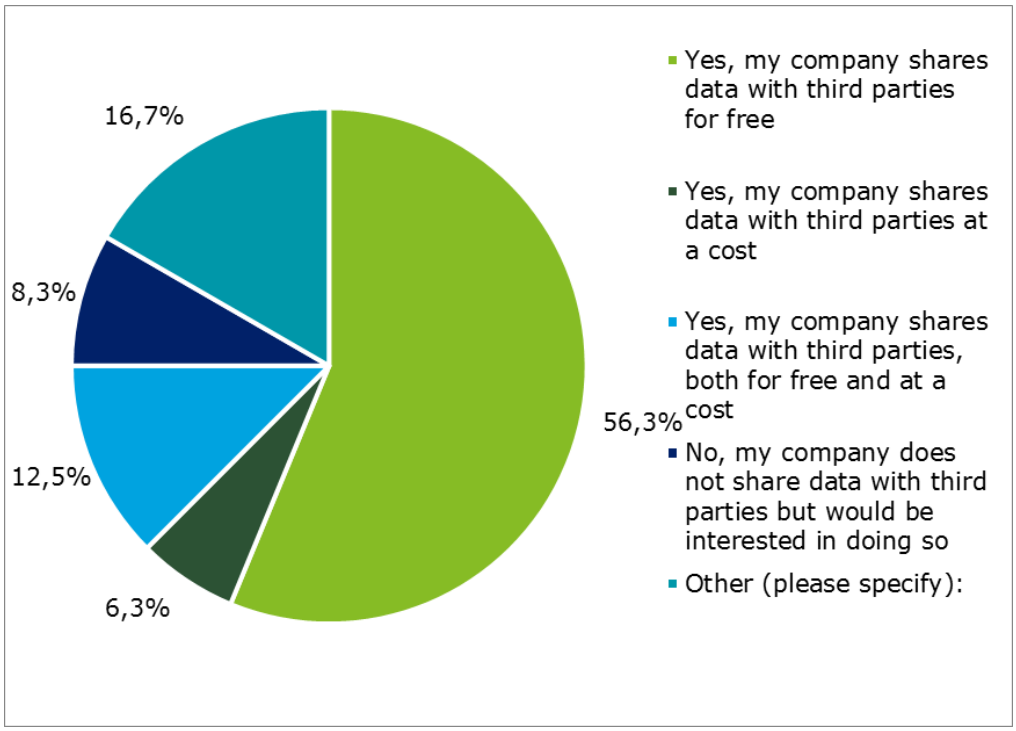


Source: Deloitte

As the figure below shows, the number of companies Interested or active in sharing data with third parties without compensation (56,3%) is higher than the number of companies sharing at a cost (6,3%). 12,5% of respondents share data in both ways. Companies interest-

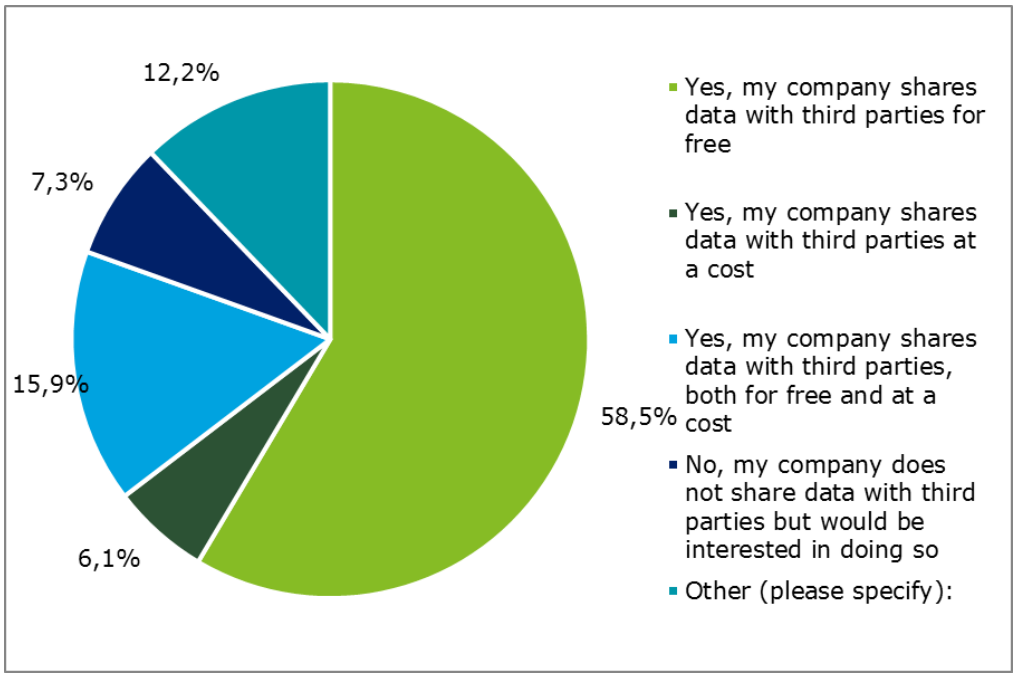
ed or active in both sharing data with third parties and accessing data from third parties give a similar picture (58,5% sharing without compensation).

Figure 73: Characteristics of sharing data (Interested or active in sharing data with third parties); n=48)



Source: Deloitte

Figure 74: Characteristics of sharing data (Interested or active in both sharing data with third parties and accessing data from third parties; n=82)



Source: Deloitte

Participants were able to contribute their reasons for sharing data in their own words. Respondents from the health sector indicate that they share data in order to gain access to treatment information and improve medical care. They will share with other hospitals as long as legislative obligations allow this or patients agree with it.

Further insights on how participants assess the importance of sharing data with third parties are summarised in the table below. A high number of participants share data to optimise their status quo: They want to increase productivity and internal efficiency and to improve existing products and services.

Companies interested or active in both sharing data with third parties and accessing data from third parties share data for reasons of corporate social responsibility and public relations.

Table 48: Importance of sharing data with third parties (Interested or active in sharing data with third parties)

To what extent is sharing data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Generate additional revenues by selling data	38	0	2	1	2	5
Increase productivity and internal efficiency	13	4	2	21	8	0
Improve existing products and services	8	3	8	17	10	2
Deliver new products and services	14	9	8	10	6	1
Better segment and target existing markets	14	9	6	13	3	3
Reasons of corporate social responsibility and public relations	12	9	9	12	5	1
Foster the creation of an ecosystem through open platforms	23	7	8	4	1	5
Other	8	0	3	2	4	31
Answered Question						**48**

Source: Deloitte

Table 49: Importance of sharing data with third parties (Interested or active in both sharing data with third parties and accessing data from third parties); n=82

To what extent is sharing data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Generate additional revenues by selling data	67	4	2	3	1	5
Increase productivity and internal efficiency	7	6	15	28	26	0
Improve existing products and services	12	10	13	24	22	1
Deliver new products and services	21	16	14	19	9	3
Better segment and target	35	9	10	14	7	7

existing markets						
Reasons of corporate social responsibility and public relations	18	13	14	22	13	2
Foster the creation of an ecosystem through open platforms	38	17	14	7	2	4
Other	11	1	3	0	13	54
Answered Question						**82**

Source: Deloitte

Costs related to sharing data

The costs surrounding the exchange of data appear to be perceived as considerable or important when it comes to technical implementation. The table below summarises answers provided on several cost components. Technical implementation appears to impose moderate to high costs to most respondents.

Table 50: Costs of sharing data with third parties (Interested or active in sharing data with third parties)

How would you describe the costs of sharing data for your business with respect to the following categories?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Technical implementation (e.g. data preparation, interoperability)	4	5	21	15	2	1
Acquiring necessary skills (e.g. IT-trainings, human resources)	5	11	16	12	3	1
Administration costs (e.g. contract management, on boarding)	3	9	18	11	2	5
Legal advice	6	12	19	7	0	4
Other costs	1	5	6	1	0	35
Answered Question						**48**

Source: Deloitte

Table 51: Costs of sharing data with third parties (Interested or active in both sharing data with third parties and accessing data from third parties)

How would you describe the costs of sharing data for your business with respect to the following categories?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Technical implementation (e.g. data preparation, interoperability)	2	4	32	32	8	4
Acquiring necessary skills (e.g. IT-trainings, human resources)	4	19	29	27	3	0
Administration costs (e.g. contract management, on boarding)	3	18	36	15	6	4
Legal advice	14	23	25	6	5	9

Other costs	5	8	6	1	4	58
Answered Question						**82**

Source: Deloitte

Liability problems with sharing data

In a next step, the survey provided respondents with the opportunity to identify barriers surrounding liability questions when sharing their data. Their answers are presented in the table below.

Opinions of respondents on whether the present legislation offers clear guidance to them do not vary considerably. For most interested or active in sharing data with third parties, the legislation is clear enough, so they do not impose any further liability restrictions through contracts or terms and conditions (37,5%, 18). However, they try to exclude liability as far as possible in their contracts or terms and conditions (52%, 25).

Many completely disagree/disagree that they accept a degree of liability that they think is fair for the revenue they receive (39,6%, 19). Therefore they contractually limit what people can do with their data and do not accept liability if they use it for a different purpose (54,2%, 26).

Most are not willing to negotiate with individual users of their data because of additional liability assurance (60,4%, 29).

Table 52: Liability problems with sharing data (Interested or active in sharing data with third parties); n=48

How do you approach liability problems with data you share? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
The legislation is clear enough, so I do not impose any further liability restrictions through contracts or terms and conditions.	3	9	8	13	5	10
I try to exclude liability as far as possible in my contracts or terms and conditions.	5	5	7	14	11	6
I accept a degree of liability that I think is fair for the revenue I receive.	9	10	7	12	2	8
I contractually limit what people can do with my data and do not accept liability if they use it for a different purpose.	11	4	2	15	11	5
I sometimes negotiate with individual users of my data because they want additional liability assurance.	22	7	5	6	2	6
Answered Question						**48**

Source: Deloitte

For companies interested or active in both sharing data with third parties and accessing data from third parties, the legislation is clear enough, so they do not impose any further liability restrictions through contracts or terms and conditions (45,1%, 37). However, they try to exclude liability as far as possible in their contracts or terms and conditions (46,3%, 38).

Many completely disagree/disagree that they accept a degree of liability that they think is fair for the revenue they receive (36,6%, 30). Therefore they contractually limit what people can do with their data and do not accept liability if they use it for a different purpose (68,3%, 56).

Most are not willing to negotiate with individual users of their data because of additional liability assurance (57,3%, 47).

Table 53: Liability problems with sharing data (Interested or active in both sharing data with third parties and accessing data from third parties); n=82

How do you approach liability problems with data you share? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
The legislation is clear enough, so I do not impose any further liability restrictions through contracts or terms and conditions.	8	21	15	23	14	1
I try to exclude liability as far as possible in my contracts or terms and conditions.	14	16	8	22	16	6
I accept a degree of liability that I think is fair for the revenue I receive.	19	11	17	19	9	7
I contractually limit what people can do with my data and do not accept liability if they use it for a different purpose.	6	7	11	24	32	2
I sometimes negotiate with individual users of my data because they want additional liability assurance.	32	15	15	14	3	3
Answered Question						**82**

Source: Deloitte

Analysis of the web-based specific survey

This annex provides the analysis of the web-based survey with companies[563]. First, an overview of the survey's target group and its current response rate is presented, followed by an explanation of the structure and content as well as a discussion of the results.

