EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 304 final

PART 1/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

on a framework for the free flow of non-personal data in the European Union

{COM(2017) 495 final}
{SWD(2017) 305 final}

Table of Contents

1 Context

The political support for an EU free flow of data initiative is very strong, placing it at the centre of the development of digital technologies and services across the EU, rendering it a key element in achieving the Digital Single Market:

A majority of Member States support free flow of data in the EU:

- **16 Heads of State and Government** called for a legislative proposal on free flow of data in December 2016;
- In its Conclusions of 15 December 2016 **the European Council** stressed the need to remove "remaining obstacles within the Single Market, including those hampering the free flow of data";
- Ministers of **15 Member States** reiterated in May 2017 their call to present without delay a legislative proposal to remove data localisation restrictions that cannot be objectively justified.
- Following the structured dialogues, the positions of some **initially reticent Member States** have evolved in the direction of support.

The European Parliament is also a strong supporter of free flow of data:

- In April 2017, a **group of key MEPs** representing different political groups sent a letter to the Commission President calling for a Regulation on the free flow of data.

The **Estonian Presidency of the Council** has identified the free movement of data as a central priority and a key theme of the upcoming (September 2017) **Tallinn Digital Summit of the Heads of State and government**.

Over the last year, the Commission services have carried out further detailed assessment in order to collect as much as possible data and stakeholder's feedback to grasp those elements that represent an obstacle to the correct functioning of Digital single market in the area of free flow of data, through the following key actions:

- the public consultation on Building a European Data Economy (**January - April 2017**);
- structured dialogues with Member States (3 collective meetings and 16 bilateral discussions from **February to May 2017**);
- completion of studies on data flows, localisation restrictions and their economic impacts (including a workshop with stakeholders in **March 2017**); new studies on switching of cloud providers / data porting (including a workshop with stakeholders in **May 2017**) and on cloud certification / security.

These combined inputs have not only provided new evidence on the obstacles to data flows in the EU, but have allowed the scope of the options and of the proposed initiative to be refined in order to better target the problem and its different drivers.

1.1 Technology-driven innovation

New digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things (IoT), are transforming our society and economy and are opening up new opportunities for European citizens, businesses and public administrations.

These technologies are designed to gather, manage, distribute and analyse data in order to maximise efficiency, enable economies of scale and develop new services. They offer benefits to users, such as agility, productivity, speed of deployment and autonomy, e.g. through machine learning[1]. For instance, the new generation of data storage and processing services combine cloud and artificial intelligence software. The ability to move data easily to and between these systems - even if they

[1] Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn from data samples and improve from experience without being explicitly programmed.

are located in different Member States - is a necessary pre-condition for making full use of their potential.

Unlocking this potential requires action, in the short term, on the following issues:

- Improving the mobility of data across borders in the single market, which is limited today in many Member States by localisation restrictions or legal uncertainty in the market;
- Making it clear and ensuring that, as the free flow of data is implemented in Member States, the responsibility of private parties to provide data for regulatory control purposes remains unchanged, as trust is a key element in the development of the data economy;
- Making it easier to switch service providers and to port data, since this is key to the development of a competitive cloud market in the EU, benefiting in particular SMEs;
- Making further progress on the security of data and cloud services in order to enhance trust and to avoid fragmentation of the single market as a result of different approaches in Member States.

Resolving these issues will facilitate the movement of data across borders, across data storage and processing (cloud) services (CSPs)[2] as well as between CSPs and in-house IT systems[3]. It will **create the foundation** upon which future cross-cutting (e.g. re-use of data across borders) and sectoral[4] **data policies can be built**.

Further economic and technological context is provided in **Annex 9** to this Impact Assessment.

1.2 Data flows and data economy

Data is at the heart of all new technologies, and the data market (i.e. the market where digital data is exchanged as products or services derived from raw data)[5] has become a market on its own. In 2016, the value of the EU data market was estimated at almost EUR 60 billion, showing a growth of 9.5% compared to 2015. It could potentially amount to more than EUR 106 billion in 2020[6].

The January 2017 Communication "Building a European Data Economy"[7] set out several issues, the resolution or clarification of which would contribute to a clear framework for data. This would facilitate the rapid evolution of technology, the emergence of data as a key factor of production as well as a competitive differentiator, and create the right conditions for investment and innovation in Europe. These issues include:

- free flow of data (the focus of this initiative);

- data access and transfer (whether 'ownership' rights exist on non-personal data that are generated as part of a business process or that are de facto in the possession of a business; what are the conditions of usability and access to such data);

- liability (how to provide certainty to both users and manufacturers of data technologies and services in relation to their potential liability);

- portability, interoperability and standards (how non-personal data exchange and competitive data markets could be stimulated; partly the focus of this initiative).

