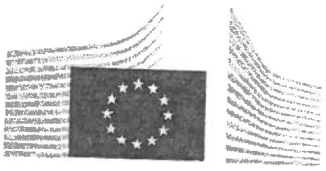

EUROPEAN
COMMISSION

Brussels, XXX
[…](2016) XXX draft

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"

"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, 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 data holders, researchers and infrastructure providers – collaborating to ensure that data is accessible and usable. This enables the market players to extract value from this data, such as by creating applications for traffic management or for optimising harvesting.

The value of the EU data economy was over EUR 257 billion in 2014, over 1.85% of the 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.

In April 2016 the General Data Protection Regulation was adopted. It modernises the principles of the 1995 Data Protection Directive, tailoring them for the digital age and harmonising the data protection law in Europe. The new Regulation is a key enabler for the Digital Single Market, economic growth, job creation, innovation and scientific progress in Europe. Strong data protection rules are necessary to rebuild the trust of individuals in how their personal data is being used. The Regulation will apply from 25 May 2018 and its effective implementation is key.

In its 2014 Communication "Towards a thriving data-driven economy", the Commission recognised 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 may contribute to insufficient access to large datasets, the possibility of 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

---

[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

by public authorities (i.e. not by private entities) 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 a mixture of personal and non-personal data, machine generated or created by individuals, and data flows and datasets regularly combine these different types of data. In the Digital Single Market (DSM) strategy, the Commission announced that it would propose an initiative that tackles 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 both legal acts adopted by Member States, as well as administrative rules and practices having the same effect. Their number tends to expand with the growth of the data economy[3], and this trend is generating uncertainty as to where data can be stored or processed. This has an impact across all sectors of the economy and on both businesses and public sector organisations, which could be deprived of a possibility to use more innovative and/or cheaper data services. Unjustified data location restrictions impair the Treaty freedom to provide services and the freedom of establishment, 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.

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. The enormous diversity of data sources and types, and the rich opportunities for applying insights into this data in a variety of domains are only beginning to emerge. To exploit these opportunities, players in the data market need to have access to large and diverse datasets. The issues of ownership, access and transfer 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 particular, the regulatory framework on liability might still work for the type of technology which is always controlled and managed by human beings. However, in the context of new technologies such as the Internet of Things (IoT) or robotics we face complex and sophisticated interdependencies between the product and the software layers, and respectively problems for unintended consequences of autonomous behaviours of robots that may put to the test our traditional liability reasoning and rules.

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. To this end, the Commission is presenting focussed issues for discussion with a view to "Building a European data economy".

Accordingly, this Communication, which is accompanied by a Staff Working Document (SWD), explores the issues of free flow of data; access and transfer in relation to data; liability and safety in the context of emerging technologies; and portability,

[3] See the accompanying Staff Working Document

interoperability and standards. It also sets out suggestions for experimenting with these regulatory issues 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 will be a public consultation.

2. FREE FLOW OF DATA

A well-functioning and dynamic data economy requires that the flow of data in the internal market is enabled and protected. The free flow of data contributes to making sure the four freedoms are protected in a data economy context. Data services are a growth sector for the European economy. If the Single Market in this sector is made a reality, the additional opportunities for growth and jobs will be significant.

The General Data Protection Regulation (GDPR) provides for a harmonised and high level of protection of personal data and is the foundation for the free flow of data in the EU. However, non-personal data remain outside the scope of GDPR. Furthermore, the GDPR bans restrictions to the free movement of personal data but only where these are motivated by the protection of personal data. Restrictions motivated by other reasons than the protection of personal data, e.g. under taxation or accounting laws, are not covered by the GDPR.

This dynamic growth and the innovation the data economy can bring are jeopardised by barriers to the free movement of data in the EU, such as unjustified data localisation requirements imposed by public authorities (i.e. not by private entities). These requirements can apply to all types of data, whether personal or non-personal. According to the OECD, data localisation measures reintroduce digital 'border controls'. These 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.

Data location restrictions are legal rules or administrative guidelines or practices that limit the storage or processing of data in electronic format to a particular geographical area or jurisdiction. They are imposed by Member States sometimes in the belief that supervisory authorities can more easily scrutinise data that is stored locally. Localisation is also used as a proxy for assurances in terms of privacy, audit and law enforcement. But paradoxically, these measures rarely contribute positively to the objectives they are intended to achieve.

Indeed, information security depends on a range of factors besides where the data is physically stored, such as maintaining its confidentiality and integrity at locations where 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. There is a misconception that localised services are automatically safer than cross-border services. For example, to avoid impact 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 in line with the Directive on Security of Network and Information Systems (the NIS Directive). Also, the availability of data for regulatory or supervisory purposes would be better ensured through enhancing

the cooperation between national authorities, or between such authorities and the private sector, and not by its localisation.