The web-based survey was launched in March 2017 and is still open for participation. It is related to the use of data within and between businesses, covering the following main issues:

- Relevance of accessing/sharing data within the business model;
- Main barriers to accessing and/or sharing data;
- Costs related to accessing and/or sharing data; and
- Liability problems with accessing and/or sharing data.

The survey was disseminated broadly, using various channels. For example, it was sent to **140 interest groups and business associations across several relevant sectors** in all Member States, with the request to be circulated to all member companies in order to cover a full range of both big companies and SMEs. In addition, the survey was shared via different social networks.

Basic information about the survey respondents

On 24 March 2017, the survey was filled in by a **total of 35 respondents representing companies across several sectors and Member States**. Until now, companies from 14 Member States (Austria, Belgium, Croatia, Denmark, Finland, France, Germany, Italy, Luxembourg, the Netherlands, Romania, Spain, Sweden and UK) participated in the survey. Overall, 59% (20) of these companies operate in more than one country (see *Table 54*).

Table 54: Share of companies operating in more than one country

Does your company operate in more than one country?		
Answer Options	**Response Percent**	**Response Count**
Yes	58,8%	20
No	41,2%	14
Answered Question		**34**

Source: Deloitte

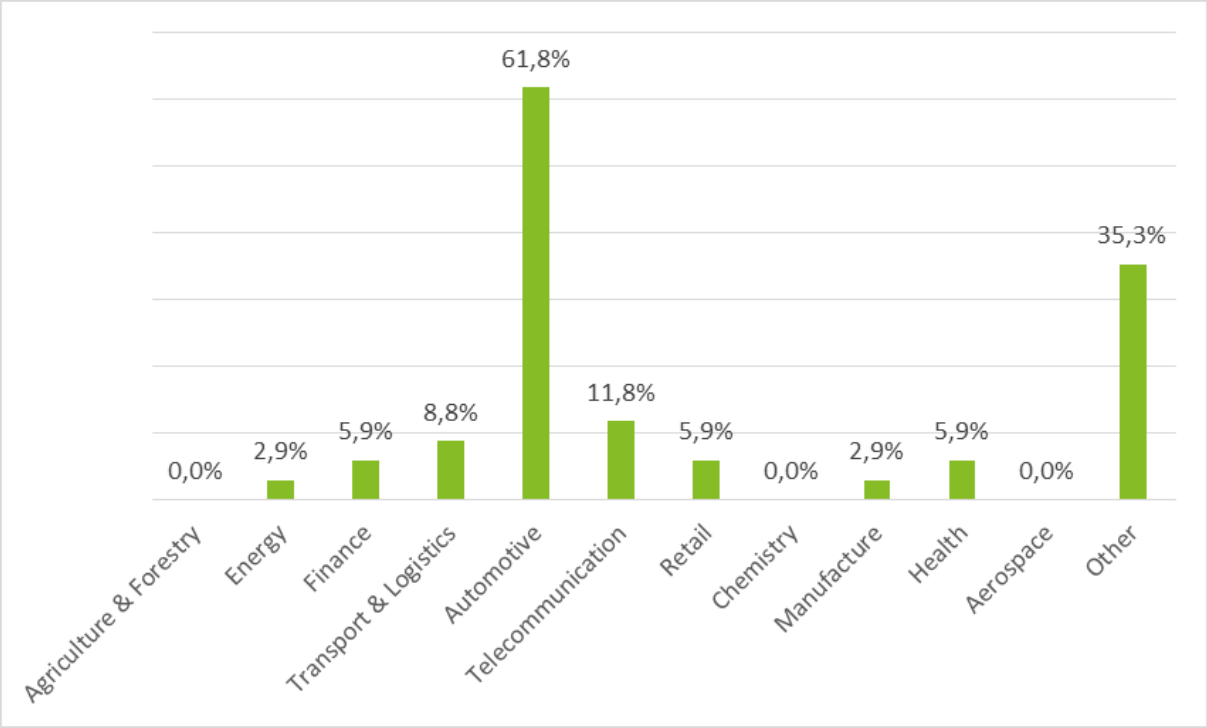
Table 54 provides an overview of the sectors in which the companies are situated. [564] The majority of respondents, about 62% (21), is active in the automotive sector. Therefore, the current answers mostly express opinions from companies within this area and cross-sectoral representativeness is limited. Moreover, 12% (4) of respondents operate in Telecommunication and 9% (3) in Transport & Logistics. The comparatively large response rate form the automotive, telecommunication and transport sectors may be because these sectors are usual-

[563] Please note that the survey is still open and that its final results will be presented for the Fourth Interim Report.

[564] The question allows multiple answer options as it can be assumed that some companies operate cross-sectoral.

ly the main focus of the discourse about digitisation and assumed to experience the greatest disruptions in the future. Other sectors mentioned by participants are, amongst others, Media, Marketing and Real Estate.

Figure 75: Sectors in which participating companies operate



Source: Deloitte

Data analytics companies account for 35% (12) of respondents, compared to 65% (22) that work at a company mainly offering non-data driven goods and services.

Table 55: Share of data analytics companies

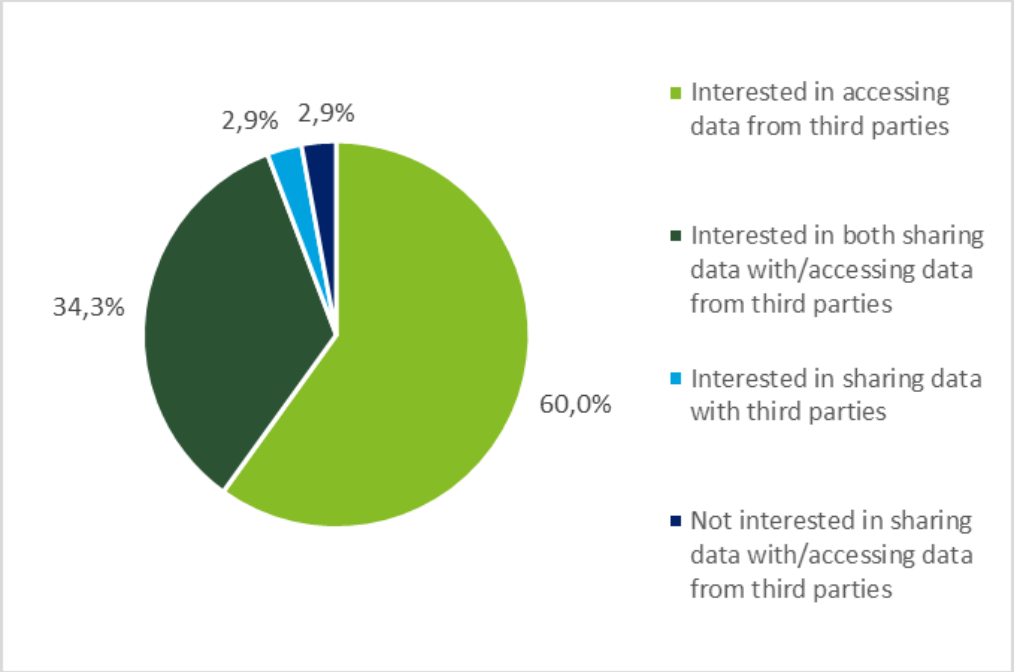
Is your company a data analytics company?		
Answer Options	**Response Percent**	**Response Count**
Yes	35,3%	12
No	64,7%	22
Answered Question		**34**

Source: Deloitte

Participants were also asked about the nature of their interest in data: whether they are interested in accessing data, sharing data, both, or not at all interested in data.

As demonstrated in the figure below, a majority of respondents (60%; 21) is only interested in accessing data from third parties while one third (34%; 12) is interested in both the access and distribution of data. One respondent is only interested in sharing data, another is not interested in data for his/her company in general.

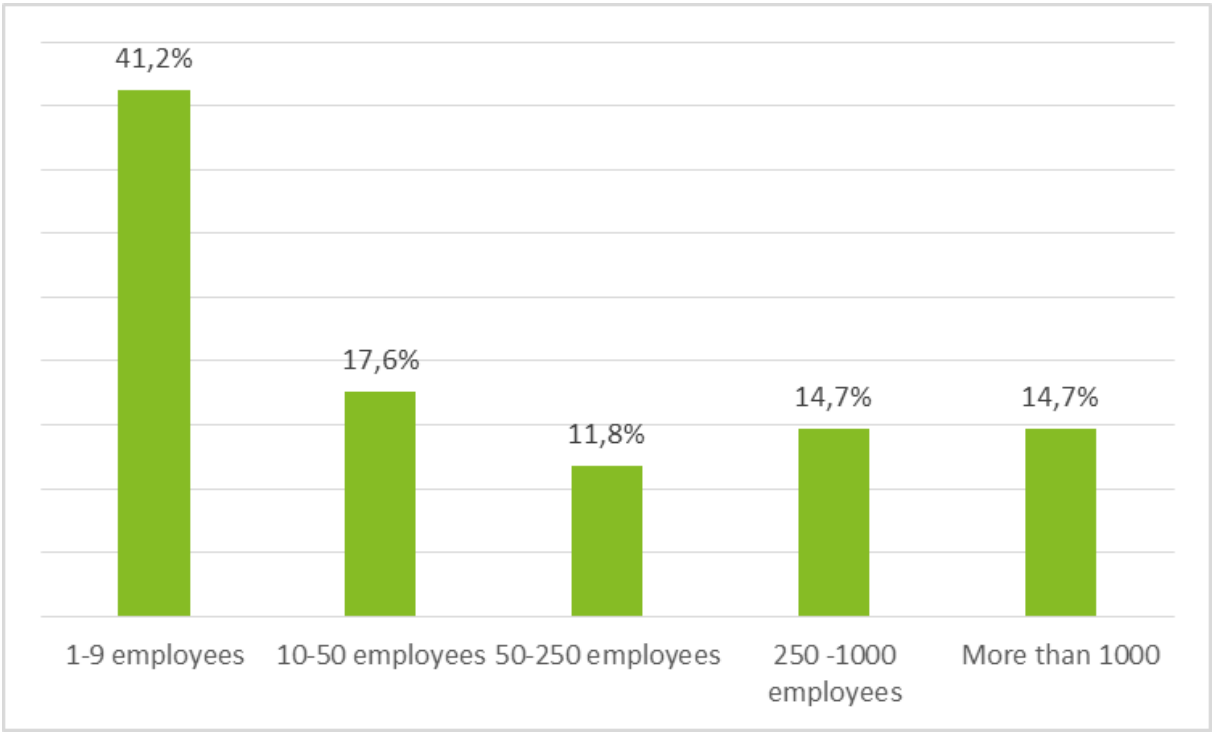
Figure 76: Company's interest in data (n=31)



Source: Deloitte

As concerns the size of the companies, small companies with a maximum number of 9 employees account for 41% (14) of the respondents. The share of companies with more employees is almost evenly distributed as can be inferred from the figure below.

Figure 77: Company size (n=30)



Source: Deloitte

As regards growth rates, around 44% (15) of the companies experienced a 10% growth annually either in people or revenue over the past 3 years, compared to 35% (12) that did not experience such development.

