EU2017.EE

Estonian Vision Paper on the Free Movement of Data – the Fifth Freedom of the European Union

Estonian Vision Paper on the Free Movement of Data – the Fifth Freedom of the European Union

Europe has been starting place for many innovative concepts, and we should continue the conceptual framing of future enablers for a better understanding of **the future of Europe** and the endless possibilities lying ahead of us. Making good use of technology has been and will be the key to success for Europe. At **the era of artificial intelligence and gigabit society**, we have to re-think some of the concepts dating back decades or even centuries. We are on the **brink of digital society**, and we should be like a visionary architect who designs the environment in a way which helps the habitats to flourish not to crumble. **Therefore the free movement of data is a concept to work on together** and to understand the freedoms and enabling features it gives us if put to good use.

Data[1] as an enabler for new business models, jobs and innovation is not merely a by-product of the free movement of goods, capital, services and people. It is both an enabler for these four freedoms, but it could be argued that is also a right in itself as data is neither a person, a physical good, capital nor a service, but to help them move, data must also be able to cross borders[2]. Therefore, **data should be treated as a separate freedom of the EU together with the existing four freedoms of the internal market set out in the Treaty on the Functioning of the European Union** ("TFEU"). As described in this concept paper, the free movement of data[3] is a future-looking long-term goal. This does not mean that we endeavour to open the Treaties. Here, we speak about the need for a debate whether such a freedom would be feasible and only then analyse practical steps for achieving the "fifth freedom".

Data is the basis for information, knowledge and wisdom[4]. Data is often compared to resources like oil or gold[5]. However, data should not be treated as a consumable resource; rather, it should be treated as infrastructure and a non-rivalrous capital good that can be used across society for a theoretically unlimited range of productive purposes, without being depleted[6]. Thus, unlike other assets, data has a different nature and trying to fit it under the known notions of "a service" or "a good" is often difficult if not impossible. Furthermore, data and its value have highly contextual meaning. However, it is undisputable that data is the input for other goods and services – data is the means rather than the ends[7]. **Therefore, we should find ways to promote the secure exchange of data across silos and borders to benefit the society at large**, not try to make it into a scarce resource. For this, we need robust and unambiguous rules and policies (and interpretations thereof) regarding access and (re)use of data to provide legal clarity and create trust among the industry and consumers alike.

This requires a wider debate on data and fostering such constructive debate is not a simple task. Many initiatives already exist (see below) and overregulating a dynamic and growing fields related to data may have a chilling effect on innovation in the long run[8]. This would run counter to what **the free movement of data aims to achieve – to make Europe the place where (digital) innovation happens first**.

[1] "Data" in the context of this position paper denotes both personal and non-personal data.

[2] Address of President Toomas Hendrik Ilves at the European Parliament, February 2, 2016. Accessible: https://vp2006-2016.president.ee/en/official-duties/speeches/11972-address-of-president-toomas-hendrik-ilves-at-the-european-parliament-february-2-2016/index.html.

[3] "Free movement of data" in the context of this paper denotes the situation opposite the current situation where data remains is „silos". This means that there are no border controls inside the digital single market for neither personal nor non-personal data. It also means that public authorities make the data they collect available to other public authorities where applicable and exchange it on the basis of the "once-only" principle and private entities in some situations share the data with the general public and with their consumers to increase competition and consumer choice.

[4] See https://www.i-scoop.eu/big-data-action-value-context/dikw-model/.

[5] Roundtable on Online Data Collection, Targeting and Profiling, 31.03.2009, speech by Commissioner Kuneva. Accessible: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.
The world's most valuable resource is no longer oil, but data. Economist (06.05.17). Accessible: http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource.

[6] OECD, Data-Driven Innovation. Accessible: http://www.oecd.org/sti/ieconomy/data-driven-innovation.htm, p 39

[7] Ibid, p 180.

[8] Graef, Inge and Husovec, Martin, Response to the Public Consultation on 'Building a European Data Economy', p 3, April 25, 2017. Accessible: https://ssrn.com/abstract=2958287.

Distinguishing data as an asset in the context of free movement of data takes into account both personal[9] and non-personal data[10]. In practice, it is difficult to draw the line between the two as datasets often involve a mix of both personal and non-personal data[11]. In order to achieve a functioning single market and a data economy where innovation and data-dependent technologies thrive, we need a functioning system of data access, (re)use and portability for all types of data to unlock it from silos so it could be used in decision-making processes by the governments, process optimisation or new product offerings for companies and better decision-making for consumers and SMEs. Unlocking data is also important for greater efficiency and cost-savings.

In order to promote the free movement of data, the **EU should focus on three main areas: a) removal of any unjustified data localisation requirements to non-personal data; b) promote the cross-border exchange of public administration data on the basis of the once-only principle[12]; and c) enabling access and portability of both personal data and raw machine-generated data for the benefit of competition and innovation**. These different policy measures cannot be hierarchized as the focus of these measures and potential solutions do not have common denominators considering that challenges related to data exchanges and access to public data are different from issues related to access in the private sector. For example, data access initiatives thus far have been more related to the public sector (open data initiative[13]). Additionally, the measures encompass different types of data – while the

[9] 'Personal data' is defined in article 4(1) of the Regulation 2016/679/EU (the GDPR). According to the definition, it is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

[10] 'Non-personal data' has no legal definition. The definition could be derived from the definition of 'personal data' – any information that does not relate to an identified and identifiable natural person.

[11] Graef, Husovec, p 4.

[12] The principle of once-only "ensures that citizens and businesses supply certain standard information
only once, because public administration offices take action to internally share this data, so
that no additional burden falls on citizens and businesses". Study on eGovernment and the Reduction of Administrative Burden. Accessible: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5155.

first and the third pillar mostly focus on non-personal data, the utilisation of the once-only principle also covers personal data besides non-personal data (see page 3).

The potential value of the EU data market by 2020 may vary from € 361 billion (2.3% of the EU GDP) to € 739 billion EUR (4% of the EU GDP) depending on the way we tackle the challenges related to data in the upcoming years[14].

Many aspects for enabling these changes are already in place. However, the discussions around data often stumble upon the data protection complexities. Furthermore, the problems and solutions are difficult to quantify, as digital matters have brought and continue to bring along a lot of disruption in the society. Therefore, a **new approach to data use fit for the digital era is required**. The three pillars proposed and described below are framed by key legislative initiatives of the Digital single market strategy, including the e-commerce package, the European Communications Code and developments in cyber security (e.g. implementation of the security of network and information systems directive (NIS[15])). These form the foundation for trust without which the free movement of data will not function. These enablers will not, however, be the subject of this concept paper.

