EUROPEAN
COMMISSION

Brussels, 10.1.2017
COM(2017) 9 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

"BUILDING A EUROPEAN DATA ECONOMY"

{SWD(2017) 2 final}

"BUILDING A EUROPEAN DATA ECONOMY"

1. INTRODUCTION

Data has become an essential resource for economic growth, job creation and societal progress. Data analysis facilitates the optimisation of processes and decisions, innovation and the prediction of future events. This global trend holds enormous potential in various fields, ranging from health, environment, food security, climate and resource efficiency to energy, intelligent transport systems and smart cities.

The "data economy"[1] is characterised by an ecosystem of different types of market players – such as manufacturers, researchers and infrastructure providers – collaborating to ensure that data is accessible and usable. This enables the market players to extract value from this data, by creating a variety of applications with a great potential to improve daily life (e.g. traffic management, optimisation of harvests or remote health care).

The value of the EU data economy was estimated at EUR 257 billion in 2014, or 1.85% of EU GDP.[2] This increased to EUR 272 billion in 2015, or 1.87% of EU GDP (year-on-year growth of 5.6%). The same estimate predicts that, if policy and legal framework conditions for the data economy are put in place in time, its value will increase to EUR 643 billion by 2020, representing 3.17% of the overall EU GDP.

Under the General Data Protection Regulation (GDPR)[3], as of May 2018, there will be one single pan-European set of rules contrary to 28 national laws today. The newly created one-stop-shop mechanism[4] will ensure that one data protection authority ("DPA") will be responsible for the supervision of cross-border data processing operations carried out by a company in the EU. Consistency of interpretation of the new rules will be guaranteed. In particular, in cross-border cases where several national DPAs are involved, a single decision will be adopted to ensure that common problems receive common solutions. In addition, the GDPR creates a level playing field between EU and foreign companies in that companies based outside the EU will have to apply the same rules as European companies if they are offering goods and services or monitoring the behaviour of individuals in the EU. An increased level of consumer trust will benefit both EU and external commercial operators.

---

1 The data economy measures the overall impacts of the data market – i.e. the marketplace where digital data is exchanged as products or services derived from raw data – on the economy as a whole. It involves the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data enabled by digital technologies (European Data Market study, SMART 2013/0063, IDC, 2016)

2 European Data Market study, SMART 2013/0063, IDC, 2016

3 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 95/56/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1

4 Article 56 of the GDPR.

The ePrivacy Directive concerns the confidentiality of electronic communications services in the EU. The revised ePrivacy Directive, proposed in parallel to this Communication in the form of a Regulation[5], aims at ensuring a high level of protection in full coherence with the GDPR. Strong data protection rules create the trust that will allow the digital economy to develop across the internal market.

As President Juncker stressed in his State of the European Union speech on 14 September 2016, "*[b]eing European means the right to have your personal data protected by strong, European laws. Because Europeans do not like drones overhead recording their every move, or companies stockpiling their every mouse click. This is why Parliament, Council and Commission agreed in May this year a common European data protection regulation. This is a strong European law that applies to companies wherever they are based and whenever they are processing your data. Because in Europe, privacy matters. This is a question of human dignity*."

In its 2012 Communication "Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century"[6] and 2014 Communication "Towards a thriving data-driven economy"[7], the Commission recognised that modern, coherent rules across the EU are needed for data to flow freely from one Member State to another, that the European digital economy had been slow in embracing the data revolution compared with the USA and also lacked comparable industrial capability. It concluded that the lack of a legal environment adapted to the trade of data within the EU may contribute to insufficient access to large datasets, possible entry barriers to new market entrants, and stifling effects on innovation.

Unjustified **restrictions on the free movement of data** are likely to constrain the development of the EU data economy. These restrictions relate to requirements imposed by public authorities on the location of data for storage or processing purposes. The issue of free movement of data concerns all types of data: enterprises and actors in the data economy deal with industrial and machine-generated data whether personal or not, as well as data created due to human action. In the Digital Single Market (DSM) strategy, the Commission announced that it would propose an initiative to tackle restrictions on the free movement of data for reasons other than the protection of personal data within the EU and unjustified restrictions on the location of data for storage or processing purposes. Such restrictions include legal acts adopted by Member States, administrative rules and practices having the same effect. Their number tends to expand as the data economy grows, hence generating uncertainty as to where data can be stored or processed. This may impact all sectors of the economy, and both private and public-sector organisations, which could have difficulties accessing more innovative and/or cheaper data services. Unjustified data location restrictions impair the freedom to provide services and the freedom of establishment stipulated in the Treaty, also contravening the relevant secondary law. This risks fragmenting the market, reducing the quality of service for users and reducing the competitiveness of the data service providers, especially smaller entities.