Table 56: Share of companies with 10% growth

Has your company experienced a 10% growth annually either in people or in revenue in the past 3 years?		
Answer Options	**Response Percent**	**Response Count**
Yes	44,1%	15
No	35,3%	12
I do not know	20,6%	7
Answered Question		**34**

Source: Deloitte

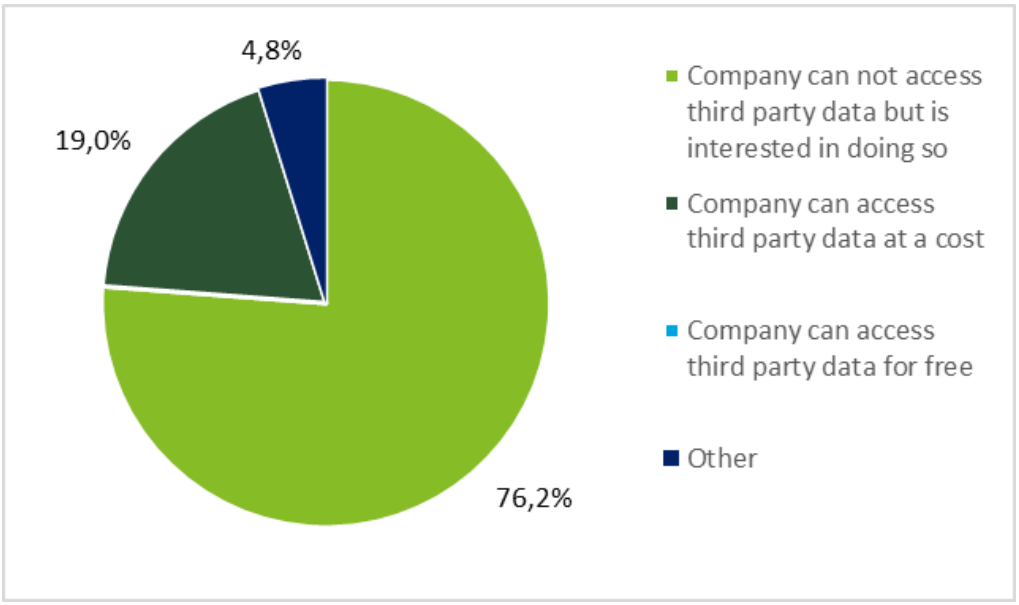
Data access

In the following, the results of questions concerning the **access to data** will be presented. The chapter contains results from companies only interested in accessing data and from companies that are interested in both; accessing *and* sharing data.

Relevance of accessing data within the business model

Participants were asked a set of questions relating to the relevance of accessing data. First, participants are asked whether they can access third party data or not. The figure below shows the share of respondents whose companies are only interested in data access. Four participants (19%) indicated that their company pays for accessing data held by third parties. However, 76% (16) are **not able to access** the data they want to obtain – neither for free, nor at a cost.

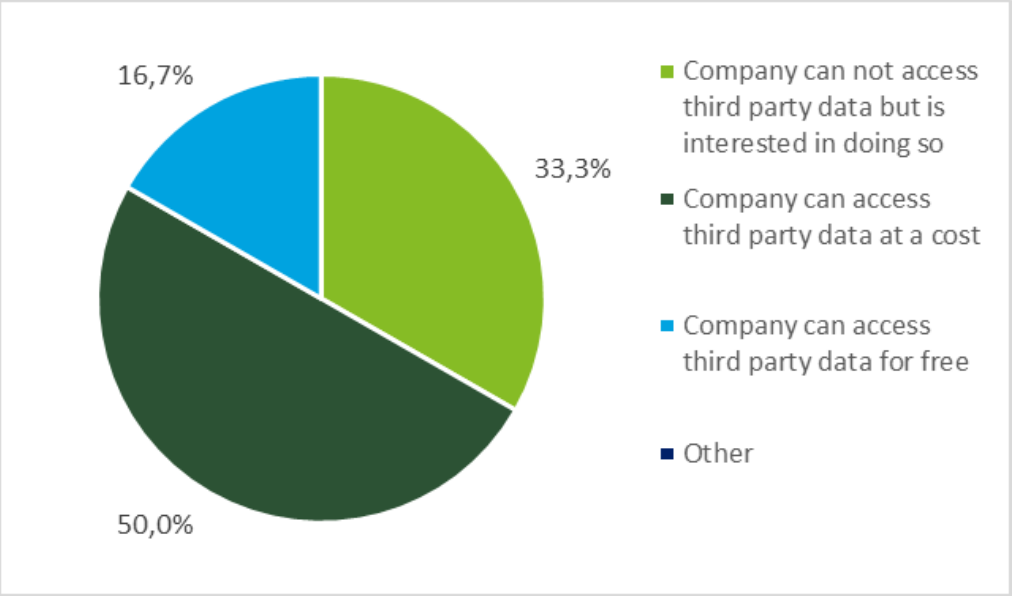
Figure 78: Characteristics of access to data (n=21)



Source: Deloitte

Of those respondents answering on behalf of a company interested in both accessing and sharing data, 50% (6) indicated that they are able to access data at a cost while 17% (2) can obtain data for free. One third (3) cannot access data at all, but is interested in doing so.

Figure 79: Characteristics of access to data (n=12)



Source: Deloitte

As concerns the reasons why data access is needed in the particular company's business model, the companies mentioned the following points in open comments (mostly reflecting the automotive industry):

- Survive and compete in the digital era;
- Create new and innovative business models (e.g. prognostics and predictive services);
- Provide new services to customers;
- Directly process data and be able to diagnose it; and/or
- Look up car specifications in the automotive aftermarket

As one respondent generalised, "access to third party data is vital for all independent after market operators".

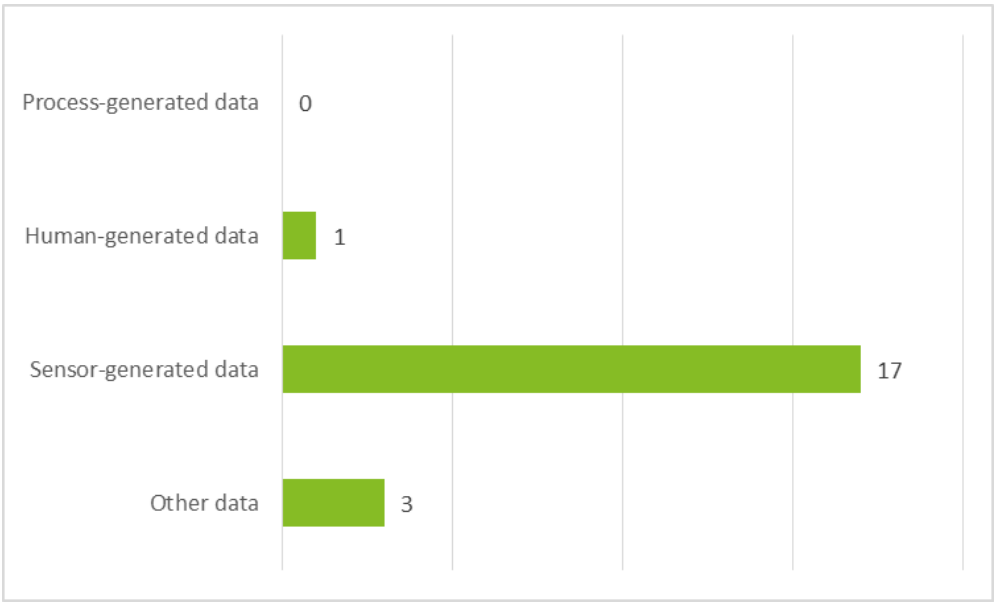
Companies that are interested in both, accessing and sharing, use data to, for example:

- Improve internal processes by data integration into their systems;
- Improve goods and services offered to their clients;
- Access contact information;
- Use third party customer data for promotion of own products;
- Detect new business opportunities; and/or
- Compare the company's situation to the market

The figure below presents an overview of the data needed by companies for which only data access is interesting. Taking into account that a majority of respondents operate in the automotive sector, it can be observed that around 81% (17) need sensor-generated data. This

data may originate, for example, from traffic sensors, webcams installed at the front or rear end of a vehicle as well as location tracking systems. One respondent expressed the necessity to access human-generated data. Other data can refer, for example, to car-specific data depending on the individual vehicle's ability to collect information.

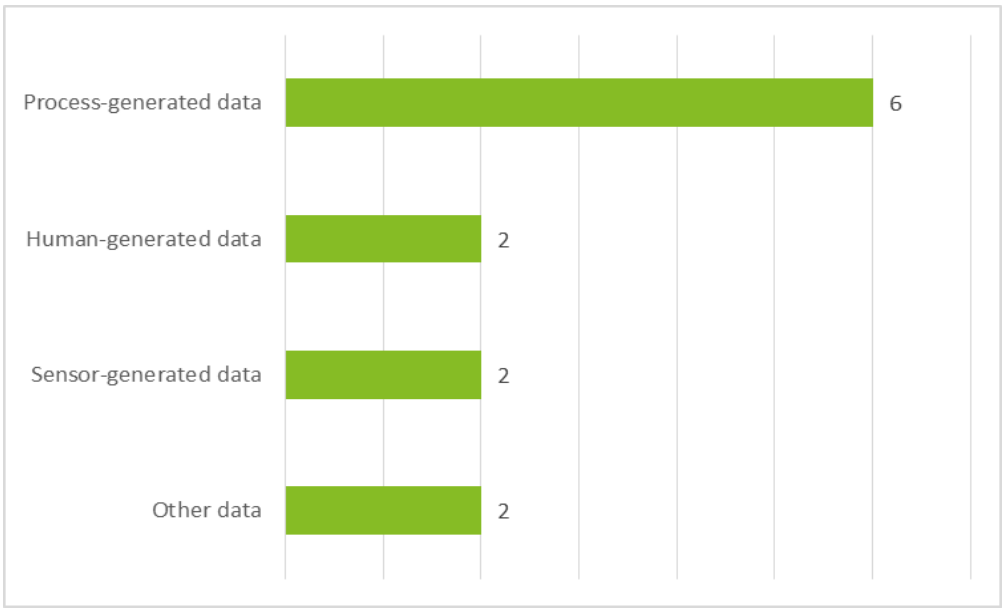
Figure 80: Categories of data to which access is needed, data users (n=21)



Source: Deloitte

Companies that are interested in both accessing and sharing data require different categories of data as can be inferred from the figure below (*Figure 81*). Six respondents (50%) claim that their companies are interested in process-generated data. Interest in human- and sensor-generated is expressed by two respondents (17%) for each case. Another two participants mentioned their need for all kind of data, no matter their nature, in order to provide goods and services to as many other companies as possible.

Figure 81: Categories of data to which access is needed, data users and sharers (n=12)



Source: Deloitte

In general, accessing data from third parties is very important within the whole range of survey participants. The table below shows the importance of several reasons ranked by the respondents only interested in data access. For them, to compete in markets otherwise restricted, to improve existing products and services and to deliver new products and services is at least important. A great majority (90%; 19) indicated that these purposes are *very* important. Except for one respondent each, to better segment and target existing markets and to increase productivity and internal efficiency are also rated as important to very important.

Table 57: Importance of accessing third party data, data users

To what extent is accessing third party data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Better segment and target existing markets	1	0	0	2	18	0
Compete in markets otherwise restricted	0	0	0	2	19	0
Improve existing products and services	0	0	0	2	19	0
Deliver new products and services	0	0	0	3	18	0
Increase productivity and internal efficiency	0	1	0	4	16	0
Other	0	0	0	0	2	0
Answered Question						**21**

Source: Deloitte

A similar picture is drawn by the respondents working at companies interested in data accessing as well as sharing. The access of data in relation to the improvement of existing products and services is ranked as important to very important by all twelve respondents, followed by the provision of new products and services (also 12 respondents). Accessing data to compete in markets otherwise restricted and to better segment and target existing markets is also important to very important for a majority of respondents (83%; 10). Using data to increase productivity and internal efficiency is important to very important for 67% of respondents (8) while the remaining 33% see this as somewhat important.