[13] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.

[14] The Power of Data for European Growth, IDC. Accessible: http://www.dataland-scape.eu/data-driven-stories-news-stud-ies/ european-data-market-study-final-mon-itoring-tools%E2%80%99-results-soon-be.

[15] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri =uriserv:OJ.L_.2016.194.01.001.01.ENG&toc=OJ:L:2016:194:TOC

Free Movement of Data as the high-level political goal (the fifth EU freedom) to promote data exchange between governments and its agencies for better decision-making, efficient supervision and transparency in the public sector and providing legal clarity on the use and re-use of non-personal data and in the private sector

Trust framework

- security of network and information systems[16],
- high-speed and secure electronic communications,
- regulation on electronic identification
- and trust services for electronic transactions in the internal market ("eIDAS regulation")[17],
- the general data protection regulation ("GDPR")[18].

[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.

[17] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[18] 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 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

Removal of unjustified data location restrictions for non-personal data to benefit both the public and private sectors

Problem description

Data localisation stems from legal rules, administrative guidelines or practices that dictate and influence the localisation of non-personal data for its storage and/or processing[19]. Such localisation rules force companies to store documents and data in separate silos and even in several jurisdictions which is costly and hinders cross-border business.

What should fall under the category of "justified" data location restrictions? The categories of data that should fall under the category of justified cases where data location measures should be reasonable would fall under the need to guarantee national security and public order. However, for legal clarity, these categories cannot be too ambiguous and should be interpreted restrictively.

Instead of forcing localisation, the norm should be functional – not stating that some data or document specifically needs to be stored in

[19] SWD (2017) 2 final, page 5. Accessible: http://ec.europa.eu/digital-single-market/news-redirect/52044.

[20] Ibid.

[21] Ibid.

[22] For more information, see http://e-resident.gov.ee/.

[23] T.Kotka, I.Liiv. Concept of Estonian Government Cloud and Data Embassies, p 151. Accessible: http://innar.com/personal_copy_Estonian_Government_Cloud_Kotka_Liiv_2015.PDF.

[24] See Bauer, M et al. Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, p 4. Accessible: http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf. See also OECD Working Party on the Trade Committee document Localising Data in a Globalised World, p 26.

[25] OECD Working Party on the Trade Committee document Localising Data in a Globalised World, p 18-19.

some Member State due to supervisory purposes, but outline that access to data for supervision needs to be guaranteed. It should not matter where the data is stored within the single market, as long as adequate safeguards in regard to confidentiality, integrity and availability (i.e. the pillars of information security) are in place.

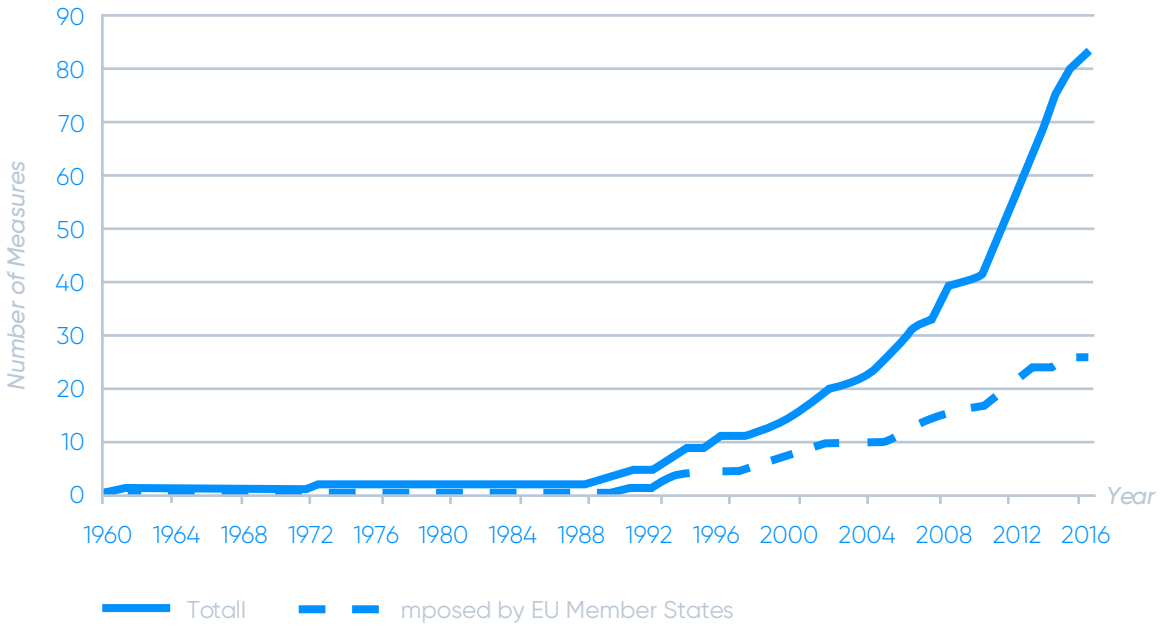
There is an Estonian start-up that is providing a platform for managing application process for universities. Although their platform is used by 150 universities in Europe, they have met obstacles because of data localisation restrictions in some Member States. The problem is that some member states require them to keep the admission documents (both personal and non-personal information) in the same country as the university is, not in a cloud like the modern systems would.

The Commission's analysis of a sample of 50 data localisation restrictions in 21 Member States shows that the highest share of data localisation restrictions applies across sectors and, in many cases, to privately-held data: e.g. accounting documents and tax records, invoices or company records and registers. Current laws require the localisation of, e.g. invoices, books and records, accounting documents, commercial letters on servers within the country with less restrictive legal provisions; and with more restrictive provisions even the placement of such documents on the very premises of the company[20].

Government and public sector data are also concerned by restrictions – e.g. judicial records and other public records, national registries, and national archives[21].

To enable cloud in the public sector, Estonia has launched the government cloud and data embassies project ("EE Government Cloud concept") to: a) eliminate server farm fragmentation and ensure high-quality cost-effective service provision by the government; b) ensure the certified IT security level and support for the creation of new e-services and innovation; c) ensure Estonia's digital continuity and the functioning of the state in any situation or emergency regardless of any interruptions; and d) ensure the reliability and quality of cross-border services (for example, due to the launch of the e-Residency programme[22]). As a result of the EE Government Cloud concept, the public sector will develop a private cloud infrastructure to ensure high-quality and cost-effective service provision, embrace the use of the public cloud for certain databases and information systems and conclude international agreements to host some of the most critical databases in secure locations abroad (data embassies) for digital continuity reasons[23].