---

5 COM (2017) 10

6 COM (2012) 9

7 COM (2014) 442

Unjustified data localisation is also part of discussions between the EU and its trading partners, given the increasing importance of data and data services in the global economy and potential attitudes of third countries towards this question. The EU data protection rules cannot be subject of negotiations in a free trade agreement. As explained in the Communication on exchanging and protecting personal data in a globalised world[8] dialogues on data protection and trade negotiations with third countries have to follow separate tracks. Beyond this, as indicated in the Trade for All Communication[9], the Commission will seek to use EU trade agreements to set rules for e-commerce and cross-border data flows and tackle new forms of digital protectionism in full compliance with and without prejudice to the EU's data protection rules.

Furthermore, as the data-driven transformation reaches into the economy and society, ever-increasing amounts of data are generated by machines or processes based on emerging technologies, such as the Internet of Things (IoT), the factories of the future and autonomous connected systems. Connectivity itself changes the way data can be accessed: increasingly, data which were usually accessed through physical connections can now be accessed remotely. The enormous diversity of data sources and types, and the rich opportunities for applying insights into this data in a variety of domains, including for public policy development, are only beginning to emerge. To benefit from these opportunities, both public and private players in the data market need to have access to large and diverse datasets. The issues of access and transmission in relation to the data generated by these machines or processes are therefore central to the emergence of a data economy and require careful assessment.

Other emerging issues concern the application of the rules on liability for any damages resulting from a fault in a connected device or a robot; and portability and interoperability of the data. In the context of new technologies such as the Internet of Things (IoT) or robotics there are complex and sophisticated interdependencies both within products (based on hardware and software) and across interconnected devices. Moreover, new issues can emerge from autonomous machines, whose unexpected and unintended behaviour could create damages to persons and objects. These phenomena may create legal uncertainty in relation to the application of the existing framework on liability and safety.

As announced in the DSM, the Commission's objective is to create a clear and adapted policy and legal framework for the data economy, by removing remaining barriers to the movement of data and addressing legal uncertainties created by new data technologies. Further objectives underpinning this Communication aim at increased availability and use of data, the fostering of new data business models as well as improving the conditions for access to data and the development of data analytics in the EU. To this end, the Commission is presenting focussed issues for discussion with a view to "Building a European data economy".

Accordingly, this Communication explores the following issues: free flow of data; access and transfer in relation to machine-generated data; liability and safety in the context of emerging technologies; and portability of non-personal data, interoperability and

[8] COM (2017) 7

[9] COM (2015) 497

standards. This Communication also sets out suggestions for experimenting with common regulatory solutions in a real-life environment.

The Commission is launching a wide stakeholder dialogue on the issues explored in this Communication. The first step of this dialogue is a public consultation, launched in parallel to the data economy package[10].

2. FREE FLOW OF DATA

A well-functioning and dynamic data economy requires the flow of data in the internal market to be enabled and protected. In a rapidly evolving technological context, a safe and reliable free flow of data is instrumental to the protection of the four fundamental freedoms of the EU single market enshrined in the Treaties (goods, workers, service provision and capital). Data services are growing rapidly in the EU and worldwide. An efficient and barrier-free Single Market in this sector would create significant opportunities for additional growth and jobs.

This growth and innovation in the data economy as well as the implementation of cross-border public services can be jeopardised by barriers to the free movement of data in the EU, such as unjustified data localisation requirements imposed by public authorities. Data localisation measures effectively reintroduce digital 'border controls'[11]. They range from requirements by supervisory authorities that financial service providers store their data locally, to the implementation of professional secrecy rules, implying local data storage or processing, and sweeping regulations requiring the local storage of archived information generated by the public sector, whatever its sensitivity.

Privacy concerns are legitimate concerns but should not be used by public authorities as a reason to restrict the free flow of data in an unjustified way. As indicated above, the GDPR provides a single set of rules with a high level of protection of personal data for the entire EU. It reinforces consumer confidence in online services, and ensures a uniformed application of the rules in all Member States through stronger national data protection authorities. The GDPR fosters the necessary trust for data processing and is the foundation for the free flow of personal data in the EU. The GDPR bans restrictions on the free movement of personal data within the Union where these are based on reasons connected with the protection of personal data[12]. However, restrictions based on other reasons than the protection of personal data, e.g. under taxation or accounting laws, are not covered by the GDPR. Furthermore, non-personal data, i.e. data not relating to an

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

[11] OECD, "Emerging Policy Issues: Localisation Barriers to Trade", 2015 and on-going work

[12] Article 1(3). E.g. a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public will qualify as personal data, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person. See judgment in Case C-582/14, Breyer, ECLI:EU:C:2016:779, at para. 49.

identified or identifiable natural person[13], remain outside the scope of GDPR and can concern for instance non-personal machine generated data.

