EUROPEAN
COMMISSION

Brussels, 10.1.2017
SWD(2017) 2 final

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

{COM(2017) 9 final}

Staff working document

Accompanying

The Communication "Building a European Data Economy"

Part 1: Context and purpose of this document

A thriving data-driven economy is essential for innovation, growth, jobs and European competitiveness as well as for a functional Digital Single Market. The Communication "Towards a data-driven economy"[1] presents a vision for the data-driven economy as an ecosystem with different types of players (e.g. data providers, data analytics companies, skilled data and software professionals, cloud service providers, companies from the user industries, venture capitalists, entrepreneurs, public services, research institutes and universities), leading to more business opportunities, in particular for SMEs. The availability of good quality, reliable and interoperable datasets was specifically highlighted as an important enabler for new data products.

Building on this, the Digital Single Market strategy[2] outlined a set of concrete actions to address existing barriers to the free flow of data across borders and sectors. It emphasised the commitment of the EU to the highest standards of protection of personal data. In this respect it expressed the view that the General Data Protection Regulation (GDPR) – still under discussion at the time – would increase trust in digital services through the protection it would offer to individuals with respect to the processing of their personal data. Subsequently, the GDPR was adopted. It constitutes a comprehensive and complete framework with respect to processing of personal data.

The Communication "Building a European Data Economy" that this Staff Working Document accompanies suggests that Europe is not tapping into the potential of data for business, research and innovation purposes. In this document, the Commission sets out the policy context and a first analysis of the problem drivers on these emerging issues together with a non-exhaustive list of broad principles that could help shaping an EU framework for the free flow of data and improved sharing of commercial data and in particular machine-generated data which are either non-personal in nature or personal data that have been anonymised.

The purpose of this Staff Working Document is to provide additional evidence and a detailed description of the emerging issues relevant for the EU data economy. The objective is to inform the debate and in particular the stakeholder consultation announced in the Communication. It builds on preliminary available evidence and a first set of stakeholder consultation meetings.

[1] COM(2014)442 final of 2 July 2014.
[2] COM(2015)192 final of 6 May 2015.

Part 2: Free Flow of Data

1. Introduction

Since the 2012 Communication "Unleashing the Potential of Cloud Computing in Europe", the Commission efforts focused on improving the uptake of cloud-based IT services and on removing barriers that preclude such uptake within the EU boundaries, since in a data-driven economy industrial competitiveness depends on the widespread use of data services, enabled by technologies, such as cloud computing. This new industrial revolution is bound to reshape entire business sectors, such as automotive, aerospace, logistics, energy, finance, manufacturing, agriculture and of course, the ICT sector.

Part of building a vibrant European Data Economy is to enable providers and users of data-driven services, such as cloud computing, to benefit from a single market that does not restrict the flow of data across borders.

2. Typology of data localisation restrictions

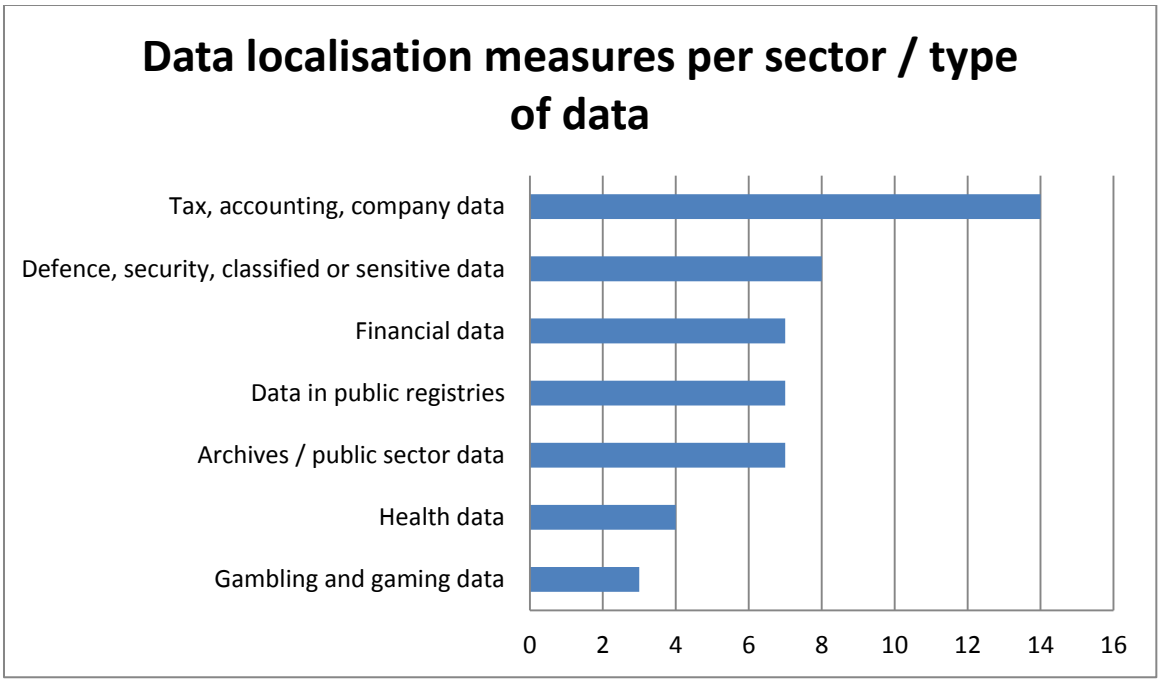
Data localisation stems from legal rules or administrative guidelines or practices that dictate or influence the localisation of data for its storage or processing. Such requirements restrict the free flow of data between regions or Member States within the European Union.

The analysis of a sample of 50 data localisation restrictions in 21 Member States[3] shows that the highest share of data localisation restrictions applies across sectors and, in many cases, to privately-held data: e.g. accounting documents and tax records, invoices or company records and registers. Legal provisions include localisation of invoices, books and records, accounting documents, commercial letters on the very premises of the company in some cases, or on servers within the country, in other, less restrictive, laws.

Government and public sector data are also concerned by restrictions – e.g. judicial records and other public records, national registries, and national archives. In some Member States, strong provisions exist, such as the obligation for a state-owned data processing facility to process and store electronic registries, or complete prohibition for local authorities to use cloud services without a special certification for storing and processing any document received by the public authorities.

Sector-specific restrictions concern in particular health and financial data, but also gaming and gambling:

[3] Identified in Time.lex, Spark Legal Network and Consultancy, Tech4i2, Cross-border data flow in the digital single market: study on data location restrictions, 2016, https://ec.europa.eu/digital-single-market/news-redirect/51708, London Economics, Facilitating cross border data flow in the Digital Single Market, 2016, https://ec.europa.eu/digital-single-market/news-redirect/51704 and other relevant inputs from Member States and industry that contribute towards the European Commission's activities in the policy area of data localisation rules.

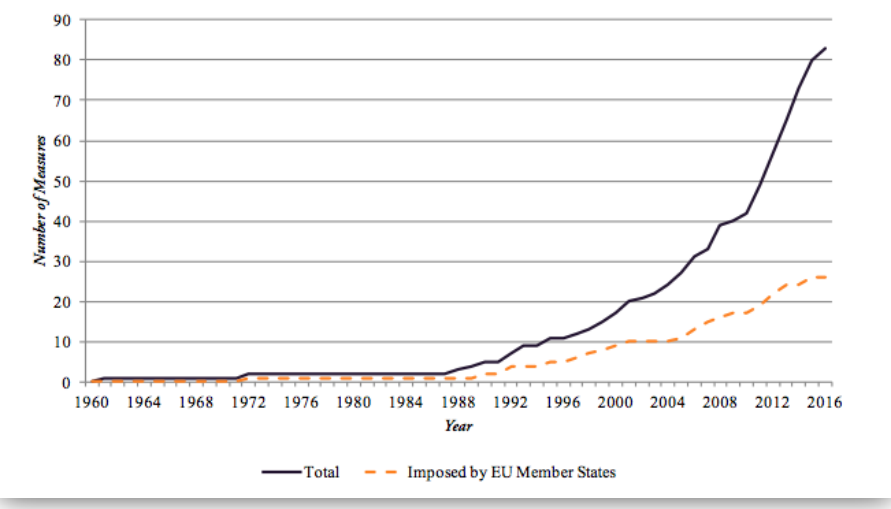


The presence and the scale of restrictions vary depending on the Member State: the analysis identified up to twelve restrictions in one country, whereas for the majority of the Member States one (8 countries) or two (7 countries) restrictions were reported.

It should, however, be noted that the numbers of localisation measures indicated in this section is not necessarily a reflection of the magnitude of the problem as certain data localisation measures can have an impact across sectors.

Moreover, further barriers are likely to emerge from numerous administrative rules and practices[4] and the trend, both globally (+160% since 2006[5]) and in Europe (+100% since 2006[6]), is towards more data localisation:

[4] For example, an internal verification has revealed that the sample of 50 restrictions contains 3 localisation requirements in the online gambling sector out of the total of around 11 such requirements identified by the Commission services.
[5] From around 31 restriction in 2006 to around 81 restriction in 2016.
[6] From around 13 restrictions in 2006 to around 26 restrictions in 2016.



Number of data localisation measures implemented globally and intra-European Union (ECIPE, Digital Trade Estimates, 2016)

It should also be stressed that the market players detect a strong perception of the need to localise data, despite the actual legal situation. A study outlined that "perceptions are as powerful as hard restrictions in deterring cross-border data transfers".[7]

While security risks are ranked high in the users' options[8] for ICT services, security-oriented data localisation measures fail to take account of advances in technology, not least brought about by the distributed nature of the Internet, and the possibilities they present for access, retrieval, distributed packets and multiple locations and encryption of data. In most cases, the level of security of data in electronic format does not depend on its storage location, but rather on the security of the IT infrastructure and strength of the encryption techniques used. Ways to achieve secure data storage or processing include removing obstacles to keep data in larger state of the art data centres, which are much less vulnerable to attacks, and enabling cross-border cooperation, i.e. one data centre being the back-up of another located in a different Member State.

3. The economic and environmental impact of data localisation requirements

In 2014 alone, cross-border data flows generated $2.8 trillion in economic value exceeding the value of global trade in goods. Such growth reflects not just the dynamism of the technology industry, but also the digitization of the economy as a whole. Digital trade is crucial for nearly all firms, from large multinationals to small businesses that rely on online platforms to connect and trade with customers around the world.[9]

[7] London Economics, Facilitating cross border data flow in the Digital Single Market, 2016.
[8] A survey by Eurostat points to 57% of large companies and 38% of SMEs concerned with the risks of security breaches when using cloud computing services (Eurostat, "Cloud computing - statistics on the use by enterprises", 2014 http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises).
[9] McKinsey Global Institute, "Digital Globalization: the New Era of Global Flows", 2016.

International Monetary Fund (IMF) data from 2008 to 2012 presents cross-border information flows as the fastest growing component of US as well as EU trade.[10] A study by Mandel[11] found these flows to have increased by 49% over the period while trade in goods and services simultaneously grew by only 2.4%. Comparing the EU and the US in data flows, cross border data flows in the United States are roughly 16-25% of all U.S data traffic whereas Europe compares roughly with 13-16%.

Energy costs, planning laws and tax regimes are important factors when deciding on data centre locations. But market size is the prime factor, and the fragmented nature of data storage in the EU brought about by data localisation requirements explains partly why only 4% of world data is stored in the EU. The free flow of data is a necessary pre-condition to the development of large data centres serving the continent and attracting data business to Europe. Currently, out of the top 25 public cloud service providers active on the EU market, 17 with headquarters in the US collectively generate 83% of revenues. Seven EU-based providers account for 14%.[12] The remaining 3% of revenues are spread across small providers, generally EU based.[13]

Some estimates[14] show that data centre construction costs may be up to 120% higher and operating costs may also double in some European locations compared to others.[15] The EU average data centre lifetime[16] cost (excluding land costs and capital costs associated with servers and other equipment)[17] is 276.9 million €.[18]

According to the Organisation for Economic Co-operation and Development (OECD)[19], data flows enhance the efficiencies of trade with specialised services firms offering a host of data storage, transfer and data mining services within and across borders, vastly reducing transaction costs. In this context, "No forced data localisation" is among the policy recommendations of the recent "Scale Up Europe: A Manifesto for Change and Empowerment in the Digital Age"[20] which states, in particular, that "*Enforced data localisation will mean higher costs for the cloud-driven services upon which so many startups rely"*, that *"it will add further uncertainty and immensely greater regulatory burden on fast-growing enterprises"* and that *"localised data is not necessarily safer data"*.

[10] Aaronson, Susan Ariel, "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", 2015.
[11] M. Mandel, Data, Trade and Growth, 2014.
[12] IDC Study, Uptake of Cloud in Europe, Follow-up of IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up, 2014.
[13] IDC Study, Uptake of Cloud in Europe. Follow-up of IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up, 2014.
[14] ECIPE, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, 2016, http://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/?chapter=all.
[15] Because of higher land, labour and operating costs, such as higher energy prices or increased energy consumption to maintain efficient operating temperatures when located in warmer European regions.
[16] The typical lifetime of a data centre is 10 years, with servers being replaced every 3 to 5 years.
[17] Time.lex, Spark Legal Network and Consultancy, Tech4i2, Cross-border data flow in the digital single market: study on data location restrictions, 2016.
[18] The most expensive location is Belgium (421.4 million €), and the cheapest location is Bulgaria (81 million €).
[19] OECD, Emerging Policy Issues: Localisation Barriers to Trade, 2015 http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2014)17/FINAL&docLanguage=En.
[20] http://scaleupeuropemanifesto.eu/.

The ECIPE study[21] attempted to quantify the economic losses that result from data localisation requirements and related data privacy and security laws in various jurisdictions that discriminate against foreign suppliers of data. For the EU the study estimates a welfare loss of USD 193 bn and an impact on overall domestic investments of -3.9% compared to China (-1.8%), India (-1.4%), or Korea (-0.5%), generating a direct loss of competitiveness.