Studies outline that the trend indicates that restrictions like the ones mentioned above are on the rise both globally and inside the EU[24]. It is argued that the main reasons for creating digital "border controls" are: a) to protect the privacy of data subjects; b) security (keeping data out of reach for foreign surveillance); and c) legal jurisdiction (e.g. tackling fraud)[25].



Potential benefits of removing unjustified data localisation requirements

The **aim of removing digital borders is enabling cross-border business**. Locating data and vital information systems of a company is a business decision driven by cost-efficiency, access to communications infrastructures and the location of customers. Also, laws and regulations set out where data and documents needs to be stored for supervisory purposes. Some time ago, it could indeed be argued that the best way to guarantee access to such documents was to have them located at the premises of the company, it was the best way to guarantee access to these documents. However, with the digital transformation, the Europe needs to look at how it can improve and remove restrictions where they have become obsolete. Thus, the aim of removing unjustified data localisation requirements is to cut this type of unnecessary bureaucracy via paper-era mechanisms.

Cloud computing[26] enables secure sharing of documents and data and guarantee the same result as in case of documents stored at the premises. Even though paper is still the norm in many sectors, creating an atmosphere where digital technologies can thrive is important as companies and governments are able to cut costs and be more effective at their work.

Data localisation is the measure for the 20th century, not in the 21st century.

[26] According to NIST, "cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,net- works, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. See The NIST Definition of Cloud Computing, p 2. Accessible: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nist specialpublication800- 145.pdf.

[27] According to NIST, "big data" refers to the inability of traditional data architectures to efficiently handle the new datasets. Characteristics of Big Data that force new architectures are: 1) Volume (i.e., the size of the dataset); 2) Variety (i.e., data from multiple repositories, domains, or types); 3) Velocity (i.e., rate of flow); and 4) Variability (i.e., the change in other characteristics). See NIST Big Data Interoperability Framework: Volume 1, Definitions, p 4. Accessible: http://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.1500-1.pdf.

[28] Measuring the economic impact of cloud computing in Europe, Deloitte. Accessible at: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

[29] Commission Communication on "Building a European data economy" (2017).

[30] M.Bauer et al., Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, p 1. Accessible: http://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/.

The idea is about **sending a signal that Europe is open for cross-border business, especially for data and digital economy companies**. Cross-border business should not be nuisance for European companies. Furthermore, clear rules on the storage of data and documents could also attract companies from non-EU countries to do business in the EU.

According to McKinsey, in 2014 alone, cross-border data flows generated $2.8 trillion in economic value exceeding the value of global trade in goods. Such growth reflects not just the dynamism of the technology industry, but also the digitisation of the economy as a whole.

Removing localisation requirements is a key element in unlocking the potential of the digital trade as the free flow of data will make the flow of goods and services easier, faster and cheaper. Furthermore, it is an enabler for emerging technologies such as cloud computing and big data[27].

According to Deloitte, policy initiatives aiming at promoting existing relevant certifications and standards and at removing data localisation restrictions would increase benefits for users and providers of cloud computing, as well as for society as a whole to a total of over EUR 19 billion between 2015 and 2020[28].

The removal of data localisation requirements, however, holds enormous potential in others fields as well, ranging from health, food security, climate and resource efficiency to energy, intelligent transport systems and smart cities, which Europe cannot afford to miss out on[29].

According to a study conducted by the European Centre for International Political Economy, the EU could benefit 8 billion euros per year (up to 0.06% of the GDP) if existing data localisation measures are removed[30].

Challenges regarding the removal of unjustified location measures imposed to non-personal data

Increasing trust among Member States. One of the key findings of the structured dialogues that the European Commission has been organising to discuss with Member States is the lack of mutual trust that is the root cause behind data location restrictions. Therefore, the main challenge is to increase trust among Member States.

New vs existing rules? Lack of clear analysis in terms of how existing laws (the TFEU[31], e-commerce directive[32], services directive[33], transparency directive[34] and data protection directive[35]/ the GDPR) fall short on tackling the problem via existing legal acts.

Bringing legal clarity regarding the scope. Another issues seems to be related to the definition of "non-personal data". Although the definition of non-personal data is the negative of "personal data" (data that is not related to an identifiable or identified person), it is still not clear to all Member States what is meant by this. Experts involved with the implementation of the GDPR argue strongly that the free flow of data initiative cannot limit the scope of "personal data" defined in the GDPR[36]. Yet, the industry demands clear rules and guidelines under which it could be understood what is "personal data" and what can be considered as "non-personal data".

Refuting false beliefs or protectionism. Some Member States argue against this initiative on the basis of the pretext that it would make the life of U.S cloud companies easier to control the data about Europeans[37].

[31] Treaty on the Functioning of the European Union. More specifically articles 49 (freedom of establishment) and 56 (free movement of services).

[32] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[33] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[34] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[35] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[36] Presentation made by DG JUST at the 2nd structured dialogue on the free flow of data on 30 March 2017.

[37] Top 5 cloud companies are from U.S origin. Together, they control 57% of the market. See https://www.tharawat-magazine.com/facts/top-5-largest-cloud -companies-world/#gs. 5DA8HGg.

Further actions

The fact that **unjustified data localisation needs effective tackling at the EU level** to enable cross-border business has been found in many studies, industry non-papers and in the letters of likeminded Member States[38]. **We very much support that this issue needs to be dealt with effectively**.

The potential further actions regarding tackling unjustified data localisation requirements can be twofold - whether to tackle the localisation requirements via a **separate legal act, or via commencing infringement procedures** on the basis of existing legal rules (TFEU[39], e-commerce directive[40], services directive[41], transparency directive[42] and data protection directive[43]/ the GDPR).

This is a matter of choosing the tool. However, a separate legal act would be a simpler, clearer and a less divisive solution. Infringement proceedings work best when there is a clear contradiction with the EU law. Although we see the horizontal legal act as the best solution to address the issue of unjustified data localisation requirements, we are ready to work on effective alternative solutions if such measure is supported with firm evidence.