Data location restrictions may arise from legal rules or administrative guidelines or practices that require the storage or processing of data[14] in an electronic format[15] to be limited to a particular geographical area or jurisdiction. Sometimes restrictions are imposed by Member States in the belief that supervisory authorities can more easily scrutinise locally stored data. Localisation is also used as a proxy for assurances in terms of privacy, audit and law enforcement, as well as security of data. However, in practice, these measures rarely contribute to the objectives they are intended to achieve.

Information security depends on a range of factors besides where the data is physically stored, such as maintaining its confidentiality and integrity when the data is available outside its storage facility. In this respect, rather than data location restrictions, the real enablers of secure data storage and processing are state-of-the-art ICT management best practices on a scale far larger than individual systems. For example, to keep data safe from localised natural disasters or cyberattacks, data storage facilities located in different Member States may be the back-up for one another and make use of the technical and organisational measures foreseen in the Directive on Security of Network and Information Systems[16] (the NIS Directive). Moreover, the availability of data for regulatory or supervisory purposes, which is not called in any way into question, would be better ensured by enhancing the cooperation between national authorities, or between such authorities and the private sector, rather than through localisation restrictions. Indeed, in an area characterised by close cooperation between supervisory authorities, such as financial services, data localisation requirements could prove counter-productive.[17]

Nevertheless, data localisation requirements may be justified and proportionate in particular contexts or in relation to certain data, especially before effective cross-border cooperation arrangements are put in place, such as ensuring the secure treatment of certain data pertaining to critical energy infrastructure, or the availability of electronic evidence (e.g. as localised copies of datasets) for law enforcement authorities, or local storage of data held in certain public registers.

Unfortunately, the trend, both globally and in Europe, is towards more data localisation, an approach often based on the misconception that localised services are automatically safer than cross-border services. Moreover, the data services market is substantially influenced by lack of transparent rules and a strong perception of the need to localise

---

13 As defined in Article 4(1) of the GDPR.

14 Both privately-held and publicly-held data

15 Including copies of datasets

16 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1

17 A number of EU provisions concerning financial services and the European system of financial supervision require that supervisors have access to data on financial institutions and transactions anywhere in the territory of the EU. Requirements that data be stored in a particular national territory, or which condition supervisory access to administrative procedures could reduce access by the supervisory authorities to data that is essential for them in the implementation of their mandate.

data. This may limit the access of businesses and public sector organisations to cheaper or more innovative data services, or force businesses operating cross-border to arrange excess data storage and processing capabilities. This could also inhibit data-driven businesses, in particular start-ups and SMEs, from scaling-up their activities, entering new markets (e.g. by having to invest in data centres in 28 Member States) or centralising data and analytics capacities in order to develop new products and services.

Europe currently sources 84% of its final demand in "ICT-related" services (consulting, hosting, development) internally within the EU. If these services could also operate more easily across borders within the EU through the removal of data localisation restrictions, this could lead to GDP gains of up to EUR 8 billion per year in cost savings and efficiency gains[18].

Data localisation also hampers the wider adoption of cloud storage and computing. This could also have wider societal effects. Indeed, a more efficient use of IT resources could contribute to the reduction of energy consumption and carbon emissions by net 30% or more. A small business moving to the cloud could reduce its energy consumption and carbon emissions by more than 90%, by running its business applications in the cloud instead of running those same applications on its own infrastructure. The global energy-efficient data centre market is expected to grow to almost EUR 90 billion by the end of 2020. A fragmented data services market would hinder the full development of these more energy-efficient services in the EU and also put at risk the willingness to invest.

In order to address the issues and restrictions outlined above and realise the full potential of the European data economy, any Member State action affecting data storage or processing should be guided by a "**principle of free movement of data within the EU**", as a corollary of their obligations under the free movement of services and the free establishment provisions of the Treaty and relevant secondary legislation. Any current or new data location restrictions would need to be carefully justified under the Treaty and relevant secondary law to verify that they are necessary and proportionate to achieve an overriding objective of general interest, such as public security[19].