Table 58: Importance of accessing third party data, data users and sharers

To what extent is accessing third party data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Better segment and target existing markets	0	1	1	5	5	0
Compete in markets otherwise restricted	0	0	2	4	6	0
Improve existing products and services	0	0	0	5	7	0
Deliver new products and services	0	0	0	6	6	0

To what extent is accessing third party data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Increase productivity and internal efficiency	0	0	4	3	5	0
Other	0	0	0	0	0	3
Answered Question						**12**

Source: Deloitte

Main barriers to accessing data

Nevertheless, companies can encounter barriers concerning the access to third party data. The table below provides insights about the extent to which data-related problems are a barrier to a smooth functioning for the companies interested in accessing data only. The majority of respondents (86%; 18) claims that technical difficulties and unequal bargaining power with the data holder are a blocking factor to their business, closely followed by non-availability and the costs of data (81%; 17). In contrast, 90% of participants (19) only encounter small barriers related to uncertainty about data liability. Another 76% (16) see uncertainty about data ownership as small barriers to their companies.

Table 59: Main barriers to accessing third party data, data users

What are the main barriers to accessing third party data?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considerable barrier**	**4 - Very important barrier**	**5 - Blocking factor**	**I do not know**
Data are not made available to my company	2	0	0	2	17	0
Data are too expensive to acquire	2	1	1	0	17	0
Uncertainty about who owns and what can be done with the data	1	16	2	0	2	0
Technical difficulties between the involved parties (e.g. different data formats)	1	0	1	1	18	0
Unequal bargaining power with the data holder	1	0	1	1	18	0
Uncertainty about liability of using data	0	19	1	0	1	0
Other	12	0	1	0	3	0
Answered Question						**21**

Source: Deloitte

Those participants operating within the automotive sector mainly see barriers in the availability of data. They note that car manufacturers design in-vehicle telematics systems as "black boxes", therefore not permitting access from outside.[565] As a result, they argue that

[565] The respondents already mentioned this point in the comment section of Question 2. However, to follow the chapter structure, it is presented here under "Main barriers to accessing party".

innovation within their businesses is impeded. On the contrary, and in their point of view, data ownership is not a barrier because machine- and vehicle-generated data is not owned by anybody. However, one respondent also mentions that it remains unclear whether the manufacturer or the driver should own the data.

One respondent explained that his/her company lost an important business related to a fleet as it did not have the vehicle/sensor-generated data that the car brand producer could possibly provide. The respondent concluded that in such case, fair competition between the parties is not made possible.

Another example refers to a diagnostic test method to conduct a 'road test' to monitor the real-time functionality of a system under real driving conditions. Respondents argued that, if data access is restricted by the vehicle manufacturer, this test method would not be possible anymore. Again, as a conclusion, fair competition in the automotive aftermarket would not be present and companies as well as consumers could encounter more difficulties and higher costs.[566]

Companies interested in accessing and sharing data do not encounter the mentioned barriers at such level which can be seen in the table below. It is striking that the results are evenly distributed for the most items. Nevertheless, for 50% of respondents (6), non-availability of data is a very important barrier or blocking factor to their business. 67% of participants (8) encounter this with the price of data. Uncertainty about data ownership and technical difficulties are considerable barriers for four respondents each (34%). There is no consensus about the extent to which unequal bargaining power with the data holder and uncertainty about data liability is a barrier to business.

Table 60: Main barriers to accessing third party data, data users and sharers

What are the main barriers to accessing third party data?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considerable barrier**	**4 - Very important barrier**	**5 - Blocking factor**	**I do not know**
Data are not made available to my company	2	1	3	2	4	0
Data are too expensive to acquire	2	1	1	6	2	0
Uncertainty about who owns and what can be done with the data	2	1	4	3	2	0
Technical difficulties between the involved parties (e.g. different data formats)	1	4	4	2	1	0
Unequal bargaining power with the data holder	2	2	2	2	3	1
Uncertainty about liability of using data	2	0	3	3	3	1

[566] This example was made under Question 8 of the survey: „ Could you please briefly describe a case where you encountered one of the barriers mentioned above and how this resulted in specific costs or prevented you from achieving certain outcomes?"

What are the main barriers to accessing third party data?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considera-ble barrier**	**4 - Very important barrier**	**5 - Block-ing factor**	**I do not know**
Other	0	0	0	0	1	2
Answered Question						**12**

Source: Deloitte

Additional barriers mentioned by the respondents include:

- Data is often scattered between several parties (e.g. different cities);
- Countries have different, specific data privacy laws; and
- Processes to acquire data are long and costly.

Only one participant commented that he/she did not encounter any of the above mentioned barriers.

Costs related to accessing data

Another key factor of accessing third party data are the costs involved. The table below summarises the extent to which costs play a role for the respondents on behalf of companies interested in data access. In general, all queried categories of costs are mostly ranked as high to very high. Especially the technical implementation (81%; 17) and the obtaining of third party data (76%; 16) cause *very* high costs, followed by high administration and legal advice costs both(81%; 17). Additionally, the acquisitions of necessary skills also imposes high costs (71%; 15) to the majority of companies.

Table 61: Costs of accessing third party data, data users

How would you describe the costs of accessing data for your business with respect to the following categories?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Buying data	0	1	1	3	16	0
Technical implementation (e.g. data preparation, interoperability)	0	2	2	0	17	0
Acquiring necessary skills (e.g. IT-trainings, human resources)	0	1	3	15	2	0
Administration costs (e.g. contract management, on boarding)	0	2	2	17	0	0
Legal advice	0	1	0	17	0	0
Other costs	7	0	0	0	3	1
Answered Question						**21**

Source: Deloitte

Nevertheless, it is important to mention that the majority of respondents described **anticipated costs** in this table rather than current costs which becomes evident when analysing the individual comments. Again, those respondents operating within the automotive sector raised their opinion that vehicle-generated data are not owned by anybody. Currently, they are accessible and free of charge so **"buying data" does not impose any costs on these**

companies. However, the participants remark that car manufacturers are planning on restricting this access, making it mandatory to pay for data which could eventually result in high to very high costs for the companies affected. Besides this, the respondents acknowledged that any other costs are manageable in-house.

Companies interested in both data access and data distribution also encounter different types of costs as displayed in the table below. The costs related to the acquisition of necessary skills are ranked as high to very high from 67% of participants (8), followed by the costs for technical implementation (58%; 7) and the costs of buying data (50%; 6). Administration costs and legal advice are described as moderate each.

Table 62: Costs of accessing third party data, data users and sharers

How would you describe the costs of accessing data for your business with respect to the following categories?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Buying data	2	0	1	4	2	2
Technical implementation (e.g. data preparation, interoperability)	2	0	3	6	1	0
Acquiring necessary skills (e.g. IT-trainings, human resources)	1	0	2	6	2	1
Administration costs (e.g. contract management, on boarding)	1	1	5	3	2	0
Legal advice	1	1	5	2	1	2
Other costs	0	0	0	0	0	3
Answered Question						**12**

Source: Deloitte

Liability problems with accessing data

Companies can have diverse approaches towards data liability. The table below provides an overview of the extent to which survey participants interested in accessing data agreed (or disagreed) with several statements. It becomes obvious that there is no general consensus amongst the respondents how to handle data liability. About 29% (6) examines liability assurances on a case by case basis. Some do not accept data as provided (43%; 9) while others do or have to, including potential errors (19%; 4). Contractual limitations towards people who continue to use the data are relevant for 38% of participants (8), in contrast to 34% (7) who deem this irrelevant. Negotiations with individual data providers about additional liability assurance do not appear relevant.

Table 63: Liability problems with third party data, data users

How do you approach liability problems with data you use? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
I examine on a case by case basis what liability assur-	0	4	4	1	6	6

ances are attached to the data I use.						
I accept data as provided, and accept that it may contain errors.	0	9	2	4	0	6
I contractually limit my liability towards people who use my data that I previously obtained from a third party.	0	7	1	8	1	4
I sometimes negotiate with individual data providers because I want additional liability assurance.	0	6	1	2	1	11
Answered Question						**21**

Source: Deloitte

Respondents from the automotive sector mention that dealers or independent repairers currently rely on EU product liability laws and the producer's liability under national tort law.

Also when analysing the answers of companies interested in both accessing and sharing data, no clear consensus can be found as displayed in the table below. Five participants (42%) contractually limit liability of data they use. Four (34%) examine external data liability on a case by case basis and/or accept data as provided, including possible errors. Negotiations with individual data providers are relevant for a small amount of survey respondents (25%; 3).

Table 64: Liability problems with third party data, data users and sharers

How do you approach liability problems with data you use? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
I examine on a case by case basis what liability assurances are attached to the data I use.	1	1	3	4	0	3
I accept data as provided, and accept that it may contain errors.	1	2	4	3	1	1
I contractually limit my liability towards people who use my data that I previously obtained from a third party.	1	0	4	4	1	2
I sometimes negotiate with individual data providers because I want additional liability assurance.	1	0	4	3	0	4
Answered Question						**12**

Source: Deloitte

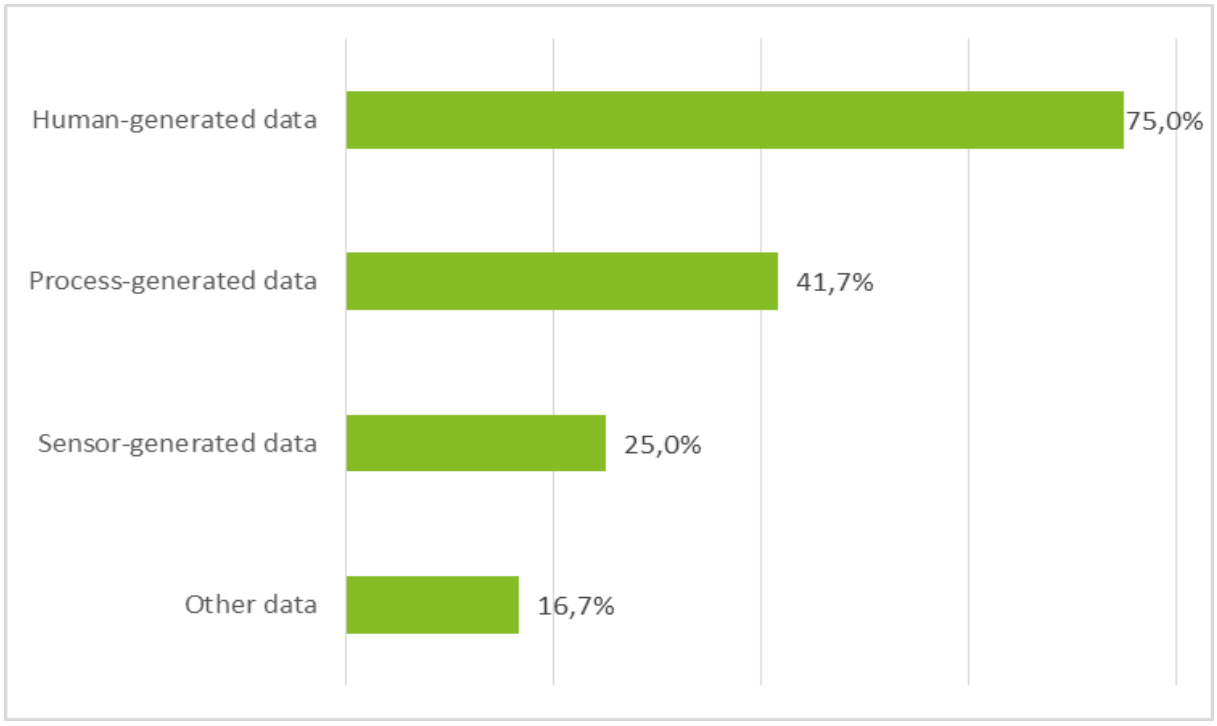
Data sharing

The survey revealed that few respondents exclusively share data as part of their business model. Instead, twelve of the thirty-one participants in the survey indicated that they are interested in both accessing and sharing data with third parties. Below, we discuss the replies of the latter type of companies.