Removing existing data localisation measures would lead to GDP gains of up to 8 bn € per year.[22] In particular, the net benefits increase for cloud users is estimated at 7.2 bn € over the period 2015-2020.[23] The positive cost effect of the possibility to use cloud services based in other Member States is estimated at around 9%, which represents the differential in pricing per machine per hour between the selected locations in Western and Central Europe or Northern and Western Europe.[24]

Cloud computing is increasingly used for the storage and processing of data, in particular across national borders. Projections for the use of cloud computing services in Europe are illustrative of the volume of cross-border data transfers and point to a general adoption of cloud solutions in all sectors of the economy.[25]

Forecasts of cloud service providers' revenues partially account for the data localisation restrictions as long as one can realistically estimate the percentage of business secured by cloud service providers outside their national borders. In 2013, cloud computing accounted for about 10% of global IT expenditure, however the cloud share is expected to reach 17% by the end 2017. The share of traditional IT solutions is expected to grow by 4% (CAGR from 2013 to 2017), whilst the share of public cloud services is expected to grow at 22% CAGR from 2013 to 2017.[26]

The removal of data localisation restrictions is expected to support the development and the uptake of cloud computing. According to one estimate, policy initiatives aiming at promoting existing relevant certifications and standards and at removing data localisation restrictions would increase benefits for users and providers of cloud computing, as well as for society as a whole to a total of over EUR 19 billion between 2015 and 2020.[27]

Businesses that choose to run business applications in the cloud can help reduce energy consumption and carbon emissions by a net 30 percent or more versus running those same applications on their own local infrastructure. The benefits become even more significant for a small business moving to the cloud, where the net energy and carbon savings can be more than 90 percent. The global energy efficient data centre market is expected to grow to almost €90 billion by the end of 2020.[28]

---

[21] ECIPE, The Costs of Data Localisation: Friendly Fire on Economic Recovery, 2014 http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

[22] ECIPE, Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, 2016.

[23] Deloitte, Measuring the Economic Impact of Cloud Computing in Europe, 2016, https://ec.europa.eu/digital-single-market/news-redirect/51685.

[24] London Economics, Facilitating cross border data flow in the Digital Single Market, 2016.

[25] Deloitte, Measuring the Economic Impact of Cloud Computing in Europe, 2016.

[26] PwC Strategy & analysis, 2015.

[27] Deloitte, Measuring the Economic Impact of Cloud Computing in Europe, 2016.

[28] Microsoft, Accenture and WSP Environment & Energy, "The Environmental Benefits of Moving to the Cloud", 2010.

4. EU legal regime applicable to data localisation requirements

The EU legislative acquis contains a number of instruments of relevance for assessing data localisation requirements in national law.

The General Data Protection Regulation (GDPR), that will replace Directive 95/46/EC as from 25 May 2018, provides for a harmonised and high level of protection of personal data and is the foundation for the free flow of personal data in the EU. Furthermore, like Directive 95/46/EC, the GDPR bans prohibitions or restrictions to the free movement of personal data for reasons connected with the protection of natural persons with regard to the processing of personal data. Restrictions justified by other reasons than the protection of personal data, e.g. under taxation or accounting laws, are thus not covered by the GDPR. Furthermore, non-personal data remain outside the scope of GDPR.

Restrictions to the storage or processing of non-personal data and restrictions to the storage and processing of personal data justified by other reasons than the protection of personal data therefore need to be assessed on the basis of other EU legal instruments, namely[29]:

- Secondary legislation giving effect to the Treaty provisions on the free movement of services (Article 56 TFEU) and the freedom of establishment (Article 49 TFEU) that includes Directive 2000/31/EC (the E-commerce Directive). The Directive bans restrictions to the freedom to provide information society services from another Member State and prohibits Member States to make the taking up and pursuit of the activity of an information society service provider subject to prior authorisation or any other requirement having equivalent effect.
- Similarly, Directive 2006/123/EC (the Services Directive) deals with authorisation schemes and other requirements regulating access to, or the exercise of, a service activity and contains provisions both to ensure the right of providers to provide services in a Member State other than that in which they are established and to prevent Member States from imposing on a recipient requirements which restrict the use of a service supplied by a provider established in another Member State.
- Finally, Directive 2015/1535 (the Transparency Directive) puts in place a mechanism aimed at preventing the adoption by Member States of rules on information society services, including data storage or processing services that may create obstacles to the free movement of services in the internal market. According to the Directive, the Commission and the Member States may submit a detailed opinion to the Member State notifying a draft measure to raise concerns on aspects that may hinder the free movement of services.

[29] This is the list of main relevant EU secondary legislation. Other instruments might have to be taken into account when assessing specific restrictions, such as Directive 2009/101/EC (company law) which requires storing and disclosing information on limited liability companies in Member States' business registers in order to ensure the transparency and legal certainty.

Part 3: Data access and transfer

A second key area to address is data access and transfer. Within this broad area and as announced in the Communication on the Digital Single Market[30], the Communication "Building a European Data Economy" and this accompanying Staff Working Document aim at examining the "emerging issues of ownership, ... and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data". In light of the adoption of the General Data Protection Regulation (GDPR)[31] which provides a comprehensive and complete legal framework on the processing of personal data, the scope of this examination is limited to non-personal or personal data that have been anonymised. At the same time, as pointed out by the Article 29 Working Party[32], the new right of data portability under article 20 GDPR is "an important tool that will support the free flow of personal data in the EU and foster competition between data controllers."

This section begins by describing the current EU policy acquis on access to data generated by the public sector. It then presents preliminary available evidence on current business practices on sharing of data. It also summarises the relevant current legislation with respect to data by looking at the EU legal acquis and at relevant legislation and policy discussions in Member States, and illustrates the relevance of studying these emerging issues in a number of selected contexts before discussing possible ways forward.

1. Current EU policy on access to data has focussed on data generated by the public sector

Making available data for re-use has been at the forefront of a number of Commission initiatives, such as the policy on public sector information, on geo-spatial information (INSPIRE) and on making available satellite data (COPERNICUS).

In particular the policy on re-use of public sector information (PSI), which led to Directive 2003/98/EC[33], has been motivated by the innovation potential of opening up such information for re-use.[34] When making data available for re-use, public sector bodies are bound to ensure compliance with data protection legislation.[35] Similarly, facilitating access to geo-spatial information is an important element of the INSPIRE Directive.[36] Through the COPERNICUS programme, the EU collects earth observation data and makes it available to public bodies, researchers, business and citizens through a free and open data policy.[37] The Commission is currently working together with the European Space Agency (ESA) and the European Organisation for the Exploitation of Meteorological Satellites (EUMESTSAT) on the implementation of a new e-infrastructure for a user-friendly access to Copernicus data and

[30] COM(2015)192 final of 6 May 2015.
[31] Regulation 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, OJ L 119 of 4.5.2016, p. 1.
[32] Guidelines on the right to data portability of 13 December 2016. We note that these guidelines may be subject to changes on the basis of comments that can be submitted until end of January 2017.
[33] Directive 2003/98/EC on the re-use of public sector information as revised by Directive 2013/37/EU.
[34] COM(2011) 882 final of 12.12.2011.
[35] Article 1(4) Directive 2003/98/EC as revised by Directive 2013/37/EU.
[36] Directive 2007/2/EC establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).
[37] On the basis of Regulation (EU) No 377/2014 of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010; see in particular article 23 of that Regulation; http://www.copernicus.eu.

other earth observation data with the objective to stimulate the development of geospatial data based added value services.

Next to work on the appropriate legal framework, the development of technical infrastructures that facilitate the discoverability of information and access to data is a principal area of work. In this respect, the INSPIRE Directive is of prime relevance as it sets in place a legal interoperability framework for spatial information covering both legal aspects of data sharing and technical access and interoperability issues for web-based services and spatial data interoperability.[38] To a certain extent this approach is now being applied to public sector information through Open Data portals which now exist in virtually all EU Member States and at the level of the EU institutions. The Commission is currently working on the implementation of a new e-infrastructure for a user-friendly access to Copernicus data and other earth observation data with the objective to stimulate the development of geospatial data based added value services.

A third element common to both Open Data and INSPIRE policies are the value added by harmonised metadata annotations of the available data.[39] Additionally, the new European Interoperability Framework, focussing on data exchange between public sector bodies, addresses access and reuse of open data by including specific recommendations covering aspects such as the use of machine readable, non-proprietary formats, the use of meta-data, quality and licensing.

What is common to the data made available under both policies is that it relates to data that has been generated by the public sector and thus funded from the public budget. In the case of INSPIRE, Member States also have to ensure that third parties whose spatial data sets and services comply with implementing rules laying down obligations with regard, in particular, to metadata, network services and interoperability can link their resources to the network of services.

2. Sharing data in commercial contexts

2.1 Introduction

For companies requiring access to data held by another company, voluntary data trading[40] should be considered as the solution best suited in a market economy based on the principle of freedom to contract. Companies (especially SMEs and start-ups) that do not wish to or cannot generate all the data they need for their products or services should be able to obtain data like any other (physical) resource. At the same time, such data trading allows companies to monetise certain data they hold (e.g. anonymised data), opening additional sources of revenue.

[38] INSPIRE Geoportal: http://inspire-geoportal.ec.europa.eu/.

[39] This is a particularly important feature of the INSPIRE policy and has been subject to specific implementing legislation (Commission Regulation (EC) No 1205/2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata); on open data, work has been on-going on a DCAT Application Profile for data portals in Europe, an action funded under the ISA and ISA^2 programmes, http://ec.europa.eu/isa/ready-to-use-solutions/dcat-ap_en.htm.

[40] As opposed to data trading on the basis of an obligation to licence, see below under 7.2.

2.2 The current state of data sharing

(a) *Examples of well-developed data markets*

For centuries, *information* has been traded. However, with the availability of information stored in a digital form, *data* trading has drastically increased. Examples of well-developed markets for non-personal data are the markets for financial or commodities market data[41]. Data markets using also data available as "open data" (often public sector information) have developed, in particular as a result of EU Directive 2003/98/EC on the re-use of public sector information.[42] Specific data markets exist for a diverse range of data.[43]

Also, a number of companies are opening up some of the data they hold through Application Programming Interfaces (APIs) for access by third party applications. Examples are not limited to the mobility sector[44], banking[45] or the information services sector[46]. This appears to be done with a view of having the data used for such a wide range of potential applications that it would be inconceivable for the data-holding entity to develop them in-house or through commercial partnerships. Instead, they rely on an open number of third party developers to integrate the data in the applications they develop.

The number of organizations and companies seeking to sell their data or purchase new data sets from others to provide new business models and additional revenue streams is expected to increase exponentially.[47] The growing number of data marketplaces (see below under 2.3) will give organizations, in particular smaller ones who have data sets to sell, additional routes to market as well as easier billing and subscription mechanisms.

There are a number of data marketplaces in existence. Yet many of these seem to be either marketplaces focused on the trading of predominantly personal data for marketing purposes or marketplaces that specialize in trading very particular kinds of data or data generated within a specific sector or situation. There is also a variety of companies specializing in data analytics, e.g. business or market intelligence, but few of these offer full access to raw, non-curated data for re-use. Based on very preliminary research, few examples have been identified of independent two-sided marketplaces offering companies full access to the modalities of the trade (e.g. negotiations, pricing) and operating across different sectors.

---

[41] The market for financial markets data is expected to reach $ 6.65bn (€ 5.94bn) by 2018, http://www.marketsandmarkets.com/PressReleases/financial-analytics.asp; we understand that, on the mentioned markets, data is traded often in a processed form or as 'information' (= 'data structured and put in context').

[42] As amended by Directive 2013/37/EU; noteworthy European companies are: C-Radar (www.c-radar.com), Qlik (www.qlik.com), and DueDil (www.duedil.com), US examples include: Enigma (http://enigma.io/).

[43] Examples include AAAData (www.aaa-data.fr; data about car matriculations sold to car insurance agents), Cerved (www.cerved.com; credit scoring data sold to banks); Climpact-Metnext (www.climpact-metnext.com; weather data sold to farmers).

[44] https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/; https://developer.jcdecaux.com/#/home.

[45] https://www.bbvaapimarket.com/web/api_market/bbva/bbva-connect; https://www.creditagricolestore.fr/castore-data-provider/docs/V1/rest.html.

[46] https://customers.reuters.com/developer/apis_tech.aspx and https://permid.org/; https://dev.elsevier.com/; https://dev.twitter.com/rest/public; see e.g. the API of tractor and construction engine developer John Deere: https://developer.deere.com/#!welcome.

[47] Consultancy IDC in a report for the European Commission, Europe's Data Marketplaces – Current Status and Future Perspectives, 2016 http://www.datalandscape.eu/data-driven-stories/europe%E2%80%99s-data-marketplaces-%E2%80%93-current-status-and-future-perspectives.

(b) *Examples of open sharing of data*

There are some interesting examples on the sharing of data as open data, i.e. data being shared with no or very limited restrictions.[48]

For many business actors this can be regarded either as "data philanthropy" or being part of "corporate social responsibility".[49] In the utilities sector, for example, such data sharing is based on the recognition that there is a case for wider access to such data.[50] Mobility providers[51], on the other hand, have a strategic interest in having their mobility offers embedded in as many applications as possible and thus are likely to make relevant data on schedules and similar available for free and only subject to certain conditions, notably under the condition not to use the data in order to develop competing offers. Other examples include sharing of privately held data specifically for common good purposes such as humanitarian intervention and disaster management.

Community-driven initiatives like OpenStreetMap[52] build on individual persons volunteering to record data and share with others for the establishment of mapping information.

Additionally, data portals are being developed in order to foster the discoverability of data published by non-public actors and to allow collaboration of such data.[53]

(c) *Yet voluntary data trading is not common in all sectors: Evidence from a survey of business models*

Business models based on data are still emerging and constantly evolving. This makes it difficult to present a stable picture of the state of data sharing in Europe across all sectors. However, research currently conducted by Deloitte on behalf of the European Commission[54] has produced a first classification of the main aspects of data sharing.

The chart below on the 'distribution of data-sharing models' is the result of applying a typology of business models in the data economy developed for the purpose of the study on 100 real cases identified through desk research.[55]

[48] Examples include ThomsonReuters allowing re-use of its permanent identifiers scheme (https://permid.org/, on the motivations see: http://theodi.org/open-enterprise-big-business-case-study-thomson-reuters); Syngenta (http://www4.syngenta.com/what-we-do/the-good-growth-plan/progress/progress-open-data); Utilities such as ENEL (http://data.enel.com/) or Berlin electricity grid data (http://www.stromnetz.berlin/de/open-data.htm).

[49] See for example the considerations of the founders of data.world: https://www.datainnovation.org/2016/11/5-qs-for-brett-hurt-and-matt-laessig-of-data-world/.

[50] See under 7.2 below.