The principle of free movement of personal data[20] enshrined in primary and secondary law should also apply in the cases where the GDPR allows Member States to regulate specific matters. Member States should be encouraged not to make use of the opening clauses in the GDPR to further restrict the free flow of data.

---

18 "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", ECIPE, 2016, calculation based on increased competitive pressure under a fully price-transparent "industrial" DSM

19 Taking into account that the Treaty exceptions are to be interpreted restrictively. Such relevant secondary law includes the GDPR, Directive 2000/31/EC (the E-commerce Directive), Directive 2006/123/EC (the Services Directive) and, as regards draft technical regulations and draft rules on Information Society Services, Directive 2015/1535 (the Transparency Directive).

20 The free movement of personal data is contained in Article 16 of the Treaty on the Functioning of the European Union, and the rules for the free movement of personal data are set out in the current and future EU data protection legislation. Article 1(3) of the General Data Protection Regulation states: "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

In its conclusions of 15 December 2016, the European Council called for removing remaining obstacles within the Single Market, including those hampering the free flow of data.[21]

In order to implement the principle of free movement of data, the Commission will take the following two steps:

- Following the publication of this Communication, the Commission will enter into structured dialogues with the Member States and other stakeholders on the justifications for and proportionality of data location measures, taking as a starting point the restrictions identified so far by the Commission.

- Following the results of the dialogues and the further evidence-gathering on the extent and nature of data location restrictions and their impacts, notably on SMEs and start-ups *inter alia* through the accompanying public consultation, the Commission will, where needed, launch infringement proceedings to address unjustified or disproportionate data location measures, and, if necessary, the Commission may also take further initiatives on the free flow of data. In this context, any follow-up action will be undertaken in line with Better Regulation principles.

3. DATA ACCESS AND TRANSFER

Ever-increasing amounts of data are generated by machines or processes based on emerging technologies, such as the Internet of Things. Such data is increasingly used as a key component for new, innovative services, in order to improve products or production process and to support decision-making.

The diversity of data generated by these machines or processes presents rich opportunities for players in the data market to innovate and apply insights into this data. For example, the data captured by sensors used in modern farms could be used to create an application to optimise harvesting, or the data generated by sensors in traffic lights could be used to create an application for traffic management, or route optimisation.

In order to extract the maximum value from this type of data, market players need to have access to large and diverse datasets. However, this becomes more difficult to achieve if the generators of the data keep it to themselves, and the data is consequently analysed in silos. The issues of access and transfer in relation to the raw data (i.e. data that has not been processed or changed since its recording) generated by these machines or processes are therefore central to the emergence of a data economy and require careful assessment.

The issue of access to machine-generated data is under consideration in several sectors, such as transport, energy markets, smart living environments, and the health and care sector.

[21] http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/

Before examining the current situation with respect to data access in the EU, it is important to clarify the type of data under consideration in this context.

3.1. Type of data under consideration

In general, data can be personal or non-personal. For example, data generated by home temperature sensors may be personal in nature if it can be related to a living person, while data on soil humidity is not personal. Personal data can be turned into non-personal data through the process of anonymisation. Where data qualifies as personal data[22], the data protection framework, in particular the GDPR, will apply.

Machine-generated data is created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real.

Machine-generated data can be personal or non-personal in nature. Where machine-generated data allows the identification of a natural person, it qualifies as personal data with the consequence that all the rules on personal data apply until such data has been fully anonymised (e.g. location data of mobile applications).

One common theme linking the free flow of data with the emerging issues of access and transmission of data is that enterprises and actors in the data economy will be dealing with both personal and non-personal data, and that data flows and datasets will regularly contain both types. Any policy measure must take account of this economic reality and of the legal framework on the protection of personal data, while respecting the fundamental rights of individuals.

3.2. Limited access to data

In order to assess this emerging issue, analysis is first required of how companies and other market players can access the large and diverse datasets that are needed in the data economy.

Available evidence[23] reveals that companies holding large quantities of data generally tend to use mostly in-house data analytics capabilities. In the majority of cases, data is generated and analysed by the same company, and even when data analysis is subcontracted, further re-use of the data may not take place. Furthermore, in some cases manufacturers, companies offering services or other market players holding data keep the data generated by their machines or through their products and services for themselves, thus potentially restricting reuse in downstream markets. Many companies do not benefit from or allow for the possibility of user-friendly Application Programming Interfaces

22 As defined in Article 4(1) of the GDPR.

23 IDC, European Data Market Study, First Interim Report, 2016; Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, First interim report, 2016; DG Connect high-level conference, 17 October 2016

(APIs)[24] (which specify how different applications should interact with each other) that can serve as safe entry ports for new and innovative uses of data held by the companies.