[38] See Bauer, M et al. Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States. Accessible: http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf, Measuring the economic impact of cloud computing inEurope, Deloitte. Accessible: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184 ,
Joint Industry letter of 15 November 2016 by ACT, Application Developers Alliance, AmCham EU, BSA, CCIA Europe, COCIR, DIGITALEUROPE, EACA, eCommerce Europe, EDiMA, EMOTA, EPC, EuroISPA, FEDMA, FENCA, IAB Europe, ISFE, JBCE, TABC, and WFA. Likeminded letter of 2 December 2016 by 14 EU MS to the European Commission supporting the Free flow of data initiative. Estonian Association of Information Technology and Telecommunications position on the data economy (13.04.2017 nr 6.1-1/30).

[39] Treaty on the Functioning of the European Union. More specifically articles 49 (freedom of establishment) and 56 (free movement of services).

[40] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[41] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[42] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

With the Mid-Term Review on the implementation of the Digital Single Market Strategy, the Commission agrees that besides securing the free flow of personal data, we need to ensure trustworthy and effective **cross-border free flow of non-personal data**. The Mid-Term Review sets forth that for the better functioning of the Digital Single Market, the principle of free flow of data within the EU should be the guiding principle for both the Member States as well as the industry. Therefore, the Commission outlines that by Autumn 2017, they will prepare a legislative proposal on the EU free flow of data cooperation framework which takes into account the principle of principle of free flow of data within the EU, the principle of porting non-personal data, including when switching business services like cloud services as well as the principle of availability of certain data for regulatory control purposes also when that data is stored in another Member State.[44]

[44] Mid-Term Review on the implementation of the Digital Single Market Strategy, COM(2017)228 final, p 12. Accessible. http://ec.europa.eu/newsroom/document.cfm?doc_id=44527.

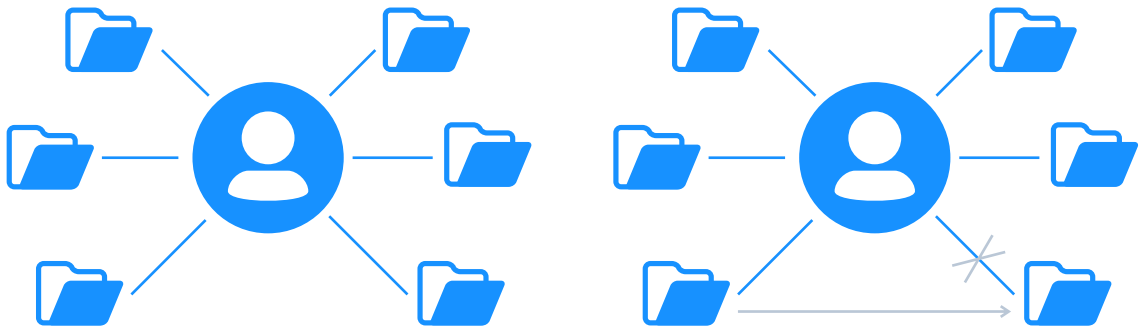
Cross-border exchange of data between public administrations based on the principle of "once-only"

Problem definition

Communication with the government is in many cases compulsory for both natural and legal persons (e.g. declaring taxes, requiring a permit to operate in a specific field, applying for a social benefit). In many cases, the government authorities already possess the data that they are requesting for making a required decision (for example, identifying whether a person or a company is eligible for the permit or benefit). However, this data may not be in the possession of the specific authority that needs to make the decision regarding the individual or a company. The public authority has two options:

a) it asks all the information required from the person (i.e. creating costs for the applicant and meaning that the same data is stored in multiple locations);

b) or it could re-use the data that is already in the possession of the government.



The second option can be greatly enabled by introduction and application of the principle of "once-only". This means that a company or a citizen supplies to the government any data only once and this data is then re-used within the government's base registries when adequate safeguards (e.g. for the protection of personal data via legally rooted "need-to-know" access rights or personal consent) have been applied.

The principle has been long in practice in Estonia, established in national legislation since 2007[45]. At the EU level, it is listed as one pf the fundamental principles in the eGovernment Action Plan 2016-2020. However, practical implementation is nowhere near as in case of Estonia – or some other Member States, too[46]. At the EU level, there is an ongoing H2020 Large Scale Pilot on the cross-border application of the once-only principle ("TOOP") which focuses on the exchange of non-personal data[47]. Within TOOP, there will be three pilot projects in different areas:(1) cross-border e-Services for business mobility, (2) updating connected company data and (3) online ship and crew certificates to connect 60 information systems from at least 20 countries[48]. The pilots are supported by an analysis of the legal landscape and the drivers and barriers that assist or impede the cross-border implementation of the once-only principle. Based on a cost-benefit analysis and an evaluation of the pilot results, TOOP will propose a generic framework to facilitate the future implementation and expansion of TOOP solutions to new countries and domains.

[45] On 25 February 2007, the amended version of the Public Information Act entered into force which included the chapter on base registries under which it was forbidden to establish separate base registries for the collection of the same data. Accessible: https://www.riigiteataja.ee/akt/12789344.

[46] For example, Estonia, Netherlands and Belgium have national legislation in place that not only refers explicitly to the Once-Only Principle but also enforces its implementation. See EU-wide digital Once-Only Principle for citizens and businesses. Policy options and their impacts, p 140. Accessible: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42300.

[47] This project started in January 2017 and will last for 30 months. The project's lead is Tallinn University of Technology.

[48] Press release from the kick-off meeting for the "Once-Only" Principle Project (TOOP). Accessible: http://toop.eu/assets/custom/docs/TOOP_PR.pdf.

Recently, the Commission tabled a proposal for a regulation for the Single Digital Gateway[49] which highlights the importance of the once-only principle for exchanging evidence (documents and data) between base registries.

A company from Member State Z wishes to start operating in Member State Y. For this, it requires a permit. The company has, however, submitted the data required for the permit already to the officials in Member State Z as the data required for this is the same. Nevertheless, the representative of the company is forced to supply the same data again. This may require travelling between Member States Z and Y, or reliance on middlemen with power of attorney which both add costs and inefficiency for business. To cut this type of bureaucracy, the norm should be that the company is not forced to supply the same data again, instead, the official of the requesting Member State Y should query the data from a database in the Member State Z. The process of applying the permit should be the same in the cross-border dimension and public authorities should work seamlessly in the back.