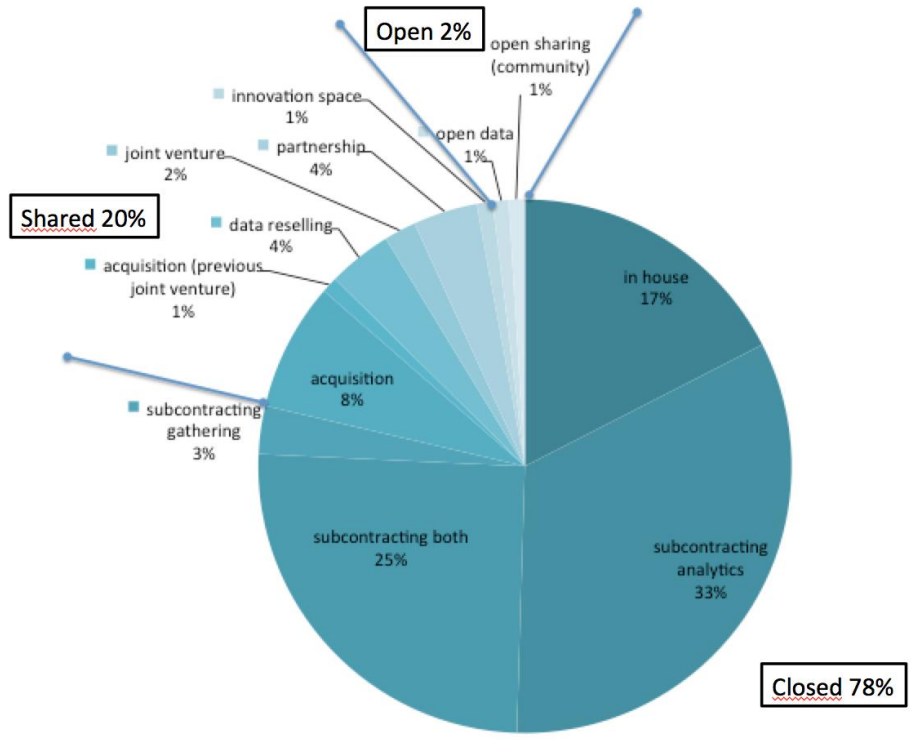
[51] See examples in footnote 44.

[52] http://wiki.osmfoundation.org/wiki/Main_Page.

[53] E.g. by public benefit corporation data.world (https://data.world/), or https://opencorporates.com/ , or the government-sponsored portal https://www.opendataportal.at/; see also: http://www.johnsnowlabs.com/dataops-blog/sharing-data-future-corporate-philanthropy/ .

[54] Estimation and preliminary conclusions in the Impact Assessment Support Study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability – SMART 2016/0030.

[55] From different sectors of the industry, namely aerospace, automotive, agriculture, chemical, energy, finance, health, machinery, retail, telecommunications and transport.



Distribution of data sharing models
[Source: Deloitte, Impact assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data and liability. First interim report (forthcoming)]

This overview suggests that in the vast majority of cases (78% of the companies surveyed) data is generated and analysed in-house by the company or by a sub-contractor. Vertical integration remains the principal strategy in the sectors surveyed. Data stays within an organisation and is not traded with third parties.[56]

Within the strategy of vertical integration, the data holder develops services on top of its data, e.g. for enhancing the efficiency of internal processes or for improving client service.[57] In sectors such as machinery, automotive and energy, in particular, data analytics is used to provide new services. However, the services are closely related to the traditional non-data product and service the company has been producing previously.

Data analytics is performed in-house by some companies, but to a much larger extent analytics services are sub-contracted. This is true for more than half of the companies surveyed. In these cases, the sub-contractor analyses the data only for the specific purpose and within the limits of the contract. Further re-use of the underlying data is typically not allowed.

Subcontracted data gathering and analytics is typical of sectors such as agriculture, energy, machinery and retail. The technology providers install sensors on the clients' premises, gather

[56] This is particularly the case in sectors with a high presence of large, technologically advanced companies, such as banks and telecom providers or automotive and machinery producers.
[57] Especially automotive and machinery producers are exemplary of sectors in which the main players produce and collect sizeable amounts of data and use their IT capacities mostly to improve their own products rather than to develop new services on top of the data.

data and provide analytics services to the clients.[58] The sensor producers may offer an end-to-end service, which includes both the physical infrastructure and the data analysis but are typically not interested in the acquisition of the analysed data and its re-use further on.

Making available data to third parties remains uncommon. Data 'sharing' according to the model applied by Deloitte can take a number of forms, including merger & acquisition and venture capital investment, joint ventures, data trading among independent economic operators, the usage of 'data innovation spaces' or adding data gathering and analysis to traditional services and products (see graph). This applied to 20% of the companies surveyed. Data trading among independent economic operators, however, does only account for 4% of the companies surveyed.

Only 2% of companies studied make available corporate data for re-use in a more or less open manner.[59]

(d) *Contractual agreements on data appear to limit onward re-use*

Most existing arrangements to allocate rights of access, use and re-use of data created by computer processes or collected by sensors processing information from equipment, machines or software are done through contracts.

A study conducted by the law firm Osborne Clark[60] surveyed contracts dealt with by their offices which held complex data clauses. It appears that the firm deals far more frequently with the issues of "data ownership" and access to data in their UK offices.[61] The sectors involved were predominately digital business, health, new technologies, IP, retail, data centres and outsourcing deals.

The most common issues occurring in complex data clauses were:

- the possibility for a party to re-use/communicate data to third parties,
- "ownership" of data generated/processed,
- allocation of any IP rights at stake/generated by technical devices and/or
- the extent to which parties who have access to data are allowed to commercialise it.

In most cases, one party was prevented from using the data for any purpose other than fulfilling the contract. Only in a very small number of cases this party negotiated for re-use of the data for other purposes.

It is also difficult at this stage to observe any clear patterns across sectors. The usage rights seem to be highly context dependent and focused on the type of the service provided.

[58] Examples include beacon producers and app developers who provide analytics for retailers about their clients' whereabouts and behaviour.

[59] One notable example is the open sharing of anonymised and aggregated transactions via an open API by BBVA, https://www.bbvaapimarket.com/.

[60] Legal study on ownership and access to data, p. 79; https://bookshop.europa.eu/en/legal-study-on-ownership-and-access-to-data-pbKK0416811/. The jurisdictions surveyed were: France, Spain, Germany, UK, Italy, Belgium, the Netherlands.

[61] The UK office of the contractor of the cited study reported 80-110 complex data clauses drafted or reviewed within the course of the past year, whereas the other offices reported single digit numbers or none (Italy:0, Spain: 8, the Netherlands: 1, Belgium:1 and France: 2).

2.3 Typology of data marketplaces

Specific data marketplaces have emerged as a venue for commercial data trading.

There is no uniform definition of what a data marketplace is. Stahl et al. define data marketplaces as electronic marketplaces where data is traded as a commodity, an electronic marketplace being "the concrete agency or infrastructure that allows participants to meet and perform the market transactions, translated into an electronic medium".[62] This definition will be used in the following discussion.

Several typologies are being presented in scholarly writing: Some[63] group marketplaces by the number of economic players on either side of the bargain, i.e. one-to-one, many-to-one, one-to-many and many-to-many.[64] Vomfell et al.[65] merge a number of existing models and put the emphasis on the independence in managing the marketplace and the power that either the buyer or seller side can exercise on the marketplace (see figure).

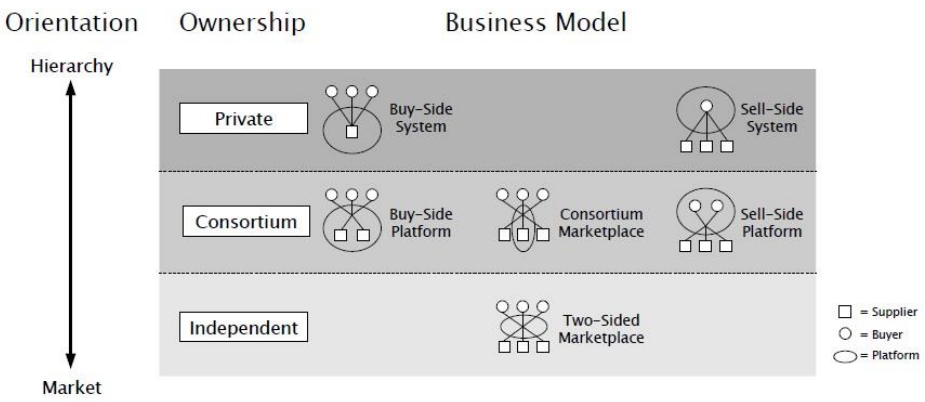


Figure taken from: Vomfell, Stahl (et. al.), A Classification Framework for Data Marketplaces, ERCIS Working Paper no. 23 (reproduction with authorisation of the authors)

DAWEX[66] is an interesting example of a platform for matching supply and demand for individual data. Different from a data broker or aggregator, its service is essentially limited to finding the right buyer for a company that wants to monetize data it holds. It is not limited to any specific sector. Clients today come from the automotive, energy, agriculture, insurance & finance, environment, health, retail & consumer goods, and media & entertainment sectors, with plans to broaden the scope.

The company operates a data transaction tool, and acts as a data intermediary that does not access data sets themselves. Nevertheless, both sellers and data buyers need to go through a compulsory registration which is meant to ensure trust and reliability. In particular, sellers stay in control regarding who can ultimately buy their data.

[62] F. Stahl, F. Schomm, G. Vossen, & L Vomfell, A Classification Framework for Data Marketplaces, Vietnam J Comput Sci, 2016, p. 137.
[63] P. Koutroumpis et al, The (unfulfilled) potential of data marketplaces (forthcoming).
[64] Examples for a many-to-many marketplace are Microsoft's Azure Marketplace and Amazon.
[65] F. Stahl, F. Schomm, G. Vossen, & L Vomfell, A Classification Framework for Data Marketplaces, Working Paper No 23, 2015, p. 9.
[66] https://www.dawex.com/en/.

It operates on the basis of a "per transaction"-remuneration model. Usually both sellers and buyers are charged a varying percentage of the total value of the transaction. The value of the transaction itself is the result of an agreement between the seller and the buyer and without DAWEX's involvement. It presents itself in this respect as a "notary" for validating data transactions, allowing companies to insert such transactions in the corporate balance sheet.

The French public investment bank *Caisse des dépôts et consignations* has in June 2016 become a minority shareholder of DAWEX, supporting this platform as a facilitator for the monetization of data open to all actors of the economy and thus contributing to a wider circulation of data in the emerging data economy.[67]

2.4 Industrial Data Platforms

Industrial data platforms can be defined as virtual environments facilitating the exchange and connection of data among different companies and organisations through a shared reference architecture, common governance rules and within a secure business ecosystem.[68] The common governance rules in particular could technically implement an open, generally recognized process and a standardised data ecosystem for the transfer of property and possession of data assets.[69] Industrial data platforms may take the form of open, multi-company-led environments that meet the requirements of a wide ecosystem of users from different industrial sectors. Industrial data spaces can, however, also take the form of single-company-led initiatives where an individual company or organisation establishes its own platform and opens it to other companies for commercial purposes. This usually happens within the boundaries of a specific industry sector.

Over the last years, a number of cross-sector solutions have come to the market or to the piloting stage, be it community-eld (e.g. the Industrial Data Space project[70] in Germany or the Swedish joint venture Combient[71]) or offered by individual companies (e.g.Mindsphere by SIEMENS[72] built in collaboration with SAP, or Predix by GE[73]).

In the context of access to and re-use of data, industrial data platforms can thus play an important role as a technical enabler for data sharing in industrial contexts, ensuring that the solutions respond to the specific needs of industrial players.

---

[67] Joint press release by DAWEX and the Caisse des dépôts et consignations, http://www.capdigital.com/wp-content/uploads/2016/07/Dawex-Communique%CC%81-de-Presse-02062016.pdf.

[68] IDC and Open Evidence, European Data Market Study, 2016, publication forthcoming, https://docs.google.com/a/open-evidence.com/viewer?a=v&pid=sites&srcid=b3Blbi1ldmlkZW5jZS5jb218ZG93bmxvYWR8Z3g6NjJiZTQ1NTYyZjdlOGNhNg

[69] R. Bauer/ B. Otto, Data Property and Data Possession in the Context of the 'Industrial Data Space', publication forthcoming, 2016. According to them, the current predominant use of contracts fails to address the need for a globally recognized framework of conditions regarding data possession, data property and its transfer.

[70] http://www.industrialdataspace.de/.

[71] https://combient.com/.

[72] SIEMENS Mindsphere, 17 Nov. 2015 https://www.siemens.com/customer-magazine/en/home/industry/digitalization-in-machine-building/mindsphere-siemens-cloud-for-industry.html

[73] https://www.ge.com/digital/predix.

2.5 Personal information management services

Personal information management services (PIMS) are a developing set of technical means, currently in its infancy, for individuals to manage control over their personal data.[74] While considerable conceptual differences exist, PIMS can be summarised as technical means which individuals can use in order to exercise their right to data portability under article 20 GDPR.[75] PIMS in this respect can serve as a means to receive back personal data from data controllers (within the limits of the right under article 20 GDPR). PIMS would then also give individuals the means to provide personal data through a web or mobile application for processing by others on the basis of one of the legal bases of the GDPR (e.g. consent, performance of a contract).
The Commission has surveyed in autumn 2015 the landscape of service offerings and their technological and commercial readiness.[76] The main findings are that some service providers had already embryonic versions of PIMS services available, but that most are still small in terms of the user base and limited in the features provided. Similar to any online platform they face the challenges of multi-sided markets and the need to generate network effects.

3. The EU law regime applicable to processing data

Data are intangible, non-rivalrous goods and as such cannot be captured by the traditional definitions of **property law**.[77] National property law has been applied, however, by courts, linking "ownership" with respect to non-personal data to the ownership of the physical means of storage of such data.[78] Machine-generated and industrial data do not benefit from protection by other intellectual property rights as they are deemed not to be the result of an intellectual effort. Results of data integration, analytics, etc. can be protected, on the other hand, as a result of a protection given to the intellectual effort made into the design of the data integration process or the analytics algorithm (software).

The General Data Protection Regulation and the *lex specialis* ePrivacy Directive[79] fully regulate the processing of personal data. The right of the protection of personal data is a

[74] See for a description of the concept and selected service providers: Ctrl+Shift, Personal Information Management Services: An analysis of an emerging market, 2014; European Commission, Personal Data Stores, 2016 https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school; European Data Protection Supervisor, Opinion 9/2016 on Personal Information Management Systems.
[75] See guidelines on the right to data portability by the Article 29 Working Party of 13 December 2016, http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf; we note that these guidelines may change based on comments that can be made until the end of January 2017.
[76] Report available at https://ec.europa.eu/digital-single-market/en/news/emerging-offer-personal-information-management-services-current-state-service-offers-and.
[77] H. Zech, Data as a Tradable Commodity, in: De Franceschi (ed.), European Contract Law and the Digital Single Market, 2016, pp. 59-60.
[78] See e.g. the decision of German Bundesgerichtshof (Federal Supreme Court) of 15.11.2006 (ownership of software on a CD-ROM); but see also the recent decision of the same court on the transfer of ownership on the physical storage as a result of data recordings (in the instant case: audio recordings on a tape) would be leading to a transfer of ownership under civil law to the party that could claim rights on the data – decision of 10 July 2015; the federal Supreme Court held that rights a party may have on data content will not ipso iure lead to co-ownership of the physical storage.
[79] Regulation 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 (General Data Protection Regulation); Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) – currently under review.

fundamental right in the EU.[80] The EU data protection legislation set out the rules for processing personal data including i.a. the collection, use of, access to and portability of personal data as well as the possibilities to transmit or to transfer personal data. The right to data portability[81] will allow individuals to obtain copies of personal data they have provided to a service provider (data controller) and to move that data to another service provider (data controller), (for example, personal data on a social media). It may assist avoiding potential lock-in effects.