Overall, therefore, exchange of data currently remains limited. Data market places are slowly emerging, but are not widely used. Companies may not be equipped with the right tools and skills to quantify the economic value of their data, and they may fear losing or compromising their competitive advantage when data becomes available to competitors.

3.3. Raw machine-generated data: Legal situation at EU and national level

Raw machine-generated data are not protected by existing intellectual property rights since they are deemed not to be the result of an intellectual effort and/or have any degree of originality. The sui generis right of the Database Directive (96/9/EC) – which gives makers of databases the right to prevent extraction and/or reutilisation of the whole or of a substantial part of the contents of a database – may provide protection only under the condition that the creation of such a database involves substantial investment in the obtaining, verification or presentation of its contents. The recently adopted Trade Secrets Protection Directive (2016/943/EU), to be transposed into national law by June 2018, will grant protection to trade secrets against their unlawful acquisition, use and disclosure. For data to qualify as a "trade secret", measures have to be taken to protect the secrecy of information, which represents the 'intellectual capital of the company".

Under the law of different Member States, legal claims are applied to data only when that data meets specific conditions for it to qualify, for instance, as an intellectual property right, database right or a trade secret. However, as at EU level, raw machine-generated data as such would not generally meet the relevant conditions.

Therefore, comprehensive policy frameworks do not currently exist at national or Union level in relation to raw machine-generated data which does not qualify as personal data, or to the conditions of their economic exploitation and tradability. The issue is largely left to contractual solutions. The use of existing general contract law and competition law instruments available in the Union might be a sufficient response. In addition, voluntary or umbrella agreements covering certain sectors might be envisaged. Nevertheless, where the negotiation power of the different market participants is unequal, market-based solutions alone might not be sufficient to ensure fair and innovation-friendly results, facilitate easy access for new market entrants and avoid lock-in situations.

3.4. Situation in practice

In some cases manufacturers or service providers may become the *de facto* "owners" of the data that their machines or processes generate, even if those machines are owned by the user. A *de facto* control of this data can be a source of differentiation and competitive advantage for manufacturers. However, this can be problematic, because the user is often prevented by the manufacturer from authorising usage of the data by another party.

[24] For example, https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

The different market players that are in control of the data, depending on the specificities of the markets, may thus take advantage of gaps in the regulatory framework, or of the legal uncertainties described above, by imposing unfair standard contract terms on the users or through technical means, such as proprietary formats or encryption. While several Member States have extended the scope of application of the consumer protection Directive on Unfair Contract Terms also to B2B transactions, not all have done so. This could result for instance in users and businesses becoming locked into exclusive data exploitation arrangements. Voluntary data sharing might emerge, but negotiating such contracts could entail substantial transaction costs for the weaker parties, when there is an unequal negotiation position or because of the significant costs of hiring legal expertise.

3.5. A future EU framework for data access

Ensuring access to machine-generated data is currently being explored by some Member States, which may decide to regulate this issue by themselves. An uncoordinated approach risks creating fragmentation and would be detrimental to the development of the EU data economy and the operation of cross-border data services and technologies in the internal market.

Accordingly, the Commission intends to engage in a dialogue with Member States and other stakeholders to explore a possible future EU framework for data access. In the Commission's view, this dialogue should revolve around the most effective ways to achieve the following objectives:

- **Improve access to anonymous machine-generated data**: Through sharing, reuse and aggregation, machine-generated data becomes a source of value-creation, innovation and diversity of business models.[25]

- **Facilitate and incentivise the sharing of such data**: Any future solution should foster effective access to data, taking into account, for example, possible differences in bargaining power between market players.

- **Protect investments and assets**: Any future solution should also take into account the legitimate interests of market players that invest in product development, ensure a fair return on their investments and thereby contribute to innovation. At the same time, any future solution should ensure a fair sharing of benefits between data holders[26], processors and application providers within value chains.

- **Avoid disclosure of confidential data**: Any future solution should mitigate the risks of disclosing confidential data, in particular to existing or potential competitors. In this regard it should also allow for proper data classification to be performed, prior to the assessment of whether or not a certain piece of data can be shared.

[25] Where personal data is concerned, the GDPR applies.

[26] The entity that manages and retains the machine-generated data in practice.