Relevance of sharing data within the business model

With regard to the type of raw data generated by companies, 75% (or 9) respondents indicate that human-generated data like queries and research data is a part of their operation. Five respondents also generate data on processes (e.g. commercial transactions or banking records). Data from sensors (e.g. on location of devices) is produced 25% (3) companies. One respondent explicitly indicates that they generate data by aggregating other sources of raw data.

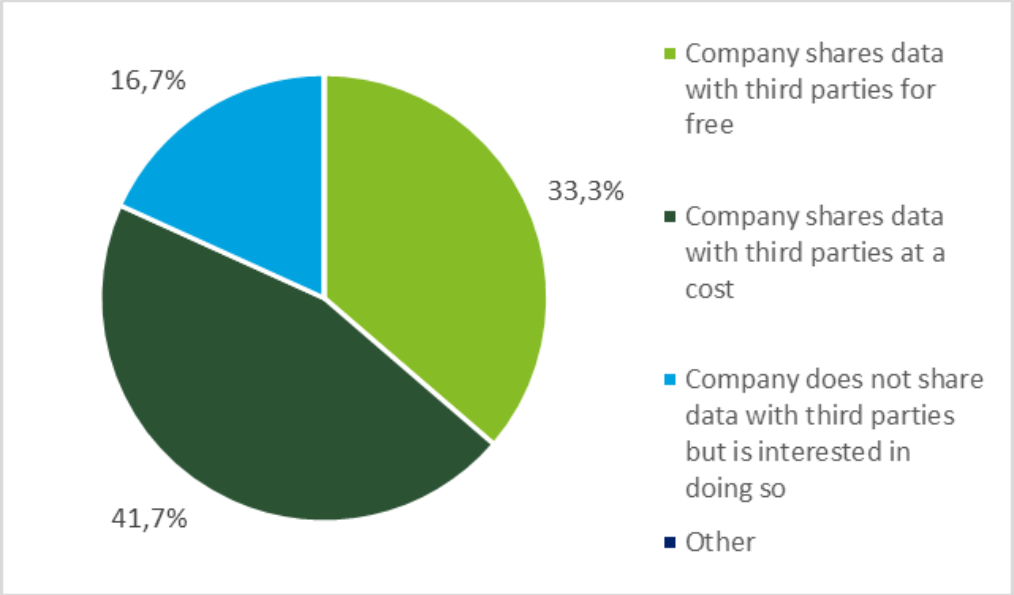
Figure 82: Categories of data shared (n=12)



Source: Deloitte

As the figure below shows, the number of companies sharing data with third party with or without compensation is roughly equal in the survey. A slight majority of 42% (5) participants shares data only for a compensation, whereas another third of participants (4) shares data with third parties for free.

Figure 83: Characteristics of sharing data (n=12)



Source: Deloitte

Participants were able to contribute their reasons for sharing data in their own words. Here, five respondents indicate that they share data in order to gain access to data of other companies. Three companies additionally report that, in doing so, they are able to benchmark and assess their performance. This information is in turn used to improve efficiency. Other reasons provided are that sharing of data increases revenue and their user base, as it enables to launch new products or improve user experiences for their clients

Further insights on how participants assess the importance of sharing data with third parties are summarised in the table below. As mentioned above, a high number of participants share data to optimise their status quo: Nine respondents consider it very important to improve their product and service, while eight see it as very important to place their product and service in the market. Another eight respondents each indicates sharing data as very important to optimise internal processes. With regards to new business opportunities, sharing data is also considered important to very important to create new products and services by all respondents, while five consider sharing data itself as a possibly very important additional source of revenue. Participants' views differ, whether fostering future cooperation and exchanges through open platforms is important.

Table 65: Importance of sharing data with third parties

To what extent is sharing data important for your business in relation to the following reasons?						
Answer Options	**1 - Not important**	**2 - Slightly important**	**3 - Somewhat important**	**4 - Important**	**5 - Very important**	**I do not know**
Generate additional revenues by selling data	1	1	2	3	5	0
Increase productivity and internal efficiency	0	0	2	2	8	0
Improve existing products and services	0	0	1	2	9	0
Deliver new products and services	0	0	0	5	7	0
Better segment and target existing markets	0	0	2	2	8	0
Reasons of corporate social responsibility and public relations	0	0	6	2	2	2
Foster the creation of an ecosystem through open platforms	0	1	2	1	6	2
Other	1	0	0	0	1	1
Answered Question						**12**

Source: Deloitte

Main barriers to sharing data

In a next step, companies both using and sharing data are asked to identify existing barriers, hindering or even fully blocking exchanges. The answers summarised in the table below reveal mixed experiences of respondents. One barrier considered as **very important or even prohibitive** are uncertainties surrounding contracts: six (combined) responses assume this position, whereas only three respondents consider this to be a small or no barrier at all. Costs and technical difficulties surrounding data exchanges, assessing the value of data as well as risks of sharing sensible commercial data with third parties are predominantly identified as **considerable barriers**. Some confusion appears to exist regarding uncertainties surrounding ownership and usage of data: Two respondents each see this as a blocking barrier or no barrier at all respectively.

Interestingly, one participating company from Belgium reported that none of the barriers included in the table below were encountered, as they are well covered in their contracts and addressed in existing legislation.

Table 66: Main barriers to sharing data with third parties

What are the main barriers to sharing data with third parties?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considerable barrier**	**4 - Very important barrier**	**5 - Blocking factor**	**I do not know**
Uncertainty from a contractual point of view	1	2	1	4	2	2
Uncertainty about the value of the data	2	3	4	1	0	2
Uncertainty about owner-	2	3	3	1	2	1

What are the main barriers to sharing data with third parties?						
Answer Options	**1 - Not a barrier**	**2 - Small barrier**	**3 - Considera-ble barrier**	**4 - Very important barrier**	**5 - Block-ing factor**	**I do not know**
ship and usage of the data						
Technical difficulties be-tween the involved stake-holders (e.g. different data formats)	2	2	4	2	1	1
Costs of sharing data (both immediate and in the long run)	2	1	6	2	0	1
Risk of sharing sensitive commercial data with third parties (e.g. competitors)	1	3	4	2	1	1
Other	1	0	0	0	0	2
Answered Question						**12**

Source: Deloitte

Costs related to sharing data

As observed above, the costs surrounding the exchange of data appear to be perceived as considerable or important. The table below summarises answers provided on several cost components. Technical implementation appears to impose moderate to high costs to most respondents. Yet costs for training and staff, as well as administration of contracts and costs for legal advice are more uniformly reported as high by five respondents respectively.

Table 67 : Costs of sharing data with third parties

How would you describe the costs of sharing data for your business with respect to the following catego-ries?						
Answer Options	**1 - Very low**	**2 - Low**	**3 - Moderate**	**4 - High**	**5 - Very high**	**I do not know**
Technical implementation (e.g. data preparation, interoperability)	1	2	4	4	1	0
Acquiring necessary skills (e.g. IT-trainings, human resources)	1	3	0	5	2	1
Administration costs (e.g. contract management, on boarding)	0	3	3	5	1	0
Legal advice	0	3	2	5	1	1
Other costs	1	1	1	0	0	2
Answered Question						**12**

Source: Deloitte

Liability problems with sharing data

In a next step, the survey provided respondents with the opportunity to identify barriers surrounding liability questions when sharing their data. Their answers are presented in the table below. Opinions of respondents on whether the present legislation offers clear guid-ance to them vary considerably: Overall, more participants presently rather disagree (6) than agree (3). Accordingly, six respondents tend to rely on further liability restrictions through

contracts or terms and conditions. Another seven participants report to define limits of how data may be used in their contracts in order to prevent liability disputes. Nevertheless, companies agree that accepting a certain degree of liability is fair in exchange for the revenue they gain via sharing data.

Table 68: Liability problems with sharing data

How do you approach liability problems with data you share? Please indicate to what extent you agree with the following statements:						
Answer Options	**1 - Completely disagree**	**2 - Disagree**	**3 - Do not agree/do not disagree**	**4 - Agree**	**5 - Completely agree**	**I do not know**
The legislation is clear enough, so I do not impose any further liability restrictions through contracts or terms and conditions.	3	3	1	2	0	3
I try to exclude liability as far as possible in my contracts or terms and conditions.	2	0	1	4	2	3
I accept a degree of liability that I think is fair for the revenue I receive.	1	2	1	6	0	2
I contractually limit what people can do with my data and do not accept liability if they use it for a different purpose.	1	1	1	4	3	2
I sometimes negotiate with individual users of my data because they want additional liability assurance.	2	0	2	3	0	5
Answered Question						**12**

Source: Deloitte

Annex 4 - Approach to the impact assessment

In this annex, we first present our approach to the assessment of the impacts, including the assessment criteria, the types of costs and benefits to be considered and the data sources. Second, we present our approach for comparing the options and determining an order of priority, which is based on multi-criteria analysis.

In this annex, we first present our approach to the assessment of the impacts, including the assessment criteria, the types of costs and benefits to be considered and the data sources. Second, we present our approach for comparing the options and determining an order of priority, which is based on multi-criteria analysis.

Assessment of the impacts

Assessment criteria

The baseline scenario and policy options should be assessed based on different standardised assessment criteria for which quantitative and qualitative information is collected.

With a view to deciding which types of impacts need to be considered in this respect, we carried out a high level analysis of the policy options.

On this basis, we used the following **assessment criteria**:

- *Effectiveness* of the policy options in reaching the specific and general policy objectives;
- *Efficiency* of the policy options, i.e. an assessment of the benefits and the costs associated with the policy options, incl. the compliance of the options with the proportionality principle; and
- *Coherence* with existing EU policies.

This list incorporates economic, social, and legislative aspects.

The following table contains a mapping of the assessment criteria for the detailed assessment of the policy options.

Table 69: Assessment criteria to be considered for the detailed assessment of the policy options

Assessment criterion	Economic aspects	Social aspects / Fundamental Rights	Legislative aspects
Effectiveness of the policy options in reaching the…			
Specific objectives	• To reduce (the long-term) costs for businesses related to sharing data • To foster the sharing of data • To reduce prices for consumers	• To ensure consumer safety • To ensure compensation of damages for consumers	n/a
General objectives	• To contribute to fostering the development of innovative business models, products, and services	• To contribute to safeguarding Fundamental Rights • To contribute to fostering digital inclusion	n/a
Efficiency of the policy options			
Assessment of the relationship between costs and benefits (effectiveness, reduction of costs)	• *Compliance costs*, e.g. administrative burden and opportunity costs • Costs related to the *legal aspects*, e.g. lawyers' fees • Costs related to the *technical implementation*, e.g. procurement and/or development of hard- and software • Benefits, including cost savings (e.g. based on clearer legal framework or lower prices for data), as well as additional revenues (e.g. based on increased data sharing)	• *Transaction costs*, e.g. communication with stakeholders, training, monitoring and enforcement of legislation • Benefits related to the options	• Costs related to the *legislative framework*, e.g. changes to national legislation and the development of guidance for public administrations and businesses • Compliance of the options with the proportionality principle
Coherence of the policy options			
Assessment of the extent to which the policy options are coherent with existing EU policies	• Achievement of the Digital Single Market	• Data protection • Right to an effective remedy	• Existing rules on product liability or competition • Existing sector-specific rules

Source: Deloitte

To the extent possible, the assessment is built on **quantitative and qualitative information, incl. on costs and benefits**.