[49] Proposal for a Regulation of the European Parliament and of the Council on on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012 (COM(2017) 256 final). Accessible: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:256:FIN.

Potential benefits of the cross-border utilisation of the once-only principle

The once-only principle serves the end-users - citizens and businesses - who are, as a result, able to receive prompt, tailor-made and high quality digital services from public administrations, both in the originating country of the user and from other EU countries alike. The **aim is user-centricity**. As such, the once-only principle fundamentally changes the delivery of public services for the benefit of the user.

The need to securely exchange data across borders is on the rise. With the rise of the need, the volume of data increases as well. Thus, in order to prepare for the rise of volume of data that needs to be securely transferred between the Member States, **the EU as a whole needs to prepare itself by agreeing on the principles, rules and standards that form the basis of cross-border data exchange – and already in the near future**.

A good example of exiting framework enabling secure cross-border electronic transactions is the eIDAS regulations. eIDAS provides a regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. The regulation creates a toolbox that helps to enable the adoption of once-only principle among public authorities and businesses alike. As the aim of eIDAS is to ensure that people and businesses use their own national electronic identification schemes (eIDs) to access public services, a person is recognised and authenticated in the digital environment. Public administrations can exchange information as there is the level of assurance who the person is. What is more, the eIDAS Regulation creates internal market for electronic trust services - namely electronic signatures, electronic seals, time stamp and electronic delivery service. These services help to exchange the information across borders as there are same rules in Member States and electronic processes have the same legal status as traditional paper based processes.

Online public services are crucial for reducing business costs and increasing the efficiency and the quality of the services provided to

citizens and companies. According to the European Commission, only in 48% of cases do public administrations reuse information about the citizen that is already in their possession without asking for it again[50]. The extension of this principle, in compliance with the data protection legislation, would likely generate an annual net saving at the EU level of around EUR 5 billion per year by 2017[51].

Moreover, a **"digital-by-default"** strategy in the public sector (all services being provided digitally only) at the EU level could result in annual saving of around EUR 10 billion of annual savings. The adoption of e-invoicing in public procurement across the EU could generate savings of up to EUR 2.3 billion. The full exploitation of public sector data could additionally reduce government administrative costs; for Europe's 23 largest governments, some estimate potential savings of 15% to 20%, with a market value estimated at EUR 40 billion a year in the EU[52].

Implementation of the once-only principle enabling reuse of public sector data allows us to circumvent several pitfalls inherent to addressing this question in the private sector:

1) Public sector bodies do not have any competitive or market considerations (and generally also no revenue considerations) which could in turn lead them not to share data. The obstacles are rather questions of inertia or insufficient technical development.

2) While regulating B2B questions is politically difficult and potentially harmful to markets, no-one should be against providing businesses with more of their own data controlled by public administration.

[50] Commission Staff Working Document, A Digital Single Market Strategy for Europe – Analysis and Evidence http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:52015SC0100 &from=EN, p 74.

[51] Ibid.

[52] Ibid, p 75

Challenges regarding cross-border utilisation of the once-only principle

Changes to the current administration and data management policies. The principle of once-only requires many organisational changes (redesign of service delivery), technical work (unique base) or connected registries where unique data is held and accessible from) and agreements (legal and technical, incl. semantical on data details). Changes are always painful. There needs to be a common framework how data is securely exchanged (an existing example is the Estonian X-Road[53]) between government agencies in manner not infringing the fundamental rights of the individuals.

Data protection complexities. The implementation of the once-only is often at face value treated as a contrary to the purpose limitation principle set out in the data protection directive (95/46/EC) and in the GDPR. Although the data protection directive and the GDPR do set out how personal data has to be processed, these do not per se limit the options for data exchange in once-only mode – e.g. if people consent to this explicitly in service interaction or legally the "need-to-know" has been established for specific authorities.

Also, one of the fundamental principles of the GDPR is also the data minimisation principle (see art 5(1)(c) of the GDPR). If personal data is queried from the initial base registry and not kept in many locations where every agency possesses the same data, it is compatible with the data minimisation principle. Storing data in multiple locations makes the protection of the personal data stored in such way also more difficult from the integrity and confidentiality perspective (see art 5(1)(f) of the GDPR). So, as a sum, the once-only principle means that unique datasets are kept in base registries and data is queried from the initial source which means that if a database is compromised, the intruders never receive the full dataset of anybody.

Transparency and trust. Reuse of data by the public sector cannot be a black box. The application of this principle should be accompanied by a transparency mechanism where the user could see what data is accessed by which government office (for which purpose)[54]. Being transparent is important for the creation of trust.

EU possibilities to act. At the EU level, the EU can only take initiative if they have the competence to do so under the Treaties. However, e-government topics are the question of single market only to an extent – if data exchange enables the free movement of people, goods, service and capital. In other words, e-government must translate into the benefit of the single market - create new opportunities for citizens, and businesses that in turn translate into new jobs and sustainable growth for Europe[55].

Possible further actions

In order to deep-root the once-only principle at the EU level, we see four potential further actions:
1) Promote the cross-border implementation of the principle on a political level and establish the principle more thoroughly (e.g. with the Tallinn declaration on e-Government intended for October 2017).

2) Including the principle of once-only into the metrics of Better Regulation in order to reduce administrative burden;

3) Launch further pilots (regional or cross-EU) for the cross-border implementation of the once-only principle for personal data;

4) Initiate development of base or similar unique data registries (or connection of theirs) at Member State level, to build the necessary data foundation for once-only – EU could do well to also support this financially to provide incentives.

[53] See description: https://cyber.ee/uploads/2013/03/cyber_xroad_NEW2_A4_web.pdf. Explainer video: https://www.youtube.com/watch?v=9PaHinkJlvA

[54] n case of Estonia, this functionality is currently provided for six base registries. For more information, see: https://blog.ria.ee/aj/.

[55] See, for example, the Single Digital gateway proposal – COM(2017) 256 final.

Future framework for data access and portability of personal and non-personal data in the private sector to unleash the potential of the data economy

Problem definition

Future actions under this pillar will be most controversial as they potentially outline how companies should give out data to other companies, their consumers and the government. Therefore, careful scrutiny of existing rules is important before creating new rules because regulation could potentially have a chilling effect on innovation in data-driven technologies and force even more companies across the Atlantic to the U.S. This would be counter-productive as **the aim should be to create the best playing field for companies so they would keep their business in Europe and innovate.**

Clear rules over the use and access to data in the business-to-consumer (B2C) (when non-personal data is processed), business-to-business (B2B) and machine-to-machine (M2M) context is vital for the EU's data economy[56]**.** Europe should not shy away of creating new rules if this would benefit the EU's competitiveness. Although many researchers call for a cautious approach regarding access and portability of data[57], the need for clear rules on the access and (re)use are outlined by many stakeholders as being the key issue[58]. Therefore, **a debate over the extent of these clear rules is needed**.