- **Minimise lock-in effects**: The unequal bargaining power of companies and private individuals should be taken into account. Lock-in situations, especially for SMEs and startups and private individuals, should be avoided.

In the stakeholder dialogues, the Commission intends to discuss the following possibilities for addressing the issue of access to machine-generated data, which differ in their level of intervention:

- **Guidance on incentivising businesses to share data**: To mitigate the effects of divergent national regulations and provide increased legal certainty for companies, 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 transparency and fairness requirements laid down by EU marketing and consumer law, the Trade Secrets Directive and copyright legislation, notably the Database Directive. The Commission intends to launch an evaluation of the Database Directive in 2017.

- **Fostering the development of technical solutions for reliable identification and exchange of data**: Traceability and clear identification of data sources are a precondition for real control of data in the market. The definition of reliable and possibly standardised protocols for persistent identification of data sources can be necessary to create trust in the system. 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. This could include making data available in machine-readable formats and the provision of associated meta-data.

- **Default contract rules**: Default rules could describe a benchmark balanced solution for contracts relating to data, taking due account also of the ongoing Fitness Check on the overall functioning of the Unfair Contract Terms Directive. They could be coupled with introducing an unfairness control in B2B contractual relationships[27] which would result in invalidating contractual clauses that deviate excessively from the default rules. They could also be complemented by a set of recommended standard contract terms designed by stakeholders. This approach could lower legal barriers for small businesses and reduce the imbalance in bargaining positions, while still allowing a large degree of contractual freedom.

- **Access for public interest and scientific purposes**: Public authorities could be granted access to data where this would be in the "general interest" and would considerably improve the functioning of the public sector, for example, access for statistical offices to business data, or the optimisation of traffic management systems on the basis of real-time data from private vehicles. Access to business data by statistical authorities would typically contribute to alleviating the

[27]. Obviously the benchmark for the unfairness level for B2B would need to be different from B2C contracts, as to reflect the higher degree of contractual freedom in B2B relationships.

statistical reporting burden on economic operators. Similarly, access to and the ability to combine data from different sources is critical for scientific research in fields such as medical, social and environmental sciences.

- **Data producer's right**: A right to use and authorise the use of non-personal data could be granted to the "data producer", i.e. the owner or long-term user (i.e. the lessee) of the device. This approach would aim at clarifying the legal situation and giving more choice to the data producer, by opening up the possibility for users to utilise their data and thereby contribute to unlocking machine-generated data. However, the relevant exceptions would need to be clearly specified, in particular the provision of non-exclusive access to the data by the manufacturer or by public authorities, for example for traffic management or environmental reasons. Where personal data are concerned, the individual will retain his right to withdraw his consent at any time after authorising the use. Personal data would need to be rendered anonymous in such a manner that the individual is not or no longer identifiable, before its further use may be authorised by the other party. Indeed, the GDPR continues to apply to any personal data (whether machine generated or otherwise) until that data has been anonymised.

- **Access against remuneration**: A framework potentially based on certain key principles, such as fair, reasonable and non-discriminatory (FRAND) terms, could be developed for data holders, such as manufacturers, service providers or other parties, to provide access to the data they hold against remuneration after anonymisation. Relevant legitimate interests, as well as the need to protect trade secrets, would need to be taken into account. The consideration of different access regimes for different sectors and/or business models could also be envisaged in order to take into account the specificities of each industry. For instance, in some cases, open access to data (full or partial) could be the preferred choice both for firms and for society.

The Commission will consult stakeholders on the issues outlined above, with a view to gathering more evidence on the functioning of the data markets by sector and exploring possible solutions. In this context, a broad macro-level discussion is essential for debating possible solutions and avoiding unintended side-effects that would stifle innovation or hinder competition. In addition, sector-specific discussions will be held with relevant stakeholders in the data value chain.

4. LIABILITY

Another emerging issue concerns the application of the current rules on liability in the data economy in relation to products and services based on emerging technologies such as the Internet of Things (IoT), the factories of the future and autonomous connected systems. IoT is a rapidly growing network of everyday objects, such as watches, vehicles, and thermostats, which are connected to the Internet. Autonomous connected systems, such as self-driving vehicles, act independently of humans and are capable of understanding and interpreting their environments. These emerging technologies use sensors to provide the many types of data that are often required for the product or service to function.