The **Database Directive (Directive 96/9/EC)** protects databases[82], which either constitutes the author's own intellectual creation or for which a substantial investment has been made by the maker of a database. Subject to exceptions, use by others (e.g. extraction of the content, reproduction of re-utilisation of the database) can be prevented by the database author or maker, but only to the extent that either their database in its entirety or substantial parts thereof are concerned (article 7(1)), or when others seek to use insubstantial parts of the database in a "repeated and systematic" manner (article 7(5)).[83] The protection offered thus does not apply to machine-generated data as such.

As concerns the content of databases, it has to be borne in mind that the Database Directive did not intend to create a new right in the data[84]. The CJEU thus held that neither the copyright protection provided for by the Directive nor the sui generis right aim at protecting the content of databases.[85] Furthermore, the ECJ has specified that the investment in the creation of data should not be taken into account when deciding whether a database can receive protection under the *sui generis* right.

Legislation has been recently adopted on the **protection of undisclosed know-how and business information (trade secrets)** against their unlawful acquisition, use and disclosure.[86] This Directive does not go so far as to introduce a new IP right for "trade secrets". Information (this can include data) qualifies as a "trade secret" if it meets the following three requirements: (a) it is secret (in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question); (b) it has commercial value because it is secret; and (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. It is doubtful that individual data generated by interconnected machines and devices could be regarded as "trade secret" in the sense of this Directive, mostly because of its lack of commercial value as individual data; however, combination of data (datasets) can be trade secrets under this Directive if all the criteria are met. Indeed, if such data is shared without being subject to sufficient protection measures to keep it secret, the Directive does not apply.

[80] See e.g. article 8 of the Charter of Fundamental Rights of the European Union.
[81] Article 20 Regulation 2016/679 (GDPR); see also part 4 on data portability.
[82] Defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means", article 1(2).
[83] Exceptions apply for the use for private purposes, for teaching and research purposes and for public security or administrative or judicial procedure (article 6, 9). The CJEU applies a quantitative and qualitative test as to whether certain data constitute a "substantial" part of a database, Case C-203/02 - The British Horseracing Board and Others v William Hill Organization Ltd.
[84] Recital 46 of Directive 96/9/EC.
[85] Case C-604/10 - Football Dataco and Others, para 30; Case C-203/02 - The British Horseracing Board and Others v William Hill Organization Ltd; Case C-444/02 - Fixtures Marketing.
[86] Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

Legislation is under discussion on certain aspects concerning **contracts for the supply of digital content**[87] which would provide rights to consumers to remedies in case of defective digital content received in exchange of either money or data (or both). The application of the Consumer Rights Directive[88] to contracts concerning digital content and online services under which a consumer provides data as counter-performance is currently being discussed in the framework of its evaluation.

The Unfair Commercial Practices Directive[89] **protects consumers** against misleading actions or omissions by traders. In particular, a trader's omission to inform a consumer that the data he provides in order to access the service will be used for commercial purposes could be considered as misleading omission of material information.[90] The Unfair Contract Terms Directive[91] provides for minimum protection rules against unfair standard terms in consumer contracts. A standard contract term is considered unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer. Some Member States apply this legislation (or principles inspired from it) also to B2B relations. Both Directives are currently part of a comprehensive regulatory fitness assessment.[92]

The proposed Directive establishing the European Electronic Communication Code[93] also covers services provided in exchange of remuneration, which may be money or data.

Sector-specific legislation regulates the access to privately-held non-personal or anonymised data in certain contexts, e.g. the access to in-vehicle data for the purpose of opening up the market for after-sales services (maintenance and repair)[94]. Such data does not have to be provided for free, but is subject to a regulated regime. Another example is the ITS Directive[95] and its delegated regulations. Similarly, the Payment Services Directive 2[96] also opens up "payment information" under certain conditions and thus acting as an enabler for companies labelled "fintech"[97].

General competition law is applicable in the context of data-driven business models. It may be invoked to claim a wider access to data held by one economic operator. The Magill[98], IMS Health[99], Microsoft[100] and Huawei[101] cases provide some indications on potential obligations

[87] Proposal for a Directive, COM(2015)634 final.
[88] Directive 2011/83/EU of 25 October 2011 on consumer rights, OJ L 304 of 22.11.2011, p. 64.
[89] Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ L 149 of 11.6.2005, p. 22.
[90] See Commission Staff Working Document "Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices accompanying the Communication from the Commission "A comprehensive approach to stimulating cross -border e-Commerce for Europe's citizens and businesses", Chapter 1.4.10 on "Interplay with the Data Protection Directive and the e-Privacy Directive", 25.5.2016, SWD(2016) 163 final
[91] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[92] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm.
[93] COM(2016) 590 final/2 of 12.10.2016.
[94] Regulation 715/2007 as amended.
[95] Directive 2010/40/EU of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJ L 207 of 6.8.2010, p. 1.
[96] Directive 2015/2366/EU revising Directive 2002/65/EC.
[97] Companies using technology to enable the provision of financial services or to drive innovation in the provision of financial services.
[98] RTE and ITV v Commission ('Magill'), Case C-241/91 P and C-242/91 P, [1995] ECR I-743.
[99] Case C-218/01 [2004] ECR I-5039.
[100] Microsoft v. Commission, Case T-201/04, [2007] ECR II-3601.
[101] Case C-170/13.

to contract flowing from competition law. The CJEU has developed four conditions that need to be fulfilled for an action based on competition law principles to lead to an obligation to licence the use of commercially-held information[102]: that the data is indispensable for the downstream product, that there would not be any effective competition between the upstream and downstream product, that refusal prevents the emergence of the second product, and there is no objective reason for the refusal.

Re-use of data held by the public sector is subject to rules by Directive 2003/98/EC on the re-use of public sector information as recently revised by Directive 2013/37/EU ("PSI Directive"). Access to public sector information is subject to Member State competence.[103] The Directive applies only to documents held by public sector bodies which are accessible under national law and which are not subject to a third party copyright.

On the basis of this analysis of existing EU law, the main findings are as follows for processing non-personal or anonymised data:

- There is no comprehensive legislative framework on what rights can be exercised with respect to access to such data, in particular with respect to data created by computer processes or collected by sensors processing information from equipment, machines or software or in respect to the conditions under which such rights can be exercised;
- Beyond the Trade Secrets Protection Directive, there is no legal protection with respect to investments made into the generation and/or collection of data;
- There are rules on access to privately-held data in a very limited number of sectors.

4. The discussions in Member States

For the vast majority of the EU Member States, the issues of ownership and access to data are indeed emerging ones, but discussions seem to still be in early stages. Most Member States have not formulated a policy on issues of "data ownership" and access to commercially-held data yet. Therefore, concrete initiatives and political discussions have only commenced in a few Member States:

France

Recent Open Data legislation[104] puts in place provisions that oblige commercial companies to open up – under certain conditions – data they hold for re-use, namely data generated in the context of procurement (article 17), commercial data for the establishment of official statistics (article 19), certain electricity and gas production and consumption data held by transmission and distribution systems operators for re-use by any other party (article 23), and certain data relating to changes in real estate ownership for re-use by certain third parties (article 24). Such data are defined as "public interest data"[105]. According to the proposal of the government, the objective of the mentioned articles is to "enhance the circulation of data and

[102] B. Martens, An Economic Policy Perspective on Online Platforms, JRC Technical Report 2016/05, at 41; J. Drexl, Designing Competitive Markets for Industrial Data in Europe – Between Propertisation and Access, 2016, at 39.
[103] Notable exception: Directive2003/4/EC of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, OJ L 41 of 14.2.2003, p. 26.
[104] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JO République Française n°0235 of 7 October 2016.
[105] "Données d'intérêt general".

knowledge" in order to give France a competitive edge in the digital economy.[106] Details are left for implementing legislation.

Germany

In Germany, there is a lively debate in academia and – to a certain extent – in government on the emerging issues of "data ownership", access to data and liability. There is a particular focus on the implications for Industrie 4.0 developments.[107] A number of German academics have also contributed to the debate on whether further regulation is needed to properly allocate rights to data.[108] Policy-makers both at federal and Länder level have started examining the need for additional regulation without concrete regulatory initiatives having been launched.[109]

Estonia

The Estonian government has launched the idea to create a fifth freedom, namely the free movement of knowledge and data, next to and in analogy to the four Internal Market freedoms set by the EU Treaties.[110]

Finland

The recently submitted legislative proposal for a new Transport Code stipulates that essential information on passenger transport services (incl. services operated by private companies) should be released as open data. The proposal also lays down provisions for the interoperability of ticket and payment systems, as well as the openness of interfaces.

Under the term "MyData", the government is developing a conceptual model of a future data architecture that is designed around the individual insofar as personal data are concerned.[111] Next to conceptual work undertaken as a research project, the government sponsors a

[106] http://www.assemblee-nationale.fr/14/projets/pl3318.asp.

[107] See position paper of Working Party "Legal aspects" of the government-sponsored and industry-driven discussion forum Plattform Industrie 4.0 (forthcoming 16 November 2016).

[108] H. Zech, "Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im Digitalen Binnenmarkt, GRUR 2015, p. 1151; H. Zech, Information as a tradable commodity, in: De Franceschi (Ed.), European Contract Law and the Digital Single Market, 2016, pp. 51-79; M. Becker, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, in: Büscher/Glöckner/Nordemann/Osterrieth/Rengier (Eds.), Marktkommunikation zwischen Geistigem Eigentum und Verbraucherschutz. Festschrift für Karl-Heinz Fezer zum 70. Geburtstag, p. 815; M. Dorner, Big Data und "Dateneigentum", CR 2014, p. 617; G. Spindler, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, p. 805; N. Härting, "Dateneigentum" – Schutz durch Immaterialgüterrecht?, CR 2016, p. 646; K.-H. Fezer, Dateneigentum, MMR 2016, p. 3; A. Wiebe, Protection of industrial data – a new property right for the digital economy? GRUR Int. 2016, p. 877; W. Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis GRUR Int 2016, p. 989; F. Faust, Digitale Wirtschaft –a analoges Recht: Braucht das BGB ein Update? Gutachten A zum DJT 2016, published in: Neue Juristische Wochenschrift Beilage 2/2016, p. 29; J. Drexl, R. Hilty (et al.), Position Statement of the Max Planck Institute for Innovation and Competition on the current debate on exclusive rights and access rights to data at the European level, 2016; D. Zimmer, Fragwürdiges Eigentum an Daten, Frankfurter Allgemeine Zeitung of 18 November 2016, p. 16; G. Surblyte, Data as a Digital Resource, Max Planck Institute for Innovation and Competition Research Paper No. 16-22.

[109] Initiatives at Länder level are being coordinated by Land Nordrhein-Westfalen: https://www.land.nrw/de/blogbeitrag/digitaler-neustart-braucht-unser-bgb-ein-update.

[110] See speech by Estonian President Ilves at European Parliament on 2 February 2016 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20160202+ITEM-005+DOC+XML+V0//EN .

[111] White Paper published in 2015: https://www.lvm.fi/-/mydata-a-nordic-model-for-human-centered-personal-data-management-and-processing-860616.

stakeholder platform with the aim of engaging with business, also in order to set up pilot projects.[112] Estonia and the Slovak Republic appear to support the conceptual vision.

5. The discussion in the United States

For many years, the term "data ownership" in the US discussion essentially referred to a debate about the protection of personal data.[113] In the absence of a fundamental or constitutional right to privacy or data protection or universal legislation at Federal and State level on the protection of (any) personal data[114], commentators and privacy advocates employed the term "data ownership" to argue for a stronger role of the individual with respect to the processing of his/ her data. As the protection of personal data enjoys the status of a fundamental right in the EU and processing of personal data is protected by the highest standards of data protection legislation in the world, in the EU personal data cannot be subject to any type of "ownership". Care should be thus applied when making reference to contributions from the US on "data ownership" when this concept is discussed with respect to personal data and only limited conclusions may be drawn given this fundamental difference in the legal approach to personal data.

With the emergence of IoT-enabled devices the scope of the discussion changed. As sensor-equipped machines, tools and devices connected to the IoT generate at almost zero marginal cost large amounts of data which in turn are an important source for Big Data analytics enabling data-driven innovation, the question of "who owns the data" has become more acute. Examples of city governments that feel expropriated with respect to data collected by buses or trains operated on behalf of the city government are being put forward as they are required to pay extra for having access to such data.[115] Due to the importance of the farming sector in the US, the discussion on "data ownership" is also particularly acute in this sector and farming associations work on helping farmers to assert their rights vis-à-vis the manufacturers.[116]

A recent Commission study[117] has shown, however, that:

- the sui generis protection offered to databases in the EU does not exist in the US;
- protection of trade secrets is available in the US at federal level by both criminal[118] and civil[119] law. At state level a uniform trade secrets act has been implemented by the state legislative chambers in almost all US state jurisdictions.[120]

There appears to be no indication of plans at Federal or State level to regulate rights on data or access to commercially-held data.

Questions of data ownership are thus left to individual contracts.

Data portability for certain data has been implemented also from a technical perspective. The "**Blue Button**" initiative[121] allows download and sharing of electronic health record

[112] https://mydatafi.wordpress.com/#about.
[113] See "Legal study on ownership and access to data", p. 79; https://bookshop.europa.eu/en/legal-study-on-ownership-and-access-to-data-pbKK0416811/ .
[114] Notable exception: health data for which certain protection exists under the HIPAA – the Health Insurance Portability and Accountability Act, enacted in 1996, and under additional legislation enacted subsequently
[115] http://fortune.com/2016/04/06/who-owns-the-data/.
[116] http://agnetwest.com/2016/03/04/data-ownership/.
[117] See "Legal study on ownership and access to data" (precit.).
[118] Economic Espionage Act of 1996.
[119] Defend Trade Secrets Act of 2016.
[120] With the notable exception of New York and Massachusetts.

information on the basis of technical standards developed by the Federal government. It originated in the US federal Veterans Affairs Administration but has since spread to other governmental actors and private health care organisations, on a voluntary basis.[122]

6. Rights on data and access to data in specific sectors

6.1 Data from connected vehicles

Access to and re-use of non-personal or anonymised data have been subject to intensive discussions with respect to data generated by the "smart" and connected car.