Types of costs and benefits

Data on **costs and benefits** are especially important with regard to the efficiency criterion.

The types of costs that are particularly relevant in the context of this assignment include:

- *Costs related to the legislative framework*, e.g. changes to national legislation and the development of guidance for public administrations and businesses;
- *Transaction costs*, e.g. communication with stakeholders, training, monitoring and enforcement of legislation;
- *Compliance costs*, e.g. administrative burden and opportunity costs;
- Costs related to the *legal aspects*, e.g. lawyers' fees; and
- Costs related to the *technical implementation*, e.g. procurement and/or development of hard- and software.

The benefits of the implementation the policy options refer to **reductions of some of the costs as well as other positive effects on (some of) the stakeholders**.

Differences and links between costs and benefits

An overall judgement about what policy option would be best from a costs and benefits perspective is challenging as, for instance, one policy option may bring about extensive benefits from the perspective of one type of company but mainly lead to costs for others. For example, an obligation to share data might provoke costs for those companies predominantly generating data, while other companies might benefit from being able to access additional data. Thus, the interpretation of what is considered a cost and what is considered a benefit depends on the point of view of the main types of stakeholders. In this context, it is helpful to link the assessment with the additional assessment criteria and apply a weighting factor for the different criteria (cf. the following section on MCA).

Data sources and limitations

We have taken various data sources into account for the assessment of the impacts, including:

- Desk research, including a legal analysis;
- Written consultations of stakeholders:
  - EU Commission public consultation;
  - Deloitte survey;
- Stakeholder interviews, including in the context of sector based case studies; and
- Several workshops with different groups of stakeholders, including Member States and businesses of various sectors and sizes.

Overall, while we aimed to collect an as comprehensive set of quantitative data as possible, **stakeholders were not able to provide us with the *ideal* set of information in relation to *all* types of costs and benefits**.

Thus, while we used quantification as far as possible based on the data available, **illustrative examples** (both in quantitative and qualitative fashion) of the effects that the policy options would have are used to complement the analysis. The aim of this exercise is to exemplify and demonstrate in which way and to what extent different stakeholders can be affected by costs and benefits to give a more "hands-on" understanding of the effects of the policy options.

Annex 5 - Supporting tables for the Multi-Criteria-Analysis

This Annex contains the tables presenting the results of the Multi-Criteria-Analysis

Policy ranking permutations

Table 70: Possible policy ranking permutations (120 in total)

#	A	B	C	D	E
1	BS	1A	1B	2A	2B
2	BS	1A	1B	2B	2A
3	BS	1A	2A	1B	2B
4	BS	1A	2A	2B	1B
5	BS	1A	2B	1B	2A
6	BS	1A	2B	2A	1B
7	BS	1B	1A	2A	2B
8	BS	1B	1A	2B	2A
9	BS	1B	2A	1A	2B
10	BS	1B	2A	2B	1A
11	BS	1B	2B	1A	2A
12	BS	1B	2B	2A	1A
13	BS	2A	1A	1B	2B
14	BS	2A	1A	2B	1B
15	BS	2A	1B	1A	2B
16	BS	2A	1B	2B	1A
17	BS	2A	2B	1A	1B
18	BS	2A	2B	1B	1A
19	BS	2B	1A	1B	2A
20	BS	2B	1A	2A	1B
21	BS	2B	1B	1A	2A
22	BS	2B	1B	2A	1A
23	BS	2B	2A	1A	1B
24	BS	2B	2A	1B	1A
25	1A	BS	1B	2A	2B
26	1A	BS	1B	2B	2A
27	1A	BS	2A	1B	2B
28	1A	BS	2A	2B	1B
29	1A	BS	2B	1B	2A
30	1A	BS	2B	2A	1B
31	1A	1B	BS	2A	2B
32	1A	1B	BS	2B	2A

#	A	B	C	D	E
33	1A	1B	2A	BS	2B
34	1A	1B	2A	2B	BS
35	1A	1B	2B	BS	2A
36	1A	1B	2B	2A	BS
37	1A	2A	BS	1B	2B
38	1A	2A	BS	2B	1B
39	1A	2A	1B	BS	2B
40	1A	2A	1B	2B	BS
41	1A	2A	2B	BS	1B
42	1A	2A	2B	1B	BS
43	1A	2B	BS	1B	2A
44	1A	2B	BS	2A	1B
45	1A	2B	1B	BS	2A
46	1A	2B	1B	2A	BS
47	1A	2B	2A	BS	1B
48	1A	2B	2A	1B	BS
49	1B	BS	1A	2A	2B
50	1B	BS	1A	2B	2A
51	1B	BS	2A	1A	2B
52	1B	BS	2A	2B	1A
53	1B	BS	2B	1A	2A
54	1B	BS	2B	2A	1A
55	1B	1A	BS	2A	2B
56	1B	1A	BS	2B	2A
57	1B	1A	2A	BS	2B
58	1B	1A	2A	2B	BS
59	1B	1A	2B	BS	2A
60	1B	1A	2B	2A	BS
61	1B	2A	BS	1A	2B
62	1B	2A	BS	2B	1A
63	1B	2A	1A	BS	2B
64	1B	2A	1A	2B	BS
65	1B	2A	2B	BS	1A
66	1B	2A	2B	1A	BS
67	1B	2B	BS	1A	2A
68	1B	2B	BS	2A	1A
69	1B	2B	1A	BS	2A
70	1B	2B	1A	2A	BS
71	1B	2B	2A	BS	1A
72	1B	2B	2A	1A	BS
73	2A	BS	1A	1B	2B
74	2A	BS	1A	2B	1B
75	2A	BS	1B	1A	2B
76	2A	BS	1B	2B	1A
77	2A	BS	2B	1A	1B
78	2A	BS	2B	1B	1A

#	A	B	C	D	E
79	2A	1A	BS	1B	2B
80	2A	1A	BS	2B	1B
81	2A	1A	1B	BS	2B
82	2A	1A	1B	2B	BS
83	2A	1A	2B	BS	1B
84	2A	1A	2B	1B	BS
85	2A	1B	BS	1A	2B
86	2A	1B	BS	2B	1A
87	2A	1B	1A	BS	2B
88	2A	1B	1A	2B	BS
89	2A	1B	2B	BS	1A
90	2A	1B	2B	1A	BS
91	2A	2B	BS	1A	1B
92	2A	2B	BS	1B	1A
93	2A	2B	1A	BS	1B
94	2A	2B	1A	1B	BS
95	2A	2B	1B	BS	1A
96	2A	2B	1B	1A	BS
97	2B	BS	1A	1B	2A
98	2B	BS	1A	2A	1B
99	2B	BS	1B	1A	2A
100	2B	BS	1B	2A	1A
101	2B	BS	2A	1A	1B
102	2B	BS	2A	1B	1A
103	2B	1A	BS	1B	2A
104	2B	1A	BS	2A	1B
105	2B	1A	1B	BS	2A
106	2B	1A	1B	2A	BS
107	2B	1A	2A	BS	1B
108	2B	1A	2A	1B	BS
109	2B	1B	BS	1A	2A
110	2B	1B	BS	2A	1A
111	2B	1B	1A	BS	2A
112	2B	1B	1A	2A	BS
113	2B	1B	2A	BS	1A
114	2B	1B	2A	1A	BS
115	2B	2A	BS	1A	1B
116	2B	2A	BS	1B	1A
117	2B	2A	1A	BS	1B
118	2B	2A	1A	1B	BS
119	2B	2A	1B	BS	1A
120	2B	2A	1B	1A	BS

Source: Deloitte.

Policy pairings within the possible policy ranking permutations

Table 71: All policy pairings within each of the 120 possible policy ranking permutations

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE
1	BS1A	BS1B	BS2A	BS2B	1A1B	1A2A	1A2B	1B2A	1B2B	2A2B
2	BS1A	BS1B	BS2B	BS2A	1A1B	1A2B	1A2A	1B2B	1B2A	2B2A
3	BS1A	BS2A	BS1B	BS2B	1A2A	1A1B	1A2B	2A1B	2A2B	1B2B
4	BS1A	BS2A	BS2B	BS1B	1A2A	1A2B	1A1B	2A2B	2A1B	2B1B
5	BS1A	BS2B	BS1B	BS2A	1A2B	1A1B	1A2A	2B1B	2B2A	1B2A
6	BS1A	BS2B	BS2A	BS1B	1A2B	1A2A	1A1B	2B2A	2B1B	2A1B
7	BS1B	BS1A	BS2A	BS2B	1B1A	1B2A	1B2B	1A2A	1A2B	2A2B
8	BS1B	BS1A	BS2B	BS2A	1B1A	1B2B	1B2A	1A2B	1A2A	2B2A
9	BS1B	BS2A	BS1A	BS2B	1B2A	1B1A	1B2B	2A1A	2A2B	1A2B
10	BS1B	BS2A	BS2B	BS1A	1B2A	1B2B	1B1A	2A2B	2A1A	2B1A
11	BS1B	BS2B	BS1A	BS2A	1B2B	1B1A	1B2A	2B1A	2B2A	1A2A
12	BS1B	BS2B	BS2A	BS1A	1B2B	1B2A	1B1A	2B2A	2B1A	2A1A
13	BS2A	BS1A	BS1B	BS2B	2A1A	2A1B	2A2B	1A1B	1A2B	1B2B
14	BS2A	BS1A	BS2B	BS1B	2A1A	2A2B	2A1B	1A2B	1A1B	2B1B
15	BS2A	BS1B	BS1A	BS2B	2A1B	2A1A	2A2B	1B1A	1B2B	1A2B
16	BS2A	BS1B	BS2B	BS1A	2A1B	2A2B	2A1A	1B2B	1B1A	2B1A
17	BS2A	BS2B	BS1A	BS1B	2A2B	2A1A	2A1B	2B1A	2B1B	1A1B
18	BS2A	BS2B	BS1B	BS1A	2A2B	2A1B	2A1A	2B1B	2B1A	1B1A
19	BS2B	BS1A	BS1B	BS2A	2B1A	2B1B	2B2A	1A1B	1A2A	1B2A
20	BS2B	BS1A	BS2A	BS1B	2B1A	2B2A	2B1B	1A2A	1A1B	2A1B
21	BS2B	BS1B	BS1A	BS2A	2B1B	2B1A	2B2A	1B1A	1B2A	1A2A
22	BS2B	BS1B	BS2A	BS1A	2B1B	2B2A	2B1A	1B2A	1B1A	2A1A
23	BS2B	BS2A	BS1A	BS1B	2B2A	2B1A	2B1B	2A1A	2A1B	1A1B
24	BS2B	BS2A	BS1B	BS1A	2B2A	2B1B	2B1A	2A1B	2A1A	1B1A
25	1ABS	1A1B	1A2A	1A2B	BS1B	BS2A	BS2B	1B2A	1B2B	2A2B
26	1ABS	1A1B	1A2B	1A2A	BS1B	BS2B	BS2A	1B2B	1B2A	2B2A
27	1ABS	1A2A	1A1B	1A2B	BS2A	BS1B	BS2B	2A1B	2A2B	1B2B