All these innovations are likely to contribute to more safety and quality of life, but inevitably there remains the possibility of design errors, malfunctioning or manipulation in every device. This could result from the transmission of erroneous data by a sensor, due to, for instance, software defects, connectivity problems or incorrect operation of the machine. The nature of these systems means that it may be difficult to establish the exact source of a problem that leads to damages, raising the issue of how to ensure that these systems are safe for the users, in order to minimise the occurrence of damage and who should be held liable for damage if it occurs.

The issue of how to provide certainty to both users and manufacturers of such devices in relation to their potential liability is therefore of central importance to the emergence of a data economy.

4.1. EU rules on liability

Civil law generally distinguishes two types of legal liability: contractual, where the liability for the damage stems from the contractual relationship between the parties; and extra-contractual[28], where the liabilities are set outside of a contract. An important type of extra-contractual liability is the one concerning the liability for defective products. At EU level, the Directive on liability for defective products (85/374/CEE) ("Products Liability Directive") establishes the principle of strict liability, i.e. liability without fault: where a defective product causes damage to a consumer, the manufacturers may be liable even without negligence or fault on their part. However, it may become difficult or unclear how to apply the provisions of this Directive[29] in the context of IoT and autonomous connected systems (e.g. robotics), for the following reasons: the characteristics of these systems, for example a complicated product or service value chain, with interdependencies between suppliers, manufacturers and other third parties; uncertainty in relation to the legal nature of IoT devices, i.e. whether they are products, services, or products that come with the sale of a service; and the autonomous nature of these technologies.

The Commission has launched a broad evaluation of the Products Liability Directive, to assess its overall functioning and whether its rules, developed for a very different environment, remain appropriate for emerging technologies such as IoT and autonomous connected systems.

4.2. Possible ways forward

The Commission's objective is to enhance legal certainty with regard to liability in the context of emerging technologies and thereby create favourable conditions for innovation. Besides the status quo[30], various approaches could be explored, including:

---

[28] EU liability rules only relate to extra-contractual liabilities.

[29] References to the strict liability of producers in case of defective products are made in other pieces of legislation on safety of products, for instance the Radio Equipment Directive (2014/53/EU), the Medical Devices Regulations, the Machinery Directive (2006/42/EC) and the General Product Safety Directive (2001/95/EC).

[30] The Commission could issue guidance on the application of the EU rules on liability to IoT and robotics.

- **Risk-generating or risk-management approaches**: Under these approaches liability could be assigned to the market players generating a major risk for others or to those market players which are best placed to minimise or avoid the realisation of such risk.

- **Voluntary or mandatory insurance schemes**: Such schemes could be coupled with the above-mentioned liability approaches. They would compensate the parties who suffered the damage (e.g. the consumer). This approach would need to provide legal protection to investments made by business while reassuring victims regarding fair compensation or appropriate insurance in case of damage.

Any approach would need to take into account the actions of the individual using the technology, and more precisely identify what should be the role of the users of that technology.

The Commission will consult stakeholders on the adequacy of current EU rules on liability in the context of IoT and autonomous connected systems, as well as on possible approaches to overcome the current difficulties in assigning liability. A parallel public consultation on the overall evaluation of the application of the Products Liability Directive is also being conducted. The Commission will assess the results and consider options for future action.

5. PORTABILITY, INTEROPERABILITY AND STANDARDS

Other emerging issues in the data economy are the portability of non-personal data, the interoperability of services to allow data exchange, and appropriate technical standards for implementing meaningful portability.

5.1. Portability of non-personal data

Data portability means that consumers and businesses can easily take their data from one system to another. It is generally associated with low switching costs, and hence with low entry barriers, in the data economy. The GDPR will give individuals a right to receive the personal data provided to the service provider, in a structured, commonly used machine-readable format, and the right to transmit it to another provider[31].

However, regarding non-personal data, there are at present no obligations to guarantee even a minimum level of data portability, even for widely used online services such as cloud hosting providers. This is partly because the requirements for implementing data portability can be technically demanding and costly, as different providers of the same services may store data differently.

Meaningful portability for non-personal data would also need to take into account broader data governance considerations involving transparency for users, managed access and interoperability to link different platforms together in ways that stimulate innovation.

[31] Article 20.

5.2. Interoperability

Frequently, data portability considerations are closely related to questions of data interoperability, which enables multiple digital services to exchange data seamlessly, facilitated by appropriate technical specifications. The Public Sector Information Directive and associated guidance (including the European Interoperability Framework) emphasise the importance of rich, standardised meta-data following established vocabularies to facilitate searching and interoperability. The Infrastructure for Spatial Information in the European Community (INSPIRE) Directive and its interoperability regulations and guidance for spatial data services and data, including sensor observation data, currently apply to public sector spatial data[32].