Unfortunately, the trend, both globally and in Europe, is towards more data localisation[4]. Moreover, the data services market is substantially influenced by lack of transparency and a strong perception of the need to localise data. This may deprive businesses and public sector organisations of the possibility to use cheaper or more innovative data services or force businesses operating cross-border to arrange excess data storage and processing capabilities. This could also inhibit businesses, in particular start-ups and SMEs, from scaling-up their activities, entering new markets 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 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[5].

More generally, wider adoption of the cloud and more efficient use of companies' own IT resources would contribute to the reduction of energy consumption and carbon emissions by a net 30 percent or more. A small business moving to the cloud could reduce its energy consumption and carbon emissions by more than 90 percent, by running its business applications in the cloud instead of running those same applications on its own infrastructure. The global green data centre market is expected to grow to almost €90 billion by the end of 2020. A fragmented data services market would hinder the full development of these services in the EU and also put at risk 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 establishment provisions of the Treaty. 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 use proportionate means to achieve an overriding objective in the general interest, such as the need to safeguard public security[6].

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

4 [Globally: +150% since 2006; in Europe: +100% since 2006: see Staff Working Document]

5 "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

6 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 the data location restrictions at a draft stage, Directive 2015/1535 (the Transparency Directive).

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 take appropriate follow-up actions that in addition to a horizontal initiative on the free flow of data, may include the launch of enforcement actions to address unjustified or disproportionate data location measures. In this context, any follow-up action will be done in line with Better Regulation principles.

3. DATA ACCESS AND TRANSFER

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. 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 to create an application for traffic management. 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 (i.e. non-processed) data generated by these machines or processes are therefore central to the emergence of a data economy and require careful assessment.

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 is personal, the rules of the GDPR apply, including the rights of individuals, obligations on data controllers and principles on how and on what basis personal data can be used.

The bulk of machine-generated data are not personal data. However, where machine generated data allow the identification of a person, they qualify as personal data with the consequence that, the GDPR applies until that data has been anonymised (e.g. location data of a satellite navigation system).

One common theme linking the free flow of data issue with the emerging issues of access and ownership is that enterprises and actors in the data economy will be dealing with a mixture of personal and non-personal data, and that data flows and datasets will regularly combine both types. Any policy measure must take account of this economic reality.

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[7] 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 exploit or allow for the possibility of user-friendly Application Programming Interfaces (APIs)[8] (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.

Therefore, exchange of data currently remains limited. Data market places are slowly emerging, but are not widely used, as 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. Legal situation at EU and national level

At EU level, the new GDPR provides a comprehensive legal framework for personal data. It contains the principles and the different grounds for the lawful processing of personal data, thereby offering a protection against the unauthorised and/or unlawful processing of personal data.

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 the contents in the database. The recently adopted Trade Secrets Protection Directive, to be transposed into national law by June 2018, will grant protection to trade secrets against their unlawful acquisition, use and disclosure. However, for data to qualify as a "trade secret", efforts have to be made to protect the secrecy of information, which represents the 'intellectual capital of the company".

Under the laws 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

---

[7] 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

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

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 EU level in relation to machine-generated data or the conditions of 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 EU might be a sufficient response to the problem. In addition, voluntary or umbrella agreements covering certain sectors might be envisaged. Nevertheless, the negotiation power of the different market participants might be so unequal, that market based solutions alone might not sufficiently ensure fair and innovation-friendly results, easy access for new market entrants and avoid lock-in situations.

3.4. "De facto" ownership

In some cases manufacturers may become the de facto "owners" of the data that their machines or processes generate, even if those machines are owned by the user. The de facto control of this data can be a source of differentiation and competitive advantage for manufacturers. However, at the same time the user is prevented from licencing usage of the data to another party or trading it on a data market place. In other cases, actors in the value chain other than the manufacturer may enjoy a de facto possession of and control over the data, because they have a stronger bargaining position with respect to other players.

The different market players that are in control of the data, depending on the specificities of the markets, may thus take advantage of the absence of a regulatory framework or of the legal uncertainties described above by imposing standard contract terms on the users or through technical means, such as proprietary formats or encryption. This could for instance result in users 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 because of their unequal negotiation position or the significant costs of hiring legal expertise.

As further explained in the SWD, the issue of access to machine-generated data is under consideration in several sectors, such as transport (connected vehicles); energy markets; smart living environments; the health and care sector; and financial technology.