Building on existing legislation providing for access to in-vehicle information for the purposes of ensuring a level playing field on the after-sales repair and maintenance market[123], and preparing for a legislative initiative on "an interoperable, standardised, secure and open-access platform"[124], the issue of access to in-vehicle data has been discussed in depth since 2014, in the framework of a C-ITS stakeholder platform.[125] Five guiding principles for access to in-vehicle data and resources have been agreed upon, including fair and undistorted competition and the importance of "standardised access" to in-vehicle data as an enabler of the "common use" of such data in the context of the "data economy".[126] Work is on-going in terms of evaluating the technical and legal feasibility of improving access to in-vehicle data.[127]

6.2 Data-driven energy markets

(a) *Importance of access to relevant non-personal or anonymised data in order to balance electricity supply and demand*

The electricity sector involves a number of different actors, who all play different roles: Electricity is produced by producers, transported by transmission system operators and brought to the consumer by distribution system operators. Transmission system operators have to ensure that they operate the grid in a secure and reliable way and that they have access to sufficient amount of electricity in order to balance supply and demand. Access to relevant non-personal or anonymised data is of key importance for system operators, but also for the functioning of the market at wholesale and retail level. In this respect, real-time information from the smart grids can support the efficient operation of the grid and facilitate electricity services.[128] Access to such data would enable innovative solutions which can lower electricity costs and enhance security of supply.

---

[121] https://www.healthit.gov/patients-families/blue-button/about-blue-button.
[122] Through the Blue Button pledge program.
[123] Regulation 715/2007 as amended.
[124] Article 12(2) Regulation (EU) 2015/758 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, OJ L 123 of 19/05/2015, p. 77; the deadline for adopting a legislative proposal is 9 June 2017.
[125] http://ec.europa.eu/transport/themes/its/c-its_en.
[126] See C-ITS platform final report, January 2016, http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf, p. 11-12.
[127] Follow-up supporting study on 'Interfaces for access to services and vehicle resources' (open in-vehicle platform), 2015/S 248-450626 (ongoing).
[128] A smart grid is an electricity supply network that uses digital communications technology to detect and react to local changes in usage.

(b) *Re-use of smart meter information*

With the massive roll-out of smart meters measuring electricity consumption on a much more detailed level and close to real-time, the amount of data produced is enormous. There are many possible uses for these data by existing energy players and new market entrants. Improving access to smart metering information is one of the objectives of the Internal Electricity Market Directive.[129]

The Directive requests Member States to ensure consumer's free access to their data and interoperability of smart metering systems, including through open standards. As a result of data protection legislation, consumers have a right to access and port their smart metering data.

Under the legislative package "Clean Energy for all Europeans" adopted on 30 November 2016, the Commission revised the Directive and proposed a new energy market design.[130] On the issues linked to this Staff Working Document,, it proposes a legislative framework for transparent and non-discriminatory data access by any third parties with whom the consumers may choose to share their metering data, under a single format and procedure to be set up at European level.

Information resulting from smart meters is important also for the purpose of compiling official statistics. Eurostat collects information on energy production and consumption on the basis of the Energy Statistics Regulation[131]. The latest revision of the Regulation introduced the mandatory reporting of more detailed statistical information on final energy consumption in households by type of end use (space heating and cooling, water heating, cooking, electricity and appliances and other end uses).

For the time being and from the information available, many Member States use surveys, modelling and other complementary methods to provide the best possible estimates in order to fulfil the obligations resulting from the Regulation.

If more detailed data from smart meters were to become available and usable for statistical purposes, it would probably not only limit the burden and costs involved for reporting countries but might also potentially improve the quality (in particular accuracy and timeliness) of the information collected. Therefore, the European Statistical System is exploring the use of anonymised smart meter data for compiling statistics on electricity consumption in households and businesses in a pilot study.[132]

6.3 Smart Living Environments and the health and care sector

Collection, storage and analysis of relevant data is increasingly important for health and care management. Modern care institutions, smart homes and living environments – enabled by sensors and connected devices – present thus an important example in which an enormous amount of such exogenous health and lifestyle data are being created, both personal and non-personal data (e.g. about detection of falls or other health-related emergencies, adherence to medication, social interaction).

Not all such data are personal data if identifiers linking the data to a natural person have being taken away and re-identification is not possible.

[129] Directive 2009/72/EC concerning common rules for the internal market in electricity.
[130] Proposal for a revised Directive on common rules for the internal market in electricity COM(2016) 864 final.
[131] Regulation (EC) No 1099/2008 of 22 October 2008 on energy statistics, OJ L 304 of 14.11.2008, p. 1.
[132] see ESSnet Big Data, https://webgate.ec.europa.eu/fpfis/mwikis/essnetbigdata/index.php/WP3_Smart_meters

Appliances and devices used in such environments are developed by a variety of manufacturers. Integrated solutions for smart homes or living environments are only emerging and currently exist only as prototypes not ready for mass market circulation.

To enhance the functionalities of the support environment and the quality of services, the exchange of data among the devices inside the smart home, living environment or care institution, also with third-party service providers and notably with emergency centres, doctors, care services, informal carers and families, is important. This objective might be achieved through wider access for individuals to their data, including the capacity to give access to non-personal or anonymised data.

As concerns data related to the health of an individual that is not anonymised, attention has to be paid to the specific protection given to such data under the GDPR. Health-related data constitute a special category of personal data. It is generally prohibited to process such data, other than under one of the specified conditions as set out in the data protection rules and in line with all the data protection principles; i.a. purpose limitation, data minimisation, storage limitation, etc.

6.4 Mechanical Engineering Industry

Mechanical engineering is one of the largest industrial sectors in terms of number of enterprises, employment, production and added value. It accounts for 9.5% of the production in EU manufacturing industries. With an estimated 36% share of the world market, the EU is the world's largest producer and exporter of machinery.

Thanks to the use of sensors, the sector generates and analyse large amounts of data, mainly on production processes. Data are collected for a number of reasons, including the realisation of "zero defect manufacturing", increase productivity, efficient use of resources, reduction of energy use, reduction of total machine downtime and maintenance, and reduction of time-to-market.

These machines usually generate data through the use by a third party. For instance, the manufacturer of a robot designed to assemble washing machines, typically sells it to a house appliances manufacturers. In practice, data is generated thanks to the use of the machine by the latter. But this would not be possible without the sensors and the data-recording protocol engineered by the former. Both parties can be interested in accessing and analyse the data to improve their products and production process, to plan maintenance etc. But there can be situations in which one party may prefer to keep data private. In our example, the washing machine manufacturer may prefer its data not be analysed by the robot manufacturer if the latter also supplies also other firms, in order to avoid potential competitors to benefit from its experience.

Moreover, the increasing connectivity of machines can provide valuable business insights along the entire value chain, allowing for collaborative decision-making and potentially enabling almost real-time feedback of data on consumers' preferences into production processes.

However, the generation and exchange of such vast quantities of commercially valuable information, which is often stored and analysed automatically in the cloud, can generate doubts: who should be allowed to access and/or analyse the data (the creators, downstream manufacturers, upstream engineering firms, cloud vendors, etc.)? Under which conditions?

6.5 Agriculture

The quantity of data generated in the agricultural sector is growing fast. Exploiting the potential of this data could help tackling the multiple challenges the sector is facing. However, developments are hampered due to the perceived risks associated to engaging in data sharing.

Certain stakeholders worry that the increasing use of ICT will change the division of the value added in the chain and that it will influence the distribution of market power within the sector."[133] The agricultural sector is characterized by a large number of farms and food companies that are SMEs combined with a limited number of large companies in the up- and downstream value chain. Market power is concentrated in the up and downstream sector. Combined with insufficient digital skills in the farming community and the concentration of data in the larger companies, a large proportion of European farmers do not enjoy a very strong position in the relevant data value chains. As a result, investments in digital technologies remain limited. Some of the main issues impeding fairness appear to be the lack of transparency on data flows and data utilisation, inadequate distribution of access rights, the absence of portability of such data and the perceived risk for unauthorised use of data.

In the agricultural sector, stakeholders therefore acknowledge the need of data sharing while reducing the associated transaction costs. Farmer's associations call for clear and unambiguous EU-wide standards and rules, while striking "*the right balance between providing a future-proof regulatory environment that adapts to the changing nature of technological advancements and creating a level playing field, whilst also avoiding excessive burdens and protecting farmers' ownership and control of farm data as much as possible*."[134]

6.6 Use of commercially-held data for the compilation of official statistics

New data sources are being explored and increasingly used by the public sector in a wide-range of applications, not least for better policy-making.[135] Commitments from decision-makers to data-driven government[136] recognise up-front the role of data in unlocking solutions to complex policy challenges and in facilitating game-changing public policy and public sector innovation. This concerns all policy areas, from economic forecasting, to disaster management, environmental policy, education, job market, migration, finance or trade, and follows all stages of policy development.

In particular, official statistics is a common good that supports policy makers, businesses, and citizens in making well-informed decisions. The production of official statistics in the EU[137] is regulated and supported by the European Statistics Code of Practice[138] that aims at ensuring

[133] https://ec.europa.eu/eip/agriculture/sites/agri-eip/files/eip-agri_seminar_data_revolution_final_report_2016_en.pdf.
[134] Position paper of COPA-COGECA, Main principles underpinning the collection, use and exchange of agricultural data.
[135] A study commissioned by the European Commission explores over 50 cases of innovative use of data for evidence-based policy-making in the Member States and identified ten areas for further exploration in EU-level policies, with emerging issues related, amongst other, to access to privately held data, as well as gaps in data collection, quality, granularity and interoperability of data sets, need for data-capability within government and policy design processes that integrate data-driven insights; see http://www.data4policy.eu/.
[136] E.g. OECD E-Leaders Statement, 2015 https://www.oecd.org/governance/eleaders/statement-2015.htm.
[137] Regulation (EC) No 223/2009 of 11 March 2009 on European statistics.
[138] http://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/KS-32-11-955.

relevance, objectivity, and quality of EU statistics. In an increasingly digitised society, statistical offices should incorporate as much as possible new data sources in their conceptual design.[139] Currently statisticians are examining to what extent such data could be used in order to develop methods to produce statistical information of high quality. These methods could partially replace traditional surveys thus reduce costs and the burden on citizens who are called to respond to such survey while ensuring privacy of individual data. Also, specific quality aspects could be improved as data with higher spatial and temporal granularity would become available.

The main issues to be addressed are access to data, the adequacy and relevance of data sources, the preservation of statistical confidentiality to protect personal and enterprise information, the distribution of burden on data holders, and balance between public and business interests. The following examples are but a starting point.

Job vacancy statistics are used by the European Commission to monitor and analyse the evolution of the labour market in Europe. They reflect the unmet demand for labour as well as mismatches between the skills and availability of job seekers and demand by employers. They are also key indicators for the assessment of the business cycle and the structural analysis of the economy. Currently this information is collected asking businesses for open jobs using sample surveys. However, many job advertisements are nowadays posted online in specialised web portals or on enterprises' websites. This represents a potential source of data that could be collected in an automated fashion (using web scraping technology) at a very low cost. In addition, the text of the advertisements can be analysed to receive information on required skills and competences. This offers the opportunity of quickly following changes in demand for skills and competences.

National statistical institutes and European Commission services are studying the usability of such data as an alternative source for producing statistical information on job vacancies. Current projects are aiming at understanding this new source. What are – from a statistical point of view – the most relevant online job portals? Which part of the job market do they cover? What types of jobs are not offered online?

First results show that the data collected in this way can be used for showing trends in the labour market. Additional efforts have to be made to complement and replace existing data collections in order to produce statistics on volumes of job vacancies.

Anonymised data from mobile phone operators are another source of data that potentially can be used in the context of preparing official statistics.

Within the European Union, the penetration rate of mobile cellular subscriptions reached a number of 120%[140] in 2008, i.e. the number of subscriptions is higher than the number of inhabitants. For the majority of persons the mobile phone has become a constant companion that they carry with them wherever they go. Communication activities are leaving digital traces that can be analysed for statistical purposes.

Statistical offices in the EU are exploring the potential of anonymised data from mobile network operators for generating information on location and volumes of population at

[139] see the Scheveningen Memorandum on "Big Data and Official Statistics", http://ec.europa.eu/eurostat/documents/42577/43315/Scheveningen-memorandum-27-09-13.
[140] see: http://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2015&locations=EU&start=1960&view=chart.

specific times. Currently, official statistics on resident population or on number of commuters, for example are essentially derived from cost-intensive surveys or using data from administrative registers. Such statistical information cannot capture population movements with a high level of granularity, e.g. population counts at any specific time or date, e.g. on the number of people in a business area, at a specific event, or which routes they take for reaching these destinations. Through the analysis of mobile phone data, such information would be much easier to obtain. It could also become possible to analyse what segments of the population are on a touristic trip inside or outside their country.

7. **Possible ways forward**

The Communication "Building a European Data Economy" which this document accompanies announces a dialogue with stakeholders for a possible future EU framework for data access that should identify the most effective ways to achieve the following objectives :

- Improve access to anonymous machine-generated data;
- Facilitate and incentivise the sharing of such data;
- Protect investments and assets;
- Avoid disclosure of confidential data;
- Minimise lock-in effects.

In order to make the debate with the stakeholders more concrete, the Communication provides a non-exhaustive list of examples to go forward to be further discussed and refined during the upcoming structure stakeholder dialogues. Several ways forward are not mutually exclusive; elements of different examples could also be combined.

In this section, some of the examples are presented in a more detailed manner as they have been discussed in academic debates.

7.1 Non-legislative approaches

Three avenues for non-legislative approaches can be identified:

- Guidance on incentivising business to share data

Both consumers and businesses ought to be well informed on how the existing legal acquis applies to data so as to make the best of the potential of data-driven innovation.
The Commission could issue guidance on how non-personal data control rights should be addressed in contracts. This guidance would be based on existing legislation (in particular the Trade Secrets Protection Directive, copyright legislation and Database Directive as well as on the transparency and fairness requirements laid down in EU marketing and consumer contract law), with a view of lowering transaction costs.

- Fostering the development of technical solutions for reliable identification, exchange of, and differentiated access to data

Independent of the creation of rights in law with respect to non-personal data, mechanisms to persistently identify the originator and the legal entity that currently wishes to attach usage restrictions on such data may increase trust and thereby foster the exchange of data in business-to-business (B2B) contexts. Entities being at the origin of data could use standardised technical means of "watermarking" certain properties into data as a technical

means to secure their economic position or expression of usage preferences.[141] This could bring additional trust and security at the data level, and thus encode access rules in the (meta-) data itself. Additional avenues can be explored for sector-specific standards.

Additionally, metadata are a critical element for the re-use of such data. They describe relevant information on the data (e.g. time and method of collection).

Application Programming Interfaces (APIs) can also foster the creation of an ecosystem of application and algorithm developers interested in the data held by companies. APIs can help firms and public authorities to identify, and profit from, different types of re-uses of the data they hold.

On this basis, broader use of open, standardised and well-documented APIs could be considered, through technical guidance, including identification and spreading of best practice for companies and public sector bodies.[142] This could include making data available in machine-readable formats and the provision of associated metadata. The work on an UK Open Banking Standard[143] appears relevant as well as the work on technical interoperability standards in the context of the US Blue Button initiative mentioned above.