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE
28	1ABS	1A2A	1A2B	1A1B	BS2A	BS2B	BS1B	2A2B	2A1B	2B1B
29	1ABS	1A2B	1A1B	1A2A	BS2B	BS1B	BS2A	2B1B	2B2A	1B2A
30	1ABS	1A2B	1A2A	1A1B	BS2B	BS2A	BS1B	2B2A	2B1B	2A1B
31	1A1B	1ABS	1A2A	1A2B	1BBS	1B2A	1B2B	BS2A	BS2B	2A2B
32	1A1B	1ABS	1A2B	1A2A	1BBS	1B2B	1B2A	BS2B	BS2A	2B2A
33	1A1B	1A2A	1ABS	1A2B	1B2A	1BBS	1B2B	2ABS	2A2B	BS2B
34	1A1B	1A2A	1A2B	1ABS	1B2A	1B2B	1BBS	2A2B	2ABS	2BBS
35	1A1B	1A2B	1ABS	1A2A	1B2B	1BBS	1B2A	2BBS	2B2A	BS2A
36	1A1B	1A2B	1A2A	1ABS	1B2B	1B2A	1BBS	2B2A	2BBS	2ABS
37	1A2A	1ABS	1A1B	1A2B	2ABS	2A1B	2A2B	BS1B	BS2B	1B2B
38	1A2A	1ABS	1A2B	1A1B	2ABS	2A2B	2A1B	BS2B	BS1B	2B1B
39	1A2A	1A1B	1ABS	1A2B	2A1B	2ABS	2A2B	1BBS	1B2B	BS2B
40	1A2A	1A1B	1A2B	1ABS	2A1B	2A2B	2ABS	1B2B	1BBS	2BBS
41	1A2A	1A2B	1ABS	1A1B	2A2B	2ABS	2A1B	2BBS	2B1B	BS1B
42	1A2A	1A2B	1A1B	1ABS	2A2B	2A1B	2ABS	2B1B	2BBS	1BBS
43	1A2B	1ABS	1A1B	1A2A	2BBS	2B1B	2B2A	BS1B	BS2A	1B2A
44	1A2B	1ABS	1A2A	1A1B	2BBS	2B2A	2B1B	BS2A	BS1B	2A1B
45	1A2B	1A1B	1ABS	1A2A	2B1B	2BBS	2B2A	1BBS	1B2A	BS2A
46	1A2B	1A1B	1A2A	1ABS	2B1B	2B2A	2BBS	1B2A	1BBS	2ABS
47	1A2B	1A2A	1ABS	1A1B	2B2A	2BBS	2B1B	2ABS	2A1B	BS1B
48	1A2B	1A2A	1A1B	1ABS	2B2A	2B1B	2BBS	2A1B	2ABS	1BBS
49	1BBS	1B1A	1B2A	1B2B	BS1A	BS2A	BS2B	1A2A	1A2B	2A2B
50	1BBS	1B1A	1B2B	1B2A	BS1A	BS2B	BS2A	1A2B	1A2A	2B2A
51	1BBS	1B2A	1B1A	1B2B	BS2A	BS1A	BS2B	2A1A	2A2B	1A2B
52	1BBS	1B2A	1B2B	1B1A	BS2A	BS2B	BS1A	2A2B	2A1A	2B1A
53	1BBS	1B2B	1B1A	1B2A	BS2B	BS1A	BS2A	2B1A	2B2A	1A2A
54	1BBS	1B2B	1B2A	1B1A	BS2B	BS2A	BS1A	2B2A	2B1A	2A1A
55	1B1A	1BBS	1B2A	1B2B	1ABS	1A2A	1A2B	BS2A	BS2B	2A2B
56	1B1A	1BBS	1B2B	1B2A	1ABS	1A2B	1A2A	BS2B	BS2A	2B2A

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE
57	1B1A	1B2A	1BBS	1B2B	1A2A	1ABS	1A2B	2ABS	2A2B	BS2B
58	1B1A	1B2A	1B2B	1BBS	1A2A	1A2B	1ABS	2A2B	2ABS	2BBS
59	1B1A	1B2B	1BBS	1B2A	1A2B	1ABS	1A2A	2BBS	2B2A	BS2A
60	1B1A	1B2B	1B2A	1BBS	1A2B	1A2A	1ABS	2B2A	2BBS	2ABS
61	1B2A	1BBS	1B1A	1B2B	2ABS	2A1A	2A2B	BS1A	BS2B	1A2B
62	1B2A	1BBS	1B2B	1B1A	2ABS	2A2B	2A1A	BS2B	BS1A	2B1A
63	1B2A	1B1A	1BBS	1B2B	2A1A	2ABS	2A2B	1ABS	1A2B	BS2B
64	1B2A	1B1A	1B2B	1BBS	2A1A	2A2B	2ABS	1A2B	1ABS	2BBS
65	1B2A	1B2B	1BBS	1B1A	2A2B	2ABS	2A1A	2BBS	2B1A	BS1A
66	1B2A	1B2B	1B1A	1BBS	2A2B	2A1A	2ABS	2B1A	2BBS	1ABS
67	1B2B	1BBS	1B1A	1B2A	2BBS	2B1A	2B2A	BS1A	BS2A	1A2A
68	1B2B	1BBS	1B2A	1B1A	2BBS	2B2A	2B1A	BS2A	BS1A	2A1A
69	1B2B	1B1A	1BBS	1B2A	2B1A	2BBS	2B2A	1ABS	1A2A	BS2A
70	1B2B	1B1A	1B2A	1BBS	2B1A	2B2A	2BBS	1A2A	1ABS	2ABS
71	1B2B	1B2A	1BBS	1B1A	2B2A	2BBS	2B1A	2ABS	2A1A	BS1A
72	1B2B	1B2A	1B1A	1BBS	2B2A	2B1A	2BBS	2A1A	2ABS	1ABS
73	2ABS	2A1A	2A1B	2A2B	BS1A	BS1B	BS2B	1A1B	1A2B	1B2B
74	2ABS	2A1A	2A2B	2A1B	BS1A	BS2B	BS1B	1A2B	1A1B	2B1B
75	2ABS	2A1B	2A1A	2A2B	BS1B	BS1A	BS2B	1B1A	1B2B	1A2B
76	2ABS	2A1B	2A2B	2A1A	BS1B	BS2B	BS1A	1B2B	1B1A	2B1A
77	2ABS	2A2B	2A1A	2A1B	BS2B	BS1A	BS1B	2B1A	2B1B	1A1B
78	2ABS	2A2B	2A1B	2A1A	BS2B	BS1B	BS1A	2B1B	2B1A	1B1A
79	2A1A	2ABS	2A1B	2A2B	1ABS	1A1B	1A2B	BS1B	BS2B	1B2B
80	2A1A	2ABS	2A2B	2A1B	1ABS	1A2B	1A1B	BS2B	BS1B	2B1B
81	2A1A	2A1B	2ABS	2A2B	1A1B	1ABS	1A2B	1BBS	1B2B	BS2B
82	2A1A	2A1B	2A2B	2ABS	1A1B	1A2B	1ABS	1B2B	1BBS	2BBS
83	2A1A	2A2B	2ABS	2A1B	1A2B	1ABS	1A1B	2BBS	2B1B	BS1B
84	2A1A	2A2B	2A1B	2ABS	1A2B	1A1B	1ABS	2B1B	2BBS	1BBS
85	2A1B	2ABS	2A1A	2A2B	1BBS	1B1A	1B2B	BS1A	BS2B	1A2B

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE
86	2A1B	2ABS	2A2B	2A1A	1BBS	1B2B	1B1A	BS2B	BS1A	2B1A
87	2A1B	2A1A	2ABS	2A2B	1B1A	1BBS	1B2B	1ABS	1A2B	BS2B
88	2A1B	2A1A	2A2B	2ABS	1B1A	1B2B	1BBS	1A2B	1ABS	2BBS
89	2A1B	2A2B	2ABS	2A1A	1B2B	1BBS	1B1A	2BBS	2B1A	BS1A
90	2A1B	2A2B	2A1A	2ABS	1B2B	1B1A	1BBS	2B1A	2BBS	1ABS
91	2A2B	2ABS	2A1A	2A1B	2BBS	2B1A	2B1B	BS1A	BS1B	1A1B
92	2A2B	2ABS	2A1B	2A1A	2BBS	2B1B	2B1A	BS1B	BS1A	1B1A
93	2A2B	2A1A	2ABS	2A1B	2B1A	2BBS	2B1B	1ABS	1A1B	BS1B
94	2A2B	2A1A	2A1B	2ABS	2B1A	2B1B	2BBS	1A1B	1ABS	1BBS
95	2A2B	2A1B	2ABS	2A1A	2B1B	2BBS	2B1A	1BBS	1B1A	BS1A
96	2A2B	2A1B	2A1A	2ABS	2B1B	2B1A	2BBS	1B1A	1BBS	1ABS
97	2BBS	2B1A	2B1B	2B2A	BS1A	BS1B	BS2A	1A1B	1A2A	1B2A
98	2BBS	2B1A	2B2A	2B1B	BS1A	BS2A	BS1B	1A2A	1A1B	2A1B
99	2BBS	2B1B	2B1A	2B2A	BS1B	BS1A	BS2A	1B1A	1B2A	1A2A
100	2BBS	2B1B	2B2A	2B1A	BS1B	BS2A	BS1A	1B2A	1B1A	2A1A
101	2BBS	2B2A	2B1A	2B1B	BS2A	BS1A	BS1B	2A1A	2A1B	1A1B
102	2BBS	2B2A	2B1B	2B1A	BS2A	BS1B	BS1A	2A1B	2A1A	1B1A
103	2B1A	2BBS	2B1B	2B2A	1ABS	1A1B	1A2A	BS1B	BS2A	1B2A
104	2B1A	2BBS	2B2A	2B1B	1ABS	1A2A	1A1B	BS2A	BS1B	2A1B
105	2B1A	2B1B	2BBS	2B2A	1A1B	1ABS	1A2A	1BBS	1B2A	BS2A
106	2B1A	2B1B	2B2A	2BBS	1A1B	1A2A	1ABS	1B2A	1BBS	2ABS
107	2B1A	2B2A	2BBS	2B1B	1A2A	1ABS	1A1B	2ABS	2A1B	BS1B
108	2B1A	2B2A	2B1B	2BBS	1A2A	1A1B	1ABS	2A1B	2ABS	1BBS
109	2B1B	2BBS	2B1A	2B2A	1BBS	1B1A	1B2A	BS1A	BS2A	1A2A
110	2B1B	2BBS	2B2A	2B1A	1BBS	1B2A	1B1A	BS2A	BS1A	2A1A
111	2B1B	2B1A	2BBS	2B2A	1B1A	1BBS	1B2A	1ABS	1A2A	BS2A
112	2B1B	2B1A	2B2A	2BBS	1B1A	1B2A	1BBS	1A2A	1ABS	2ABS
113	2B1B	2B2A	2BBS	2B1A	1B2A	1BBS	1B1A	2ABS	2A1A	BS1A
114	2B1B	2B2A	2B1A	2BBS	1B2A	1B1A	1BBS	2A1A	2ABS	1ABS