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 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 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:

- **Enable the trading of machine-generated data**: Through sharing, reuse and aggregation, machine-generated data becomes a source of value creation, innovation and diversity of business models.

- **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.

- **Avoid disclosure of sensitive and confidential data**: Any future solution should mitigate the risks of disclosing confidential data, in particular to existing or potential competitors.

- **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 data access, 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 data control rights should be addressed in contracts. This guidance would be based on existing legislation, in particular the Trade Secrets Directive, copyright legislation and the Database Directive. The Commission intends to launch a review of the Database Directive in 2017.

- **Fostering the development of Application Programming Interfaces (APIs):** APIs have become a prime tool for creating an ecosystem of developers around data held by a company, helping companies to have their data re-used in as many instances as possible. This also helps actors to identify, and profit from, different types of re-uses of data they hold. The companies, or public authorities, that do not work proactively with APIs will risk lagging behind in terms of less innovative solutions and/or additional data development. On this basis, broader use of open, well-documented APIs could be considered, through technical guidance, including identification and spreading of best practice for companies and public sector bodies making good use of developer-friendly APIs.

- **Default contract rules**: These default rules which could be deviated from by contract would describe a benchmark balanced solution for contracts relating to data. They could be coupled with introducing an unfairness control in B2B contractual relationships[9] which would result in invalidating contractual clauses

[9]. 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.

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 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 (as proposed in the French "Loi Numérique") or the optimisation of traffic management systems on the basis of real-time data from private vehicles.

- **Data producer's right**: A right to use and licence the use of 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 clarify the legal situation and give more choice to the data producer by opening up the possibility for users to exploit 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, it would also need to be fully aligned to the EU legislative framework on data protection, in particular the GDPR. As stated above, the GDPR continues to apply to any machine-generated data qualifying as personal data 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. Relevant legitimate interests, as well as the need to protect trade secrets, would need to be taken into account.

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 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 factory of the future and autonomous connected systems. IoT is a rapidly growing network of everyday objects, such as eyeglasses, cars, and thermostats, which are connected to the Internet. Autonomous connected systems, such as self-driving cars, 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, questions 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

In general, there are two types of legal liability: contractual, where the liability for the damage stems from the contractual relationship between the parties; and extra-contractual, 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 Products Liability Directive (85/374/CEE) 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. It is however only addressed to the producer, requires still the existence of a defect and that the causality between defect and damage has to be proven. These features may make it difficult to apply it to the issues of emerging technologies.

The Commission has launched a broad evaluation of the Defective 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 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. Beside the status quo, various approaches could be explored, including:

- **Risk-generating or risk-management approaches**: Under these approaches, liability would be assigned to the market players generating a major risk for others and benefitting from the relevant device, product or service or to those which are best placed to minimise or avoid the realisation of the 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. 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.

The Commission will consult stakeholders on the adequacy of current rules on liability in the context of IoT and autonomous 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 Product 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 portability in relation to personal data, allowing the consumer to avoid "losing" all data recorded and stored at one provider when leaving that provider for another company.

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.

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.

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 to implement meaningful portability in a technologically neutral manner. The Commission

has committed itself[10] to support the appropriate standards to improve interoperability and portability of cloud services, by better integrating the work of open source communities into the standard setting process at European level. An example of such an approach is the so-called TOSCA specification for cloud applications, aiming to enhance the portability and operational management of cloud applications and services[11].

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 of digital content, further rights to portability of non-personal data could be introduced, in particular to cover B2B contexts.

- **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. 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.

Connected and autonomous driving (CAD) is ideal for such a trial, given its cross-border dimension. Projects are already underway in several Member States to develop "intelligent corridors" for CAD[12]. These corridors are test environments that enable autonomous vehicles to connect with each other and with roadside infrastructure such as traffic lights and road signs.

---

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

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

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

The Commission is currently developing with Member States and stakeholders a multilateral approach for consistent CAD deployment across Europe, with 5G as a central element. In this context, the Commission intends to work with a group of interested Member States to create a legal testing framework for conducting their CAD experiments on the basis of harmonised rules on data access and liability. A European solution, built on cooperation and experimentation among Member States, is needed for CAD and for other connected devices.

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 CAD.

Concerning the free flow of data, the Commission will continue to work on this issue in line with the step-by-step approach outlined above to fully implement the principle of the free flow of data within the EU, including through further enforcement action. The Commission will also continue to monitor and gather evidence and, if necessary, may consider taking a horizontal initiative on the free flow of data.

Based on the results of the stakeholder dialogue and the experimentation framework, the Commission will also decide whether further action is required on the emerging issues and propose solutions accordingly.