In the case of regular goods, it is clear that when buying a good the buyer becomes the owner of the good from the moment the money is paid and the good is handed over to the buyer (possession is transferred). Owner has absolute rights over the good bought. In the case of smart devices, data becomes part of the deal as the good itself may be of marginal value compared to the data it generates. **Thus, when buying a smart device, the question is who should have access to the data the smart device is generating**. Is it the manufacturer? Or is the owner of the smart device together with the manufacturer? Perhaps, it is actually solely the owner of the device? Or the manufacturer and the cloud service provider? Is there a difference when the data generating device is bought by the individual or the company? Is there a difference when a product or service costs EUR 1.99 (for example, apps) or EUR 1.999.999 (for example, a sports car)? When is data portability more important than access? These are all vital questions in the context of the future framework for data access in the private sector. The maturity of the discussion renders it unable to provide all the specific answers just yet. Thus, a wider policy debate is needed as this is a controversial and highly disputed topics[59].

Below, two potential ways of guaranteeing that more data is accessible are analysed – data access and data portability.

[56] See also the White Paper on Digital Platforms by German Ministry of Economy and Energy, p 68. Accessible: http://www.de.digital/DIGITAL/Redaktion/EN/Publikation/white-paper.html. See also Conseil National de Numerique position on free flow of data. Accessible: https://cnnumerique.fr/liberte-de-circulation-donnees-intervention-de-celia-zolynski-lors-dialogue-etats-membres-a-commission-europeenne/.

[57] See for example, Graef, Husovec, p 1.

[58] See, for example, footnote 46 above.

[59] See https://ec.europa.eu/epsc/events/hearing-building-european-data-economy_en#transcript.

Access to data

Access to data is recognised as the main challenge of the data economy[60]. The ability to compete and innovate depends on having access to an appropriate pool of data[61]. However, there is a dilemma. On the one hand, there is an interest in facilitating access and re-use of existing data to allow for decentralised follow-on innovation. On the other, policymakers do not want to discourage firms investing in the original collection, creation and generation of raw data which is an input for competitive and innovative processes[62].

In the **B2C setting**, the first issue is whether personal data is processed or not. If the company is processing personal data, the GDPR will apply with its access rules (see page 14 below). If the company does not process personal data, there are no currently clear horizontal rules under which companies need to provide access to their consumers. Some sector-specific initiatives already exist (for example, in the field of energy. See page 15 below).

In the **B2B context**, the main existing legal regimes affecting the sharing of data or the obligation to share data are intellectual property law, contract law and competition law.

Intellectual property rights applicable to data is mostly linked with database protection[63]. This is an EU-specific regime conceived as a

[60] German Ministry of Economy and Energy, White Paper on Digital Platforms, p 68. Accessible: http://www.de.digital/DIGITAL/Redaktion/EN/Publikation/white-paper.html. See also Conseil National de Numerique position on free flow of data. Accessible: https://cnnumerique.fr/liberte-de-circulation-donnees-intervention-de-celia-zolynski-lors-dialogue-etats-membres-a-commission-europeenne/.

[61] Graef, Husovec, p 2.

[62] Graef, Husovec, p 2.

[63] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

toll for investment[64]. In its design, it was meant to support the EU-industry, which explains why the application of the protection is limited to only EU-residing firms[65]. The sui generis database protection (protection of "non-original" databases[66]) grants the maker of the database the right to prevent extraction and/or re-utilization[67] of the whole or of a substantial part of the contents of the database[68]. The maker of the database receives protection if he shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents of the database[69]. The term of protection of the database is 15 years. However, any substantial change which could be considered to be a substantial new investment will lead to a new term of database rights, which could, in principle, be perpetual[70]. This is one legal act at the EU level that sets out who is the "owner" of the data.

The Commission has listed the evaluation of the database directive as one of the actions to be done in the communication on Building a Data Economy[71]. Indeed, **it needs to be considered whether this type of protection is still relevant as protection of databases naturally influences the extent to which data can be accessed and reused by third parties.**

In private law, the general principle is that "everything which is not forbidden is allowed". This gives great room for freedom of contract. Freedom of contract is the general principle that enables contracting parties agree to terms without government intervention. So, in

[64] Graef, Husovec, p 7.

[65] Ibid.

[66] See http://ec.europa.eu/internal_market/copyright/prot-databases/index_en.htm.

[67] According to article 7(2) of the database directive, 'extraction' shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form; and 're-utilization' shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. The first sale of a copy of a database within the Community by the rightholder or with his consent shall exhaust the right to control resale of that copy within the Community.

[68] Article 7(1) of the database directive.

[69] Ibid.

[70] Article 10(1) and 10(3) of the database directive.

[71] COM(2017) 9 final, page 12.

principle, companies should have the right to agree to whatever concerning the assets they "own". The principle also recognizes both contracting parties as autonomous actors free to agree on whatever they want to[72]. However, in practice, weaker parties to the contract receive protection. Consumer law has been established for this purpose. Now, in the context of B2B relations, the similar question could be raised. The Commission has, in the context of the Communication on Online Platforms and the Digital Single Market, raised the question whether action is needed to address fairness of B2B relations beyond the application of competition law[73] similar to the Unfair Commercial Practices Directive[74] and the Unfair Contract Terms Directive[75] currently applicable to B2C relations as unequal bargaining power between incumbents and new entrants results in unbalanced contractual clauses regarding access to data[76]. **There needs to be a debate whether this is the proper tool, but it could definitely be one area to explore**.

Data access issues that are neither solved in contracts nor on the basis of database protection and data protection law (concerns B2C relations) may be remedied under competition law[77]. Under competition law, a company may be forced to give access to data to a potential competitor or new market entrant if: a) the company holds a dominant position in the relevant market; and b) refusal to give access to data amounts to the refusal of that dominant position. Such refusal stipulates a form of exclusionary abuse of the dominant position under article 102 TFEU. Existing case-law of the European Court of

[72] Of course, the freedom of contract principle is not absolute, but the general principle in civil law matters is that everything is permitted as

[73] Graef, Husovec, p 9.