- Model contract terms

Transaction costs with respect to sharing non-personal or anonymised data could be lowered by making available model provisions for data usage licences that cover the most common business needs.

The Commission, together with stakeholders could work on a set of recommended contract terms. The voluntary integration of such contract terms could create more balanced terms for small businesses and reduce transaction costs for instance by making available model provisions for data usage licences that cover the most common business needs, while still safeguarding complete contractual freedom. Accordingly, weaker parties could have more and fair opportunities to exploit data.

Drawn up based on current contractual practice and in partnership with industry associations, they would reflect best business practices. The development process could be accompanied by independent legal experts.[144]

7.2 Legislative approaches

(a) Default contractual rules

Default contract rules for data licences could be laid down in legislation which could constitute a balanced solution for business-to-business contractual terms in case parties have not foreseen contractual clauses on the specific points. These rules could be deviated from by

[141] There is a whole body of literature on "data provenance" and technical implementation such as "digital watermarking", see e.g. R. Halder (et al.), Watermarking Techniques for Relational Databases: Survey, Classification and Comparison, Journal of Universal Computer Science, 2010, p. 3164-3190; see also the work of the Consortium of European Social Science Data Archives, https://www.big-data-europe.eu/cessda-persistent-identification-task-force-established/.
[142] Shadboldt/ Verdier, Update report of the UK-French Data Task Force, 2016.
[143] https://theodi.org/open-banking-standard.
[144] As proposed by Heckmann, Big Data im Freistaat Bayern. Chancen und Herausforderungen, p. 132.

contractual parties in their contracts and thereby safeguard a large degree of contractual freedom.

In addition, they could constitute benchmarks for a standard contract terms control, possibly concerning only sector-specific areas.[145] The standard of unfairness for such a standard contract terms control would need for B2B contracts to be lower than for B2C contracts and could for instance only apply if standard contract terms deviate grossly from good commercial practices.[146]

It is interesting to note in this respect that some Member States have extended the application of the relevant B2C instrument in this area, i.e. Directive 93/13/EEC on unfair terms in consumer contracts (Unfair Contract Terms Directive) also to B2B relations. In the context of the current Fitness Check of EU consumer and marketing law directives, the Commission is also evaluating the Unfair Contract Terms Directive.

(b) Access for public interest purposes

Public sector bodies like private companies are adopting data-driven decision making and build up data analytics capacities. Statistical offices are reflecting to what extent the traditional, cost-intensive data gathering methods can be replaced by Big Data analytics.[147]

In a number of scenarios, public sector bodies could significantly improve their decision making using commercially-held information, notably for reasons of public health policy, spatial and urban planning, natural and technological risk management, managing energy supply grids or protecting the environment.

Recent French Open Data legislation[148] has put in place the possibility for the government to request commercial players to give access to data they hold for the purpose of establishing public statistics.[149] This is subject to a number of procedural safeguards, namely a structured discussion with the private operator, a study on the feasibility and opportunity of such request and a consultation of the National Statistics Council. The decision to grant the right to access commercial data is taken by the minister in charge.

Along those lines, more authorities could be identified that could be granted such a right to access commercially-held data, while at the same time procedural safeguards would need to be put in place so that existing rights on data are being respected and compensation mechanism being devised.

Similarly, enhanced access to commercially-held data for scientific researchers funded from public resources could be contemplated.

---

[145] See in this respect: European Digital SME Alliance "Position paper on Data Economy" of 2 December 2016, http://www.digitalsme.eu/wp-content/uploads/2016/12/DIGITAL_SME_Position_Paper_Data-final.pdf.

[146] Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions (the Late Payments Directive) in its Article 7 uses already this standard for an unfairness control of standard contract terms in B2B contracts.

[147] See in particular the Scheveningen Memorandum on "Big Data and Official Statistics", http://ec.europa.eu/eurostat/documents/42577/43315/Scheveningen-memorandum-27-09-13; see also: https://ec.europa.eu/eurostat/cros/content/big-data_en; https://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.44/2015/mtg1/S2-8_WP16_UNSD__Snyder__P.pdf

[148] See above under 4.

[149] Article 19 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

Potentially, the notion of "public interest data" introduced in French legislation (see above) could be developed at European level for a defined class of data to which access could be given to public sector bodies and publicly funded researchers.

In case of access to and processing of personal data compliance with the General Data Protection Regulation must be ensured, notably, be based on a legal ground identified therein, respect to the rights of the data subjects concerned and comply with the obligations on controllers and other applicable guarantees.

(c) Data producer's right for non-personal or anonymised data

Another possible way forward envisaged by scholars is the creation of a new data producer right with the objective of enhancing the tradability of non-personal or anonymised machine-generated data as an economic good.[150]

In the remits of this solution, a number of questions need to be clarified:

(i) The scope of the right:

Such a right could be envisaged as a **right *in rem***[151] and assign the exclusive right to utilise certain data, including the right to licence its usage. This would include a set of rights enforceable against any party independent of contractual relations thus preventing further use of data by third parties who have no right to use the data, including the right to claim damages for unauthorised access to and use of data.

However, such right would not be conceivable with regard to personal data as the protection of the latter is a fundamental right in itself under which natural persons should have control of their own personal data (cf. recital 7 of the GDPR). Such control is ensured by legislation on the protection of personal data which confers enhanced rights on natural persons, reinforces obligations on data controllers and is backed by strong enforcement.

Alternatively, instead of creating the data producer right as a right *in rem*, it could be conceived of as **a set of purely defensive rights**.[152] This option would follow the choice made in the design of the protection given to know-how by the Trade Secrets Protection Directive[153]. Its objective would be to enhance the sharing of data by giving at least the defensive elements of an *in rem* right, i.e. the capacity for the de facto data holder to sue third

[150] In particular by H. Zech, Information as a tradable commodity, in: De Franceschi, European Contract Law and the Digital Single Market, 2016, pp. 51-79; M. Becker, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, in: Büscher/Glöckner/Nordemann/Osterrieth/Rengier (Eds.), Marktkommunikation zwischen Geistigem Eigentum und Verbraucherschutz. Festschrift für Karl-Heinz Fezer zum 70. Geburtstag, p. 815; this response is not considered to be an advisable way forward by: OECD, Maximising the Economic and Social Value of Data, (forthcoming); W. Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int 2016, p. 989; J. Drexl/ R. Hilty (et al.), On the Current Debate on Exclusive Rights and Access Rights to Data at the European Level, Max Planck Institute for Innovation and Competition Position Statement (16 August 2016), at p.12, D. Zimmer, Fragwürdiges Eigentum an Daten, Frankfurter Allgemeine Zeitung 18.11.2016, p. 16; Plattform Industrie 4.0, Industrie 4.0 – wie das Recht Schritt hält, Ergebnispapier, 2016, p. 22.

[151] A right *in rem* is the term used for property rights. Its specific characteristic is enforceable against the world (*erga omnes*) independent of contractual relations.

[152] W. Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int 2016, p. 989, appears to be favouring such an approach.

[153] Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157 of 15/06/2016, p. 1.

parties in case of illicit misappropriation of data. This approach thus equates to a protection of a de facto "possession" rather than to the concept of "ownership".[154]

In this respect, a number of civil law remedies could be introduced such as:

- the right to seek injunctions preventing further use of data by third parties who have no right to use the data,
- the right to have products built on the basis of misappropriated data excluded from market commercialisation and
- the possibility to claim damages for unauthorised use of data.

In order to not further limit discoverability of available data resources, scholars discuss whether the types of illegal uses that could give rise to such protection should be limited so that mere dissemination of (non-personal) data without that use is made of the data could remain lawful and not give rise to rights on the side of the data holder.[155]

Such an approach would, however, work on the assumption that what happens de facto is already a balanced and efficient data market. Such an assumption may not be correct. If this approach were taken in isolation and not in combination with other measures, it could be counterproductive and consolidate de facto situations which could amount to market failures.

(ii) The scope of data covered

In relation to the scope of data which could be covered, the findings on the EU legal acquis (above under 3.) points to a lack of legal certainty entailing the absence of legal protection in relation to non-personal or anonymised machine-generated data not yet structured in a protected database. Such data are also not safeguarded through intellectual or industrial property rights.

Consequently, a right *in rem* could be created on such data.

Independent of the scope, it is important to frame it so that only the syntactical level of information is protected, not the semantic level.[156] Care also needs to be taken so that any new right on data is not conceived as a super-IP right. It should only cover the syntactical (data, code) level, but not the ideas or information encoded.[157]

Metadata on the data would be part of the scope as they contain the information necessary to use the data subject to such a potential new right.

(iii) The allocation to a person or entity

If a data producer right is to be created as **a right *in rem*** and is to be awarded only on raw, non-personal machine-generated data, the allocation of the right (i.e. defining the "data producer") would be guided by a thorough analysis of all elements relevant for allocating such a right.

---

[154] H. Zech, Information as a tradable commodity, in: De Franceschi (Ed.), European Contract Law and the Digital Single Market, 2016, pp. 51 at 63.

[155] See M. Mattioli, Disclosing Big Data, Minnesota Law Review 2014, 535, at 579.

[156] See for the distinction: H. Zech, Information as a tradable commodity, in: De Franceschi (Ed.), European Contract Law and the Digital Single Market, 2016, pp. 51-79: An ebook or a photographic image, for example, has a semantic level which is the expression of ideas or the presentation of objects or persons. Copyright covers this level of information. The data file of such an ebook or image, however, is merely a representation of signs encoding such information usually requiring tools to present the information.

[157] As such ideas or information benefit already from intellectual or industrial property rights. A potential new right on data should enable data-driven innovation by providing access to relevant data for subsequent analysis.

One of the criteria for allocating the right could be to take into account the investments done and the resources put into the creation of the data. Such investments are made most often by two sides: The manufacturer of sensor-equipped machines, tools or devices (generating the data) who has invested in to the development and market commercialisation of the machine, tool or device and the economic operators using such machines, tools or devices paying a purchase price or lease and have to amortise the machine, tool or device.[158]

When several persons or entities jointly make investments into to data collection through a machine, tool or device, this could result in joint rights on the data generated. Freedom to contract should allow departing from that rule.

Other considerations could include liability obligations that either of the manufacturer or the users of the machines, tools or devices are subject to.

Some consider[159], that many data are subject to multiple players of rights and that this will make it conceptually virtually impossible to identify one or several owners. In their view, the concept of "ownership" is thus difficult to apply. Stakeholders also consider that defining rights of access to data is more relevant than defining ownership rights.[160]

If instead of a right *in rem*, a **set of purely defensive rights** is to be considered, such rights could protect *de facto* data holders that have lawful possession of data against unlawful use by others. This would complement technical efforts currently undertaken by data holders to protect their data and the transmission of such data against third parties with whom they do not have contractual relations. Similar to the approach taken by the Trade Secrets Protection Directive, the rights could even be made dependent on such technical protection efforts being made. The condition of the Trade Secrets Protection Directive that efforts must have been made to keep "information" "secret" (article 2) may need requalification when applied to "data" so as to account for the fact that in many scenarios, data need to be shared with a wider range of business partners in interconnected settings, while there remains a need to keep the data protected against any other third party.

(iv) Exceptions to the right

A potential data producer right may need to be limited by an obligation to share data. The rationale for potential exchanges depends on the person or entity to whom the right is allocated.

In case the right is allocated to the economic operator using the machine, tool or device, exceptions may need to be made for the manufacturer of such machine, tool or device. The manufacturer may not only have a legitimate interest to use such data for the purposes of further improving product design, but also may have a legal obligation to monitor the behaviour of his products on the market.[161] In some circumstances, there may be good reasons not to allocate the ownership to the economic operator using the machine, tool or device - or

[158] See H. Zech, Information as a tradable commodity, in: De Franceschi (Ed.), European Contract Law and the Digital Single Market, 2016, pp. 51 at 75; M. Becker, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, in: Büscher (et al., eds.), Festschrift für Karl-Heinz Fezer zum 70. Geburtstag, 2016, p. 815.

[159] e.g. OECD, Maximising the Economic and Social Value of Data, (forthcoming).

[160] High-level conference 17 October 2016 https://ec.europa.eu/digital-single-market/en/news/high-level-conference-building-european-data-economy.

[161] Obligation to monitor a product (Produktbeobachtungspflicht) under German law, the lack of observance of which can be the basis of tort liability.

not to allow the full range of actions usually available to an "owner"- notably on safety or security linked to the relevant data.

Secondly, in a number of instances there is a public interest to make certain data available for a number of private actors. This can be demonstrated in the case of (aggregated/ anonymised) smart metering information which is relevant for balancing the grid or in order to fully enable smart homes and living environments or care institutions.

Thirdly, public sector bodies may also have a legitimate interest in obtaining access to certain data. This has relevance for the provision of statistical information, urban planning, environmental protection, civil protection, etc. In most situations, public sector bodies would need aggregate information only.

Fourthly, in line with the Commission's policy on open science and open access, an exception ensuring access to relevant privately-held data could be considered for scientists performing research entirely or predominantly funded by public resources.

(v) Intended effects and flanking measures

According to the Coase theorem, the effects of an initial allocation of a good may be limited if the good is freely tradable and the transaction costs are sufficiently small.[162] Depending on market forces/ bargaining position, it is therefore possible that rights in data would be traded away to the actor(s) who would most benefit from its use.

Flanking measures in terms of banning unfair terms in consumer contracts or unfair business practices may be required to ensure a properly functioning market.

Technical measures such as digital watermarking (see above) would need to complement such a potential new right in order to make rights on data traceable.

(d) Access against remuneration to non-personal or anonymised data

Certain writers have been bringing forward arguments in favour of wider re-usability of data, including privately-held data by other economic players.[163]

Two situations can be broadly distinguished that may need to be considered separately: Access to data held for an economic player active on the same market and access to data for an economic player active on a different market, i.e. not being a competitor.

Firstly, linked to the very characteristic of data as a non-rival good, several parties can make use of data without a loss of quality.

Secondly, the claim is made that in many scenarios the value intrinsic to the data is minimal and critically depends on the capacity to make sense of the data (the algorithm).[164] The more the competitive advantage results from that capacity, the less important it is to control (and restrict) access to the data.

[162] R. H. Coase, The Problem of Social Cost, (1960) 3 The Journal of Law & Economics 1, 1960, pp. 1-44.

[163] Identifying avenues to make more commercially-held data available for re-use is supported at least in principle by: OECD, Maximising the Economic and Social Value of Data (forthcoming); J. Drexl, R. Hilty (et al.), Position Statement of the Max Planck Institute for Innovation and Competition on the current debate on exclusive rights and access rights to data at the European level, 2016; N. Shadboldt, H. Verdier, Report of the UK-French Data Task Force, 2016.

[164] OECD, Maximising the Economic and Social Value of Data (forthcoming).