In the case of online platforms, such data interoperability facilitates not only switching, but also the concurrent use of several platforms (so-called "multi-homing") as well as widespread cross-platform data exchange, which has the potential to enhance innovation in the digital economy.

5.3. Standards

Effective portability policies must be supported by appropriate technical standards in order to implement meaningful portability in a technologically neutral manner. The Commission has committed itself[33] to support the appropriate standards to improve interoperability, portability and security of cloud services, by better integrating the work of open source communities into the standard-setting process at European level. Examples of such an approach are the TOSCA specification for cloud applications, aiming to enhance the portability and operational management of cloud applications and services[34], and the technical specifications and guidelines of the INSPIRE implementing regulations[35].

5.4. Possible ways forward

Possible ways forward to address the above issues include:

- **Developing recommended contract terms to facilitate switching of service providers**: As data portability and switching of data service providers are mutually dependent, the development of standard contract terms requiring the service provider to implement the portability of a customer's data could be examined.

- **Developing further rights to data portability**: Building on the data portability right provided by the GDPR and on the proposed rules on contract for the supply

[32] Machine generated data are 'spatial data' as sensors usually also transmit their direct or indirection position (location) together with their measurement.

[33] COM(2016) 176 final: ICT Standardisation Priorities for the Digital Single Market

[34] https://www.oasis-open.org/committees/tosca

[35] INSPIRE legislation: http://inspire.ec.europa.eu/inspire-legislation/26

of digital content, further rights to portability of non-personal data could be introduced, in particular to cover B2B contexts, whilst taking due account of the outcome of the ongoing Fitness Check on key pieces of EU marketing and consumer law[36].

- **Sector-specific experiments on standards**: To develop a robust approach to portability rules encoded through standards, sector-specific experimental approaches could be launched. These would typically involve a multi-stakeholder collaboration including standard setters, industry, the technical community, and public authorities.

The Commission will consult stakeholders on these issues and will determine on that basis whether further action is required, possibly in the form of the above actions, either individually or in combination.

6. EXPERIMENTATION AND TESTING

Experimentation is an important part of the exploration of emerging issues in the data economy. The potential to use Horizon 2020 funding to support these kinds of trials and experiments will be explored.

Before reaching conclusions on the suitability of possible solutions for data access and liability, a dedicated trial should be organised for testing these issues in a real-life environment, in partnership with stakeholders. A European solution, built on cooperation and experimentation among Member States, is needed.

Cooperative, connected and automated mobility[37] could be considered for such a trial, given the cross-border dimension of this sector.

Projects are already underway in several Member States to develop cooperative systems and higher levels of automation [38]. These projects enable vehicles to connect with each other and with roadside infrastructure such as traffic lights and road signs. Moreover, the Commission intends to work with a group of interested Member States to create a legal testing framework for conducting experiments on the basis of harmonised rules on data access and liability. To allow for access to a sufficiently high volume of data, the trials should be based on 5G, operating in seamless co-existence with technologies already being deployed and under a complementarity principle[39].

Another interesting experimentation will come from the geo-spatial sector, with the emergence of a new data eco-system built around Copernicus, the EU earth observation programme and third largest data provider in the world. Innovative solutions are being developed by the Commission to foster the development of applications based on

[36] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

[37] See COM (2016) 766 of 30.11.2016.

[38] See COM (2016) 766: A European strategy on Cooperative Intelligent Transport Systems

[39] See COM (2016) 588: 5G for Europe: An Action Plan

Copernicus and other spatial data, notably addressing issues of data access, interoperability and predictability.

7. CONCLUSION

To build the data economy, the EU needs a policy framework that enables data to be used throughout the value chain for scientific, societal and industrial purposes. To this end, the Commission is launching a wide-ranging stakeholder dialogue on the issues explored in this Communication. The first step in this dialogue will be a public consultation. The issues of data access and liability will also be tested in a real-life environment in the field of cooperative, connected and automated mobility.

Concerning the free flow of data, the Commission will continue to work on this issue in line with the approach outlined above, to fully implement the principle of the free flow of data within the EU, including where needed and appropriate through prioritised enforcement action. The Commission will also continue to monitor and gather evidence and, if necessary, may consider taking further initiatives on the free flow of data.

Based on the results of the stakeholder dialogue, the Commission will also decide whether further action is required on the emerging issues and propose solutions accordingly. In this context, experimentation in real life conditions might play a role.