[74] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').

[75] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts; and Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

[76] Graef, Husovec, p 9.

[77] Ibid., p 2.

Justice distinguishes the 'essential facilities doctrine'[78] which, however, has a very high burden of proof[79] and could refusal to provide access under article 102 TFEU can be considered abusive only under exceptional circumstances[80] as this doctrine interferes with the generally recognised principles of freedom to contract and freedom to dispose one's property. It has been found that by obliging a dominant firm to share access to its assets with competitors may stimulate competition in the short term, but may reduce the incentives of the dominant firm, its competitors and market participants in general to invest in innovation in the long run[81].

Many of the data relevant under this pillar is already and will be more so in the future generated by **machines and sent to other machines (M2M)** for processing. Therefore, the questions of access to this type of M2M generated data are similarly important. The extent to which machine-generated data falls under the intellectual property rules, competition rules or data protection rules is not totally clear. Competition rules arguably apply if the "essential facilities doctrine applies". However, matters are more complicated with regard to database protection as it could be argued that it does not apply to raw data generated by the sensors or smart devices[82]. This leaves contract law as the mean tool for companies to deal with the question of "ownership" of the M2M generated data.

[78] See, for example, C-241/91 and 242/91.

[79] The following requirements need to be fulfilled for a refusal to grant access could constitute abuse Under article 102 TFEU: a) access to data is indispensable; b) the refusal excludes all effective competition on the downstream market; c) there is no objective justification for the refusal.

[80] Graef, Husovec, p 3.

[81] Opinion of Advocate General Jacobs in C-7/97, para 57.

[82] See COM(2017) 9 final, p 10.

Existing rules governing data access for personal and non-personal data

a) Personal data

Access to personal data is regulated with the data protection directive and the GDPR (lex generalis). To simplify, the GDPR enables the data subject to obtain:

confirmation that their personal data is being processed;
access to their personal data; and
other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see art 15 of the GDPR)

b)Non-personal data

Several sectoral initiatives exist which focus on granting access to data[83]. The important task is to see whether these initiatives already cover the problem of access to data and to which extent these need to be reviewed. Below are some of the more relevant ones:

[83] Legal study on ownership and access to data, Osborne Clarke LLP, Annex 1. Accessible: https://bookshopeuropaeu/en/legal-study-on-ownership-and-access-to-data-pbKK0416811/.

[84] Ibid, p 102-103

Sector	Legal act	Description
	Database directive (96/6/EC)	Potentially creates a form of ownership over data in the database, but has proved in practice to confer protection limited to pre-existing data which originates from third parties and so has been the subject of investment to "obtain, verify or present" the data. Data which arises in the course of a company's own activities such as operating machinery, developing and selling products, is unlikely to be protected since the investment made is in those activities rather than in verifying or presenting the data arising[84].

Sector	Legal act	Description
Automotive	Regulation 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (as amended)	Vehicle Emissions Regulations: regulates levels of pollutants for most vehicle types, including cars, lorries, trains, tractors and similar machinery, but also aims to ensure competition in the market for car maintenance services and spare parts. The Regulation stipulates that manufacturers must provide unrestricted and standardised access for independent operators to all information required for diagnosis, servicing, inspection, periodic monitoring, repair, re-programming or re-initialising of the vehicle and which the manufacturers provide for their authorised dealers and repairers, including all subsequent amendments and supplements to such information. This information includes: a) an unequivocal vehicle identification; b) service handbooks; c) technical manuals; d) component and diagnosis information (such as minimum and maximum theoretical values for measurements); e) wiring diagrams; f) diagnostic trouble codes (including manufacturer specific codes); g) the software calibration identification number applicable to a vehicle type; h) information provided concerning, and delivered by means of, proprietary tools and equipment; and i) data record information and two-directional monitoring and test data. Manufacturers may change reasonable and proportionate fees for access to vehicle repair and maintenance information; a fee is not reasonable or proportionate if it discourages access by failing to take into account the extent to which the independent operator uses it. Daily, monthly, and yearly fees must be offered, the amount varying in accordance with the respective periods of time for which access is granted.

Sector	Legal act	Description
Financial services	Directive 2014/65/EU on markets in financial instruments repealing Directive 2004/39/EC ("MiFID II") and Regulation (EU) No 600/2014 on Markets in Financial Instruments ("MiFIR")	MiFID II and MiFIR: aim to ensure price transparency in financial markets. Relevant to businesses which depend upon financial data. Requires trading venues to offer disaggregated pre- and post-contract data for all securities trades on a reasonable commercial basis, in order to prevent monopolistic market positions arising through exclusive control of financial market data.
Energy	Directive 2010/30/EU of the European Parliament and of the Council of 19 May 2010 on the indication by labelling and standard product information of the consumption of energy and other resources by energy-related products ("Energy Labelling directive")	Energy Labelling directive: mandates energy efficiency information being provided on various consumer products to enable consumers to choose energy efficient products. Now offers less useful information than it did when first introduced since most products now on the market are in the highest efficiency category, so a proposal is under consideration to redefine the efficiency categories. However, no information is provided about how the efficiency is achieved; this Directive therefore does not grant competitors meaningful access to product data.

Data portability

Personal data

Portability of **personal data** has been established with article 20 of the GDPR. This enables the data subject to receive the personal data concerning him or her, which the data subject has provided to a controller based on consent on the basis of the contract, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided[85]. The right of the data subject applies only insofar as this is technically feasible for the company[86]. According to the Article 29 Working Party guidelines on data portability, the purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her[88]. It remains to be seen how this new right will be invoked by the data subjects and how will it work in practice as the right will be in force from 25 May 2018. Several elements will need clarification in case-law. However, we see data portability as an important element to lessen consumer lock-in and for increasing consumer choice. Therefore, **we suggest that guidelines and case-law providing legal clarity on the use of this right be interpreted widely rather than restrictively**.

Currently, the right of portability of personal data does not apply vis-à-vis government agencies and as a future initiative, **portability of government data should also be seen as potential future direction to unlock personal data from government databases.**

There are several initiatives focusing on the personal information management systems (known as 'PIMS'). Existing players in the field of user-centric personal data processing are, for example, digi.me, Meeco, Dawex, Qiy Foundation. Additionally, governments have explored these initiatives – midata (UK), MesInfos (FR), MyData (FI) and ProjectVRM (U.S). Trusted intermediaries could, in the future, play an important role in the practical implementation phase of access and portability rights for personal data.