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE
115	2B2A	2BBS	2B1A	2B1B	2ABS	2A1A	2A1B	BS1A	BS1B	1A1B
116	2B2A	2BBS	2B1B	2B1A	2ABS	2A1B	2A1A	BS1B	BS1A	1B1A
117	2B2A	2B1A	2BBS	2B1B	2A1A	2ABS	2A1B	1ABS	1A1B	BS1B
118	2B2A	2B1A	2B1B	2BBS	2A1A	2A1B	2ABS	1A1B	1ABS	1BBS
119	2B2A	2B1B	2BBS	2B1A	2A1B	2ABS	2A1A	1BBS	1B1A	BS1A
120	2B2A	2B1B	2B1A	2BBS	2A1B	2A1A	2ABS	1B1A	1BBS	1ABS

Source: Deloitte

Coefficients of all policy pairings

Table 72: Coefficients of all policy pairings within each of the 120 possible policy ranking permutations

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE	Total
1	0	0	2.5	2.5	1.5	2.5	2.5	2.5	2.5	1.5	18
2	0	0	2.5	2.5	1.5	2.5	2.5	2.5	2.5	0	16.5
3	0	2.5	0	2.5	2.5	1.5	2.5	0	1.5	2.5	15.5
4	0	2.5	2.5	0	2.5	2.5	1.5	1.5	0	0	13
5	0	2.5	0	2.5	2.5	1.5	2.5	0	0	2.5	14
6	0	2.5	2.5	0	2.5	2.5	1.5	0	0	0	11.5
7	0	0	2.5	2.5	0	2.5	2.5	2.5	2.5	1.5	16.5
8	0	0	2.5	2.5	0	2.5	2.5	2.5	2.5	0	15
9	0	2.5	0	2.5	2.5	0	2.5	0	1.5	2.5	14
10	0	2.5	2.5	0	2.5	2.5	0	1.5	0	0	11.5
11	0	2.5	0	2.5	2.5	0	2.5	0	0	2.5	12.5
12	0	2.5	2.5	0	2.5	2.5	0	0	0	0	10
13	2.5	0	0	2.5	0	0	1.5	1.5	2.5	2.5	13
14	2.5	0	2.5	0	0	1.5	0	2.5	1.5	0	10.5
15	2.5	0	0	2.5	0	0	1.5	0	2.5	2.5	11.5
16	2.5	0	2.5	0	0	1.5	0	2.5	0	0	9
17	2.5	2.5	0	0	1.5	0	0	0	0	1.5	8
18	2.5	2.5	0	0	1.5	0	0	0	0	0	6.5
19	2.5	0	0	2.5	0	0	0	1.5	2.5	2.5	11.5
20	2.5	0	2.5	0	0	0	0	2.5	1.5	0	9
21	2.5	0	0	2.5	0	0	0	0	2.5	2.5	10
22	2.5	0	2.5	0	0	0	0	2.5	0	0	7.5
23	2.5	2.5	0	0	0	0	0	0	0	1.5	6.5
24	2.5	2.5	0	0	0	0	0	0	0	0	5
25	4.5	1.5	2.5	2.5	0	2.5	2.5	2.5	2.5	1.5	22.5
26	4.5	1.5	2.5	2.5	0	2.5	2.5	2.5	2.5	0	21
27	4.5	2.5	1.5	2.5	2.5	0	2.5	0	1.5	2.5	20
28	4.5	2.5	2.5	1.5	2.5	2.5	0	1.5	0	0	17.5
29	4.5	2.5	1.5	2.5	2.5	0	2.5	0	0	2.5	18.5
30	4.5	2.5	2.5	1.5	2.5	2.5	0	0	0	0	16
31	1.5	4.5	2.5	2.5	4.5	2.5	2.5	2.5	2.5	1.5	27
32	1.5	4.5	2.5	2.5	4.5	2.5	2.5	2.5	2.5	0	25.5
33	1.5	2.5	4.5	2.5	2.5	4.5	2.5	2	1.5	2.5	26.5
34	1.5	2.5	2.5	4.5	2.5	2.5	4.5	1.5	2	2	26
35	1.5	2.5	4.5	2.5	2.5	4.5	2.5	2	0	2.5	25
36	1.5	2.5	2.5	4.5	2.5	2.5	4.5	0	2	2	24.5
37	2.5	4.5	1.5	2.5	2	0	1.5	0	2.5	2.5	19.5
38	2.5	4.5	2.5	1.5	2	1.5	0	2.5	0	0	17
39	2.5	1.5	4.5	2.5	0	2	1.5	4.5	2.5	2.5	24
40	2.5	1.5	2.5	4.5	0	1.5	2	2.5	4.5	2	23.5
41	2.5	2.5	4.5	1.5	1.5	2	0	2	0	0	16.5
42	2.5	2.5	1.5	4.5	1.5	0	2	0	2	4.5	21

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE	Total
43	2.5	4.5	1.5	2.5	2	0	0	0	2.5	2.5	18
44	2.5	4.5	2.5	1.5	2	0	0	2.5	0	0	15.5
45	2.5	1.5	4.5	2.5	0	2	0	4.5	2.5	2.5	22.5
46	2.5	1.5	2.5	4.5	0	0	2	2.5	4.5	2	22
47	2.5	2.5	4.5	1.5	0	2	0	2	0	0	15
48	2.5	2.5	1.5	4.5	0	0	2	0	2	4.5	19.5
49	4.5	0	2.5	2.5	0	2.5	2.5	2.5	2.5	1.5	21
50	4.5	0	2.5	2.5	0	2.5	2.5	2.5	2.5	0	19.5
51	4.5	2.5	0	2.5	2.5	0	2.5	0	1.5	2.5	18.5
52	4.5	2.5	2.5	0	2.5	2.5	0	1.5	0	0	16
53	4.5	2.5	0	2.5	2.5	0	2.5	0	0	2.5	17
54	4.5	2.5	2.5	0	2.5	2.5	0	0	0	0	14.5
55	0	4.5	2.5	2.5	4.5	2.5	2.5	2.5	2.5	1.5	25.5
56	0	4.5	2.5	2.5	4.5	2.5	2.5	2.5	2.5	0	24
57	0	2.5	4.5	2.5	2.5	4.5	2.5	2	1.5	2.5	25
58	0	2.5	2.5	4.5	2.5	2.5	4.5	1.5	2	2	24.5
59	0	2.5	4.5	2.5	2.5	4.5	2.5	2	0	2.5	23.5
60	0	2.5	2.5	4.5	2.5	2.5	4.5	0	2	2	23
61	2.5	4.5	0	2.5	2	0	1.5	0	2.5	2.5	18
62	2.5	4.5	2.5	0	2	1.5	0	2.5	0	0	15.5
63	2.5	0	4.5	2.5	0	2	1.5	4.5	2.5	2.5	22.5
64	2.5	0	2.5	4.5	0	1.5	2	2.5	4.5	2	22
65	2.5	2.5	4.5	0	1.5	2	0	2	0	0	15
66	2.5	2.5	0	4.5	1.5	0	2	0	2	4.5	19.5
67	2.5	4.5	0	2.5	2	0	0	0	2.5	2.5	16.5
68	2.5	4.5	2.5	0	2	0	0	2.5	0	0	14
69	2.5	0	4.5	2.5	0	2	0	4.5	2.5	2.5	21
70	2.5	0	2.5	4.5	0	0	2	2.5	4.5	2	20.5
71	2.5	2.5	4.5	0	0	2	0	2	0	0	13.5
72	2.5	2.5	0	4.5	0	0	2	0	2	4.5	18
73	2	0	0	1.5	0	0	2.5	1.5	2.5	2.5	12.5
74	2	0	1.5	0	0	2.5	0	2.5	1.5	0	10
75	2	0	0	1.5	0	0	2.5	0	2.5	2.5	11
76	2	0	1.5	0	0	2.5	0	2.5	0	0	8.5
77	2	1.5	0	0	2.5	0	0	0	0	1.5	7.5
78	2	1.5	0	0	2.5	0	0	0	0	0	6
79	0	2	0	1.5	4.5	1.5	2.5	0	2.5	2.5	17
80	0	2	1.5	0	4.5	2.5	1.5	2.5	0	0	14.5
81	0	0	2	1.5	1.5	4.5	2.5	4.5	2.5	2.5	21.5
82	0	0	1.5	2	1.5	2.5	4.5	2.5	4.5	2	21
83	0	1.5	2	0	2.5	4.5	1.5	2	0	0	14
84	0	1.5	0	2	2.5	1.5	4.5	0	2	4.5	18.5
85	0	2	0	1.5	4.5	0	2.5	0	2.5	2.5	15.5
86	0	2	1.5	0	4.5	2.5	0	2.5	0	0	13
87	0	0	2	1.5	0	4.5	2.5	4.5	2.5	2.5	20
88	0	0	1.5	2	0	2.5	4.5	2.5	4.5	2	19.5

#	AB	AC	AD	AE	BC	BD	BE	CD	CE	DE	Total
89	0	1.5	2	0	2.5	4.5	0	2	0	0	12.5
90	0	1.5	0	2	2.5	0	4.5	0	2	4.5	17
91	1.5	2	0	0	2	0	0	0	0	1.5	7
92	1.5	2	0	0	2	0	0	0	0	0	5.5
93	1.5	0	2	0	0	2	0	4.5	1.5	0	11.5
94	1.5	0	0	2	0	0	2	1.5	4.5	4.5	16
95	1.5	0	2	0	0	2	0	4.5	0	0	10
96	1.5	0	0	2	0	0	2	0	4.5	4.5	14.5
97	2	0	0	0	0	0	2.5	1.5	2.5	2.5	11
98	2	0	0	0	0	2.5	0	2.5	1.5	0	8.5
99	2	0	0	0	0	0	2.5	0	2.5	2.5	9.5
100	2	0	0	0	0	2.5	0	2.5	0	0	7
101	2	0	0	0	2.5	0	0	0	0	1.5	6
102	2	0	0	0	2.5	0	0	0	0	0	4.5
103	0	2	0	0	4.5	1.5	2.5	0	2.5	2.5	15.5
104	0	2	0	0	4.5	2.5	1.5	2.5	0	0	13
105	0	0	2	0	1.5	4.5	2.5	4.5	2.5	2.5	20
106	0	0	0	2	1.5	2.5	4.5	2.5	4.5	2	19.5
107	0	0	2	0	2.5	4.5	1.5	2	0	0	12.5
108	0	0	0	2	2.5	1.5	4.5	0	2	4.5	17
109	0	2	0	0	4.5	0	2.5	0	2.5	2.5	14
110	0	2	0	0	4.5	2.5	0	2.5	0	0	11.5
111	0	0	2	0	0	4.5	2.5	4.5	2.5	2.5	18.5
112	0	0	0	2	0	2.5	4.5	2.5	4.5	2	18
113	0	0	2	0	2.5	4.5	0	2	0	0	11
114	0	0	0	2	2.5	0	4.5	0	2	4.5	15.5
115	0	2	0	0	2	0	0	0	0	1.5	5.5
116	0	2	0	0	2	0	0	0	0	0	4
117	0	0	2	0	0	2	0	4.5	1.5	0	10
118	0	0	0	2	0	0	2	1.5	4.5	4.5	14.5
119	0	0	2	0	0	2	0	4.5	0	0	8.5
120	0	0	0	2	0	0	2	0	4.5	4.5	13

Source: Deloitte

European Commission

Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability

Luxembourg, Publications Office of the European Union

2018 – 433 pages

ISBN 978-92-79-76987-0
DOI: 10.2759/781960

KK-07-17-132-ENN

Publications Office

doi: 10.2759/781960

ISBN 978-92-79-76987-0