Thirdly, for certain services, a convincing product and the capacity to create network effects may be more critical than access to data.[165]

Finally, (EU) competition law aims at ensuring a fair functioning of markets. While access to commercially-held data has not been at the heart of relevant case-law, conclusions can be drawn from case law on refusals to deal (to licence).[166]

From this it follows that certain types of data could possibly be identified to which access to third parties can be given with welfare-enhancing effects without impinging on the economic interests of the player that has invested into the data collecting capabilities. The OECD[167] in this debate refers to a "data commons" as a way to describe non-discriminatory access to certain data for at least a wider group of players, specifying that this should neither be confused with an "open data" or "open access" approach (access for the public at large), nor should it mean that access is given at no costs. The defining element of a "commons" is that non-discriminatory access is to be given, i.e. any member of a certain group (e.g. users of an industrial data platform[168]) can use the data for purposes defined by the party making the data accessible.

(i) Scope

In the context of data-driven innovation, challenges with respect to access to data can pertain in principle to any non-personal or anonymised data. A first, very wide approach could thus make any non-personal or anonymised data subject to regulated access. However, the fact that there is a cost in data generation and data have a value as a business asset, regulated access might be considered only for certain categories of data.

The fact that data can be re-used without a loss in data *quality* may not mean that the data will not lose in *value*, at least for some users. Exclusivity of access may give one party a competitive advantage, at least vis-à-vis competitors active on the same market. It requires further examination whether conclusions can be drawn for re-use of data by other economic players that are not active on the same market as the company holding the data. CJEU jurisprudence[169] points into this direction when an abuse of dominant position is examined.

In line with recently adopted French Open Data legislation[170], the notion of "public interest data" could be applied to such data. This notion would describe a specific class of data which are neither "open data" nor entirely private data. An interplay needs to be defined between principles or rules on enhanced access that apply across business sectors and sector-specific rules.

(ii) An obligation to licence

In legal terms, whatever the degree of openness mandated for non-personal or anonymised commercially-held data, access to such data would be implemented as an obligation on data holders to licence the use of the data.

The notion of an obligation to licence is not novel to the European legal framework. Noteworthy examples include:

[165] A. Lambrecht, C.E. Tucker, Can Big Data Protect a Firm from Competition? (published online).
[166] See above section 3.
[167] OECD, Maximising the Economic and Social Value of Data (forthcoming).
[168] See above under section 2.
[169] See above under section 3.
[170] See above under section 4.

- Regulation 715/2007 (as amended)[171] which foresees an obligation for "[m]anufacturers [to] provide unrestricted and standardised access to vehicle repair and maintenance information" on a basis that is not discriminating between "authorised dealers and repairers" and "independent operators".
- Similarly, Directive (EU) 2015/2366 on payment services in the internal market[172] provides for an obligation to provide access to certain information held by banks on an "objective, non-discriminatory and proportionate" basis in order to facilitate market access for new payment solutions (e.g. new schemes for card or internet payment) to the consumers and merchants and consequently lower costs for payments in the economy.
- To limit repeating the testing of chemical substances on animals, the EU Regulation on Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) obliges private companies to make study data accessible.[173]
- Recent French Open Data legislation[174] puts in place provisions that oblige commercial companies to open up – under certain conditions – data they hold for re-use.[175]
- Beyond the area of data, inspiration may be taken from practices regarding certain standards resulting from technology under patent. For the standard to be used as widely as possible, the patent holder is usually required to licence the use of relevant information on "standard essential patents"[176].

It requires further examination if – and if so – to what extent these examples are relevant when considering applying them to a wider range of types of data, economic operators or business scenarios.

It is interesting to note that the Commission proposal for the Database Directive[177] included an obligation to licence on makers of databases (on fair and non-discriminatory terms) for materials contained in databases which are publicly available but where the materials cannot be independently created, collected or obtained from another source. This obligation was subsequently discarded in the legislative process.

[171] See Recital 8 and articles 6-9 of Regulation 715/2007 of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, as last amended by Regulation (EU) No 459/2012 of 29 May 2012. The objective is to ensure an "effective competition on the market for vehicle repair and maintenance information services".

[172] Articles 35, 36 of 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, OJ L 337, 23.12.2015, p. 35; access is to be given to "payment services and "credit institutions' payment accounts services".

[173] See article 27 and 30 of Regulation 2006/1907 of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH); Commission implementing regulation (EU) 2016/9 of 5 January 2016 on joint submission of data and data-sharing in accordance with Regulation (EC) No 1907/2006 establishes detailed rules on the conditions under which data have to be shared.

[174] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JO République Française n°0235 of 8 October 2016, also referred to as "Loi Lemaire" after the government minister behind the proposal.

[175] See above section 4with details.

[176] Y Méniére, N Thumm, Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms. Research Analysis of a Controversial Concept, JRC Science and Policy Report 2015; J. Drexl, Designing Competitive Markets for Industrial Data in Europe – Between Propertisation and Access, 2016, at 47; M. Mariniello, Fair, reasonable and non-discriminatory (FRAND) terms: A challenge for competition authorities, J of Comp Law & Economics 7(3), p. 523-541.

[177] COM(92)24 final – OJ C 156 of 23/06/1992, p. 4, recital 31, article 8.

(iii) Licensing conditions

The degree of openness can range from full openness (the licensor is required to allow free access to data) to a set of intermediate options. Licensing conditions should be fair, reasonable and non-discriminatory between different licensees.[178]

In the instances referred to above, the following applies:

- In the context of access to in-vehicle information for the purposes of maintenance and repair, Regulation (EU) 715/2007 foresees that such information has to be made available on a non-discriminatory basis to both authorised and independent dealers and repairers. The manufacturer may charge a "reasonable and proportionate fee".[179]
- In the case of compulsory licensing in the context of standard-essential patents, licensing terms have to be "fair, reasonable and non-discriminatory" (FRAND). Courts are called to decide on disputes between licensors and potential licensees. This example shows also that implementation of FRAND terms in practice remains challenging.[180]
- In the context of REACH, the Regulation provides for rules on cost-sharing in the event that there is no contractual agreement on the remuneration given in exchange for access.[181]
- Finally, the Directive on re-use of public sector information[182] introduces conditions akin to FRAND principles for re-use of public sector information. It contains in particular an obligation for re-use conditions to be non-discriminatory "for comparable categories of re-use" (article 10 Directive 2003/98/EC as amended).[183] The Directive also puts a cap on the price (administrative charge) that could be asked for re-use of public sector information (article 6). With the 2013 revision of the Directive, that cap was made stricter and as a default rule no more than the marginal cost relating to the dissemination of the information can be charged for.[184] Such caps were not uncontroversial as some public sector bodies to a certain extent have been financing their activities from licensing fees for re-use of certain data they make available to third parties.[185]
- In the case of the French *Loi Lemaire*, the conditions applicable are to be set by way of delegated legislation.

[178] OECD, Maximising the Economic and Social Value of Data (forthcoming).

[179] As defined by Article 7(1) Regulation 715/2007 *e contrario* as " not [being] reasonable or proportionate if it discourages access by failing to take into account the extent to which the independent operator uses it."

[180] Notably due to the strategies of "patent hold-up" and "patent hold-out" employed by either party to the dispute on the licensing conditions, see: Y Méniére, N Thumm, Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms. Research Analysis of a Controversial Concept, JRC Science and Policy Report 2015; J. Drexl, Designing Competitive Markets for Industrial Data in Europe – Between Propertisation and Access, 2016, at 47; M. Mariniello, Fair, reasonable and non-discriminatory (FRAND) terms: A challenge for competition authorities, J of Comp Law & Economics, 2011, p. 523-541.

[181] Article 27, 30 Regulation 2006/1907.

[182] Directive 2003/98/EC as amended by Directive 201337/EU.

[183] One example is the distinction between non-commercial and commercial re-use, which under the 2003 version of the Directive was given as an example for differentiate pricing, see recital 19 of Directive 2003/98/EC.

[184] Article 6 (2) maintains the previous principle of full cost recovery, but as an the exceptional rule limited to certain cases.

[185] See justification to charge at full cost recovery in article 6(2) of the Directive.

Part 4: Liability

Based on the emergence of Big Data we have witnessed the rapid development of new technologies and, as a consequence, of sophisticated data-based products and services coming out from emerging technologies like Internet of Things (IoT) and Cloud Computing. Technological progress has contributed to the expansion and increased use of Artificial Intelligence (AI), allowing different autonomous systems applications (e.g. robots) to be deployed and used in numerous contexts, from industrial purposes to private uses.

One significant element in the operation of these emerging data based products and services are the highly complex interdependencies which are being formed between their different layers: the data layer (collection and processing), the software layer (whether embedded or not), the applications layer encompassing different apps, sensors and actuators, data services and/or tangible/ connected/ automated systems[186] devices, as well as the connectivity layer, such as the network connectivity, the data platforms and the digital infrastructures.

When damage occurs in the context of the use of such technologies, legal challenges may arise in relation to assigning liability, as well as in relation to product compliance, safety and insurance-related aspects.

Liability is defined in relation to a damage caused to another person. A liability regime defines the (natural or legal person) responsible in case damage is caused to another person and the conditions under which the latter can exercise its liability claims.

Contractual liability can be derived from the violation of the terms of the contract or statutory contract law rules.

Extra-contractual liability relates to the civil law responsibility for damage which caused outside the context of a contract (the damage being caused by a violation of a right or legitimate interest protected by law).

Product liability is a form of extra-contractual liability referring to the civil liability of manufacturers; at EU level this was introduced by the Directive on Defective Products Liability (85/374/CEE). This Directive establishes a strict liability,_i.e. where a defective product causes damage to a consumer, the producer may be liable even without negligence or fault on his part.

Under this Directive, a product is considered to be defective where it does not provide the safety which a person is entitled to expect, taking all circumstances into account[187]. The injured person carries the burden of proof having to demonstrate the actual damage, the defect in the product, and a causal link between the damage and the defect.

1. The new environment for liability in the digital economy

1.1 The Internet of Things (IoT)

Liability in relation to IoT products and services has been identified as a specific issue to be tackled as part of the Digital Single Market Strategy. A first analysis of liability and safety

[186] E.g. smart fridges, robots, drones, automated cars etc.
[187] Including the presentation of the product, the reasonable use of the product, and the time when the product was put on the market.

issues arising in relation to IoT products and services can be found in the recently published Staff Working Document "Advancing the Internet of Things in Europe"[188].

IoT is a wide-ranging ecosystem of physical objects connected to the Internet, capable of identifying themselves and communicating data to other objects with the help of a communication network for digital processing.

It is assumed that new market players will enter the chain of liability, both in relation to data gathered through IoT technologies, and in relation to any possible damage that may be caused by IoT devices introduced on the market and the related-services which are respectively being provided. Indeed, any IoT product/service is highly dependent on the quality and timeliness of the data which it receives and that are processed for various decision-making processes.

But the quality and accuracy of data are only one aspect in relation to the liability challenges that the IoT and autonomous systems raise. Thus, one of the most significant challenges for determining liability is the fact that the IoT ecosystem involves a wide range of market players which are each providing different parts and layers of this ecosystem. These different IoT layers encompass tangible elements (e.g. the hardware, products), the embedded software, the provision of software maintenance services, the supply of digital infrastructures as well as the processing and exploitation of data. Moreover, by the nature of its design, an IoT product/service is highly dependent on third party technologies to perform its functions and to also maximise the benefit to the user.

On the one hand, the multiplicity of market players may raise liability problems for defects in relation to one single IoT device, as well between the network of IoT connected devices. For instance, in the case of a connected car, damage may be caused by problems with defects which may originate from the product manufacturer, the internet provider, from the data platform holder or the connectivity provider. In the situation where the cars are connected among themselves, problems may also come from the inter-action and data exchange flow between these different vehicles.

On the other hand, and in addition to that, when different devices are being connected to the Internet and among themselves - which is the very specificity of the IoT - the difficulty for the consumer/user in identifying with which of the different market players the cause of the problem lies is all the more greater.

For instance, smart home technology promises many benefits, especially for elderly people living alone. A smart home could notify the resident when it is time to take medicine, alert the hospital if the resident falls and track how much the resident is eating. If a person is a little forgetful, the smart home could perform different tasks, such as shutting off the water before a tub overflow or turning off the oven if the cook had forgotten that. If, for instance, a problem occurs and the water is not turned off, thus leading to a flood and damage to property, the identification of where in the ecosystem of the different IoT devices the problem occurred or proving the relationship between the defect and damage may be complicated.[189]

Another example could be a security system in a smart home which will, in case of emergency, notify the resident that the fire alarm is on, connect to the system that locks the doors, by unlocking them, and connecting to the electric network of the house lighting the path to safety, finally connecting to the telephone landline and dial the fire department. If a

[188] SWD(2016) 110 final, https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe.

[189] In Hufford v Samsung Electronics (UK) Ltd., 148 for example, the claimant was unable to discharge the burden of proof that a fridge-freezer caused a fire in his home.

problem occurs and the interaction with the electric network of the house lighting is disrupted, it would be again difficult to discover whether there was for instance a problem of sensors failing to react, the data service itself being disrupted or an issue with the server connectivity.

The development of IoT technologies is therefore likely to create sophisticated interdependencies between product and service producers. These dependencies are not static. They can increase and become more complex, over the life of the product/service. They can give rise to challenges in determining where exactly the fault lies in the event of a problem. While issues relating to liability when products involve third party components are of course not new, they can be emphasised in some specific IoT applications[190] or more generally when different products are increasingly becoming connected among themselves and, for that purpose, more complex in their design and system integration features.

Any interdependency also gives rise to a number of questions such as to who is responsible for certifying the safety of the product, for ensuring the safety on an on-going basis and finally as stated before, how liability should be allocated in the event that the technology behaves in an unsafe way, causing damage.

These issues, if not properly addressed by existing legal frameworks or contractual arrangements, may result in legal uncertainty, increasing investment risks and thereby the roll-out of the Internet of Things.

It may also affect the uptake of data-driven services and products from the consumer side. Since most consumer products will tend to become "smart' products in the future, it is fair to assume that more and more end-users will be using a rather complex product involving complex interactions with third parties, necessary for its functioning.

Users of these new technologies may face legal uncertainty to claim damages and thus develop a lack of trust

1.2 Autonomous systems

Autonomous systems come in many different shapes and forms, ranging from classical industrial robots to self-driving cars, from highly autonomous combine harvester to unmanned underwater vehicles, from surgical robots to drones. What bind these diverse systems together is their physical embodiment and the fact that they are all capable to "understand" and "interpret" their environments and act appropriately.

Driven by technological progress in nano-electronics and low power computing, as well as by increased capabilities of the robots (such as sensing, actuating, cognitive vision and machine learning), these systems are increasingly endowed with the capacity to better perceive and interpret their environment, interact with humans, learn new behaviours and execute actions autonomously without a human in the loop.