[85] Article 20(1)of the GDPR.

[86] Article 20(2) of the GDPR.

[87] WP 242, p 3.

[88] For example, what are the criteria of 'technical feasibility'? What is considered as 'transmitting' personal data by the data subject? What is 'personal data' that can be ported under this right?

Non-personal data

Data portability means that consumers and businesses can easily transmit 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[89]. As such, the question of portability of non-personal data similarly arises. 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[90].

The right to data portability is relevant both in the B2C and B2B contexts. In the **B2C context**, the question is whether the individual who buys or leases a device that generates data should have the right to port the data generated from that device. Limiting the right to receive and transmit non-personal data could be a problem and limit consumer choice in the future as more and more devices and appliances people use will be connected to the Internet and generate data (Internet of Things). For example, the smart car.

Modern cars are equipped with many sensors measuring everything from the wear and tear of brake pads to fuel efficiency. The cars are capable of communicating wirelessly with manufacturers, traffic management systems, and other vehicles in real time. This data is sent to the manufacturer who has information about how the car was driven, and how soon it is likely to need a service. This knowledge can be converted into money as the manufacturer will have wireless access to the data and could then alert the owner of the car and even book the service automatically. The process can be very convenient, however, certain questions are left up in the air, e.g. what if the service is owned by the manufacturer? Additionally, the owner might not be getting the best price for the new parts and servicing. Thus, the situation of exclusive access to data clearly gives the car manufacturers a privileged position in the market and hinders business for the aftermarket (car retailers) and repair shops. This, in turn, limits consumer choice[91].

[89] COM(2017) 9 final, p 15.

[90] Ibid.

[91] Example from 'Why your car servicing costs could be about to rise' by M.Wall. Accessible: http://www.bbc.com/news/business-39103150.

The solution could be to grant individuals portability rights to the raw-data[92] **generated by the devices they own or lease (i.e. data that exists because of a person, however, the data may be non-personal)**[93]. This would enable unlocking non-personal raw data from silos and would increase consumer choice. For example, persons could be able to authorise public authorities or the universities to analyse this raw data for research. Combined with the right of personal data portability, this could potentially lead to the emergence of new business models and innovation.

In the context of **B2B relations**, the right to data portability of company's data is similarly an issue. The discussions on the extension of scope of the portability of data in the B2B context is only in its infancy, but is an important part of the discussion on future framework of the data economy as companies might be forced to lock into a service if relevant portability is not guaranteed. However, to what extent contract law should decide data portability in the B2B context requires further research as it has been argued that a legal obligation to data portability could potentially have a chilling effect on firms' incentives to innovate[94].

[93] The Commission has named this right as the 'data producer's right'.

[94] SWD (2017) 2 final, page 48. Accessible: http://ec.europa.eu/digital-single-market/news-redirect/52044. The data portability rule under the GDPR has been criticized due to the fact it applies similarly to SMEs and large multinationals.

For example, if a company wishes to start a business abroad it needs to prove its attributes (e.g. credit history) on paper. In order to tackle these shortcomings, a solution could be seen in the fact that the company should also be able to receive its data in an electronic and machine-readable format from the initial processor (a bank in our case) for transmission to another private entity (e.g. a bank in one Member State could send the data straight to a bank in another Member State).

Possible further actions

There is significant legal complexity regarding access and portability of both personal and non-personal data. In order to tackle the problems inhibiting data access and portability that arguably are the fuel of the data economy, the EU should identify existing gaps on the basis of evidence on the market and find the best options. On the basis of the maturity of the discussion, there seems to be no silver bullets and most literature refers to the need for more evidence before regulating access and portability matters. It is important to note, however, that like any other asset, data tends to concentrate. In the information age, data can be processed into information and knowledge[95] which means power – both in the public and private sector.

Issues related to data access and portability should be handled at EU level as **disparate approaches could increase compliance costs for companies involved in the cross-border activities and distort competition and put the achievement of the single market at danger**[96].

For example, French Loi pour une Republique numerique adopted on 7 October 2016 which will include a data retrieval obligation for providers of online public communications services in French consumer protection law. Articles L.224-42-1-L.224-42-4 of this act lay down that providers of online public communications service have to enable a consumer to recover free of charge all data that he or she has stored online as well as data resulting from the use of his or her user account that can be consulted online, with the exception of the data which has been significantly enhanced by the provider concerned. The law enters into force in May 2018 like the GDPR[97].

[95] See https://www.i-scoop.eu/big-data-action-value-context/dikw-model/.

[96] Graef, Husovec, p 11.

[97] Ibid.

[98] Yann Ménière, Nikolaus Thumm (ed). Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms. Research Analysis of a Controversial Concept. European Commission JRC Science and Policy Report 2015. Accessible: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96258/jrc96258.pdf.

The initial potential further actions in relation to data access and portability are:

Access:

a) The European Commission should identify gaps in the current regime and act where necessary on the basis of existing initiatives to improve access to data; be ready to adopt new general-purpose or sector-specific laws at EU level which improve access to existing data;
b) Identify incentives under which companies would be more willing to share their data. For example, access under remuneration (FRAND[98] terms or alternative intellectual property models that stimulate collaboration);
c) The horizontal rule on access should be that data must be accessible in a practically usable machine-readable format.

Portability:

Extend the scope of data portability to non-personal data in both B2C and B2B context, for example by (but not limited to):
a) In the B2C context, we propose that the obligation to provide data portability should be extended to raw non-personal data where the consumer buys (or leases) a device that generates data to enhance competition and consumer choice, stimulate data sharing and avoid vendor lock-in. Arguably, raw data, that is being generated by the sensor or smart device, is not protected by existing intellectual property rights, sui generis database rights, nor as a trade secret.
b) In the B2B dimension, no company should be locked out of data which creation it has been part of (even if only as a data source). For companies, the lack of data portability could negatively influence business continuity and force lock-in. However, whether data portability should be guaranteed under the freedom of contract or as a legal requirement for companies needs further analysis as it could be argued that a legal obligation to data portability could potentially have a chilling effect on firms' incentives to innovate.

Being a vision paper, any questions, comments and feedback is very much appreciated. Please address this to Mr Kaspar Kala from the Ministry of Economic Affairs and Communications. E-mail: kaspar.kala@mkm.ee; Skype: kaspar.kala.