The more autonomous these systems become, the less they can be considered simple tools in the hands of other actors (the manufacturer, the owner, the user, etc.). Autonomy has thus important legal implications insofar as the impact of such systems on their environment also triggers effects on third parties' rights and duties. The increasing degree of autonomy thus poses a challenge to the current regulatory framework as a natural or legal person needs to ultimately be held responsible for such an impact.

[190] The IoT agriculture market, domotics market.

More autonomous decision-making may thus conflict with the current regulatory framework which was designed in the context of a more predictable, more manageable and controllable technology. Clarifying and, if necessary, adapting the legislative framework is therefore essential for both citizens to be able to trust and make the best use of this technology and as well for the European industry to be able to lead and capture the opportunities arising in this field.

In the case of autonomous systems (e.g. robots) the increasing degree of autonomy is the feature that poses most challenges to the current liability rules. The autonomous decision-making features in robots - due to "learning", "understanding" and other "cognitive-like" features may lead to unexpected or unintended consequences.

2. Liability challenges in relation to Internet of Things and autonomous systems

To assess challenges in this field, one should ask whether the IoT and the autonomous systems trigger conceptually new liability issues or whether they raise new challenges for managing liability.

Given that IoT and autonomous systems are fairly new/emerging markets, more and in-depth information and evidence would have to be gathered to fully assess possible issues in relation to liability in the context of the use of such technologies.

Example: Connected and automated driving

Connected cars exchange information with other cars, or with the road infrastructure or with remote data bases. This allows for provision of driving assistance or mobility services or other type of services useful for the actors part of that value chain.

In principle, in EU countries, the law is currently quite clear in the respect that registered car owners are, in the first instance, liable for accidents caused by their vehicle and required to be insured against such an eventuality in accordance with the motor insurance directive. Car owners or the insurer then might have the opportunity to pursue recourse against the vehicle manufacturer if it can be established that the accident was caused by a defect for which the manufacturer is responsible under the Defective Product Directive. This was confirmed in the recommendations of the Commission GEAR 2030 working group on automated and connected vehicles.[191]

Cars have contained components produced by different entities for years, so that also for non-connected cars the technical determination of where the defect originated can be difficult. This is why the current liability framework attempts to reduce uncertainty by establishing liability ex ante, and in some cases with no necessity to prove fault.

But with increasing actors in the connectivity chain, the attribution of liability needs to be examined with care. Accidents could potentially be caused also by connectivity problems due to network failures under a complex bundle of physical products and services context.

[191] The GEAR 2030 High Level Group gathering the relevant Ministers, Commissioners and stakeholders was set up in October 2015 to make recommendations to the Commission to tackle the future challenges affecting the automotive sector by 2030. On automated and connected vehicles, the goal of the group is to present first recommendations by the end of 2016 (link here below) with final recommendations by mid-2017:
http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8640
https://circabc.europa.eu/w/browse/23eaf3be-3b5b-4b22-96a3-c4d33d254795 .

In the situation of partially self-driving vehicles, technology may take over some driving responsibilities but the driver may still be required to remain in control to monitor the operation by the vehicle software. This partial shift of paradigm may already in itself be problematic as the division and interplay between the roles, and consequently the liability, of humans and that of technology still needs to be investigated in the context of self-driving vehicles.

The problem may become more acute with fully automated vehicles. With no human in control, the product as a whole and the technology in particular need to be able to behave and perform safely, for instance the software algorithms or the sensors need to be able to cater for a wide range of unexpected situations.

With sophisticated IoT and autonomous systems, it is an open question whether liability for such emerging technologies should be modelled around rules on liability for defective products.

It is not clear either whether and how traditional concepts and provisions of the current legal regime for product liability (for instance, the definitions of ' defect', 'producer', 'damage', or the rule of the burden of proof) can apply in the context of IoT and autonomous systems.

In light of the IoT and autonomous systems characteristics, as exemplified above, questions may arise in relation to concepts used in product liability regimes.

1) It is not clear how to classify the IoT/autonomous system devices, whether for instance the IoT devices could be qualified as products or as services since it is possible that distinctions used in the past may not fully capture specificities of new complex digital technologies.[192] Most product liability regimes only apply to goods, while services and goods that come with the provision of a service being excluded. The matter is left to contractual arrangements which may provide for liability exclusions. In case of legal gaps or legal uncertainty, the consumer/user may face difficulties to claim certain type of damages that these IoT/autonomous systems can generate.

2. Does the definition of defect fit with the type of defects that may arise in systems encompassing software? Can a learnt new behaviour leading to damage be considered a defect? Even without learning systems, it needs to be clarified whether an undesirable autonomous behaviour can and should be considered a defect. Does the concept of "producer", fit with the type of roles and responsibilities that may arise in systems encompassing software and in the data value chain? Should the producer be the right or only right addressee of liability, since as stated above, the IoT devices generally involve many different actors in the value chain which all enable the IoT technology to function (product manufacturers, software producers, the connectivity service, the sensor manufacturers, the owner of the object, service provider independent from the manufacturer/software producer etc.).

In conclusion, as far as IoT products/services are concerned, and in light of their characteristics as described above it may become difficult to localise a malfunctioning problem and consequently hold a particular market player liable if something goes wrong between multiple IoT interoperating devices.

[192] For example, in the IoT context, an issue is to assess to what extent the "product" can be said to include its intangible component parts, specifically the software and the data, given that in some circumstances software was legally assessed as a service and not part of the device of which it is component.

In respect to the autonomous systems, robots may display increasing levels of autonomy and make decisions without human intervention even using in some cases degrees of artificial intelligence to perform tasks. This prompts the question whether in the case of sophisticated autonomous systems the degree of autonomy should be an important element in the legal framework.

EC services are currently evaluating the Directive on Liability for defective products. The evaluation will analyse whether the challenges of determining and allocating liability arising from the generation and processing of data based products coming out of these emerging technologies are appropriately dealt with.

Therefore, the Commission will invite stakeholders in the upcoming debate to explore the feasibility of different other approaches which may provide interesting avenues for addressing these challenges. Discussions may revolve around the following broad directions:

- A **strict liability regime**

- A liability regime based on a **risk-generating** approach. According to this principle, liability would be assigned to the actors generating a major risk for others and benefitting from the relevant device, product or service.

- A **risk-management** approach, where liability is assigned to the market actor which is best placed to minimize or avoid the realisation of the risk or to amortize the costs in relation to those risks.

- These solutions could be coupled with voluntary or mandatory insurance schemes for compensating the parties who suffered the damage. Such schemes could for instance be funded by insurance contributions made by manufacturers, software developers, as well as other relevant market players in the IoT/robotics value chain. This approach would need to build on the dual objective of both providing legal protection to investments made by business, while reassuring consumers regarding a fair compensation or an appropriate insurance in case of damage.

Finally, apart from the issues related to extra-contractual liability, further reflection may also be needed to assess whether clarification or adaptation of existing contract law rules are needed for the Machine-2-Machine contracting paradigm.

The increased use of automated auctioning systems, automated trading in stock markets, as well as, more generally of new digital technologies such as distributed ledgers technology (blockchains) deserve particular attention with a view to understand whether they raise any challenges in respect of traditional civil and contract law concepts and rules.

Part 5: Portability of non-personal data

1. Introduction

With the rise of the Internet economy, the importance of data portability – or the absence thereof – has significantly increased. However, while most of the discussions so far have revolved around the portability of personal data, there has been less discussion on the opportunities and potential adverse effects of portability of non-personal data, or the possibility for businesses to port the data they have provided to their service providers.

2. Legal discussion on data portability

Portability is generally understood as the ability to move, copy or transfer something. As a legal term, data portability is used in different contexts and for different purposes, the definitions varying slightly.

Then GDPR introduces and lays down the right of data subjects to receive or have transmitted in a structured, commonly used and machine-readable format personal data concerning her/him that they have provided to a controller and that is processed either on the basis of consent (i.e. pursuant to article 6(1)(a)) or on the basis of a contract (article 6(1)(b)). It encompasses both transmitting personal data from one controller to another, where technically feasible, and the data subject receiving the data from the controller.

One point which needs interpretation concerns the precise scope of the provision in terms of the personal data which is eligible to be ported. The provision says the data subject has a right to port any data which she or he has "provided" to the controller. The question remains what is to be considered as "provided" by the data subject in any given situation. The Article 29 Working Party[193] has issued guidelines on this specific point and applies a broad definition.[194] Not only data "actively and knowingly" provided by the data subject are to be covered by the scope of the right to data portability, but also data provided "by virtue of the use of a service or a device". Examples for the latter would be "raw data generated by a smart meter" or heartbeats recorded by a fitness tracker. On the other hand, data created by the data controller on the basis of data provided by the data subject (the Article 29 WP refers to them as "inferred data" or "derived data") would fall outside the scope of the right to data portability.

In the context of consumer protection, the Unfair Commercial Practices Directive 2005/29/EC (Article 9) prohibits traders to impose onerous or disproportionate non-contractual barriers when a consumer wishes to e.g. "switch to another product or trader".

In order to prevent lock-in situations for the consumer, article 16 of the Commission proposal for a Directive on contracts for the supply of Digital content[195] offers the consumers a right to terminate long term contracts and thereby a possibility to switch providers.

The term "switching" is, however, also often used to describe data portability, e.g. in the telecom sector and for digital services such as cloud services.

---

[193] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.

[194] Guidelines on the right to data portability of 13 December 2016; we note that these guidelines may change based on comments that can be made until the end of January 2017.

[195] COM/2015/0634 final - Proposal for a Directive on certain aspects concerning contracts for the supply of digital content.

In the telecom services legal framework[196], portability refers simply to the portability of phone numbers, i.e. the right to have your number ported, when switching providers, from a provider to a new one.

Similarly, for cloud services, data portability is the ability of a cloud service customer to move their data and/or their applications between two different cloud service providers at low cost and with minimal disruption.

Businesses currently rely on contractual arrangements to ensure the portability of data they have provided to online services, including cloud services. Anecdotal evidence[197] suggest that clauses on data portability are often left out of contracts, and that smaller business actors can experience difficulties in getting their data back e.g. upon termination of the contract.

3. Data portability from an economics perspective

Enhancing access to data is one means through which the value of data can be maximised in society. Data portability is one way to ensure such access.[198] In a standard market setting, portability lowers switching costs, i.e. reduces the cost to move from one online service to a functionally identical online service supplied by another firm. That, in turn, promotes competition between these online services. Competition benefits users but not necessarily the service providers who tend to restrict data portability, possibly as a strategic attempt to create significant switching costs. This model applies to certain extent to cloud service providers, where competing providers indeed offer similar services.

In contrast, such single-sided market assessment may change in the case of online platforms, generally characterised as two- or multi-sided markets – i.e. they bring together suppliers and customers/consumers, and possibly other categories of users, such as advertisers or other service providers and other intermediaries.

One of the main features of these platforms is the presence of indirect network effects between the different user groups.. In addition, online platforms generate and collect unprecedented volumes of data, shared – against remuneration or not – in some cases with third parties whose business models rely sometimes extensively on accessing these data. Platforms can try to maintain their user base on each side of the market through high switching costs, including through the lock-in of data in the platforms' environment. Other factors do play an important role, such as the presence of economies of scale, users' preferences that allow for platform differentiation, the platform's capacity (or congestion) constraints, direct network effects and (especially) indirect network effects, or the prevalence of multi-homing (when users are active simultaneously on multiple similar or equivalent platforms).

In general, online platforms do not consistently offer equivalent services, though there are specific exceptions (e.g. marketplaces or messaging apps). Even when switching platforms

[196] Universal Service Directive (2002/22/EC) Article 30.

[197] Comments made by participants at the EC workshop on Building the European Data Economy on 21 September 2016; findings published at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=34617

[198] OECD, Maximising the Economic and Social Value of Data (forthcoming). W. Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int 2016, p. 989; J. Drexl/ R. Hilty (et al.), 'On the Current Debate on Exclusive Rights and Access Rights to Data at the European Level' Max Planck Institute for Innovation and Competition Position Statement (16 August 2016), at p.12; D. Zimmer, Fragwürdiges Eigentum an Daten, Frankfurter Allgemeine Zeitung of 18 November 2016, p. 16.

would be possible for business users, it is not consistently true that they would be locked-in only/mainly because of restrictions on data portability. The strength of indirect network effects might, for instance, play a bigger role in their refusal to leave the platform. Multi-homing practices point to situation where data portability is not a primary condition for businesses to pick, use or switch to competing services. In terms of social welfare analysis, the economic analysis of data portability in platform markets suggests that the general presumption in favour of portability is not necessarily in the wider public interest, or even in the interest of consumers in some specific cases.[199]

An obligation to data portability could have a chilling effect on firms' incentives to innovate.[200] While widely recognised as a means to make information more accessible and communication easier, create new business opportunities and increase choice of products and services[201], online platforms are also an important example of data-driven service providers. It is unclear what effect data portability would have on their ability to build on and maintain the essential network effect.

In this context, the rapid evolution of online platforms into new markets such as business-to-business e-commerce spaces[202] or in the context of the Internet of Things can lead to new effects and dynamics which need to be carefully observed and assessed to ensure that fair and innovative markets persist.

It has been argued that for certain types of platforms, namely the online social networks, the effects of data portability on competition might not be as strong. For these types of actors, platform interoperability rather than data portability might be an alternative way to increase competition and level the playing field.[203] However, others claim there are evidence suggesting that data portability may in effect foster a certain level of interoperability of online platforms.[204]

4. Emerging opportunities around data portability of non-personal data

Introducing a general right to data portability for non-personal data could be seen as a possible means to enhance competition, stimulate data sharing and avoid vendor lock-in. Therefore, the Commission will invite stakeholders to discuss the extent to which this assessment can be generalised and what the adverse effects of a portability right for non-personal data can entail on particular markets. The consultation attempts to also gather facts on current practices. Acknowledging that portability might be more suitable for some services rather than others, the consultation opens the avenues of possible interventions ranging from a

[199] P. Swire/ Y. Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, Public Law and Legal Theory Working Paper Series No. 204, 2013.
[200] Idem. (also citing Swire and Lagos, 2013, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique).
[201] This was confirmed by the results from the European Commission's open public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy (the platforms consultation), see: https://ec.europa.eu/digital-single-market/news/first-brief-results-public-consultation-regulatory-environment-platforms-online-intermediaries .
[202]https://www.bcgperspectives.com/content/articles/sales_channels_digital_economy_out_front_exploiting_digital_disruption_b2b_value_chain/.
[203] I. Graef, Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union, Telecommunications Policy 39, 2015, 502–514.
[204] In OECD's forthcoming paper on the benefits and challenges of enhanced data access, portability is claimed to foster horizontal interoperability of platforms, which is the ability to move from one platform to another. OECD, Maximising the Economic and Social Value of Data (forthcoming).

portability right for non-personal data, to recommended contract terms for switching providers, to sector-specific data standards encoding access and portability rules.