Although all these issues are important, it makes sense to address the free flow of data in first instance. The speed with which the market is embracing new technologies is a strong reason to

[2] Although data storage and processing services encompass more than only cloud services (e.g. merely hosting servers), for reasons of brevity the term used hereafter will be 'cloud service providers', or CSPs.
[3] Servers owned and/or operated by enterprises and public sector organisations
[4] E.g. banking and finance, e-health, connected and automated driving, smart grids, etc.
[5] IDC and Open Evidence, European Data Market, Final Report, 1 February 2017 (SMART 2013/0063).
[6] IDC and Open Evidence, European Data Market, Final Report, 1 February 2017 (SMART 2013/0063).
[7] COM(2017) 9, "Building A European Data Economy", 10 January 2017; see also Commission Staff Working Document accompanying the Communication, SWD(2017) 2 of 10 January 2017, https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy.

remove immediately the remaining barriers to the movement of data within the EU and thereby ensuring effective and efficient functioning of data storage and processing, which is at the fundament of any data economy. The resulting legal certainty in the market would stimulate innovation and improve Europe's global competitiveness.

Moreover, the market maturity and opportunities for intervening are different for the different issues. For the barriers to the movement of data, the cause is relatively simple - they spring from the forced storage or processing of certain types of data in electronic format within a geographical zone or IT environment[8].

Other data issues arise from disruptive business models emerging from the digital transformation of the industry, technological advances and a fast-evolving data market, and their implications are still far from clear and need further assessment.

The **public consultation** confirmed that these other data issues, such as data access, transfer and liability, are more difficult topics and less mature topics that deserve further assessment. Indeed, when it comes to potential actions to make more data available for re-use across businesses, most stakeholders call for prudence. They argue that data value chains and business models building on data are of great variety making it difficult to conceive one-size-fits-all solutions. Regarding liability, the need for further assessment taking into account the findings gathered so far also emerges from the public consultation. .[9]

The General Data Protection Regulation (GDPR) provides a single set of rules for the entire EU ensuring a high level of protection of personal data. Businesses and public sector entities processing personal data must comply with these rules. The GDPR will enable people to better control their personal data. At the same time its modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by cutting red tape and benefiting from reinforced consumer trust.

In line with the DSM Mid-Term Review Communication[10], **the present initiative focuses on aspects of data flows within the EU that are not regulated by the GDPR**: those stemming from decisions of businesses or public sector entities on (i) the choice of a geographical location for data storage or processing and (ii) the choice of a data storage or processing service provider or the choice of in-house IT system(s) for centralised or distributed data storage or processing within a business group.

To the extent that this initiative deals with mixed data sets that include personal data, the applicable provisions of **the GDPR** must be fully complied with in respect to the personal data part of the set.

1.3 Policy background

The policy initiative covered by the present Impact Assessment should be seen in the light of the priority given by the Juncker Commission to creating a connected Digital Single Market (DSM)[11], which aims at maximising the growth potential of the economy, not least by removing the remaining barriers to a competitive data-driven economy in Europe.

The DSM Strategy announced *"a European 'Free flow of data' 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".*[12]

[8] Some of the barriers are also residual from the 'paper era'.
[9] Synopsis Report, Public Consultation on "Building a European Data Economy"
[10] COM (2017) 228, "Mid-Term Review on the implementation of the Digital Single Market Strategy", 10 May 2017.
[11] See: https://ec.europa.eu/priorities/publications/president-junckers-political-guidelines_en.
[12] In the Staff Working Document accompanying the DSM strategy, the Commission had already pointed out that data localisation restrictions can in fact limit the benefits offered by digital services such as cloud computing as they create barriers to EU cross-border data transfers, limiting the competitive choice between providers and raising costs by

The Communication "Building a European Data Economy" stated that in order to "*realise the full potential of the European data economy, any Member State action affecting data storage or processing should be guided by a "**principle of free movement of data within the EU**", as a corollary of their obligations under the free movement of services and the free establishment provisions of the Treaty and relevant secondary legislation*".

The recent **mid-term review of the Digital Single Market strategy[13],** which assessed the progress towards the implementation of the Digital Single Market, re-iterated the importance of the European data economy framework and urged political action, concluding that the Commission will:

> … *"by autumn 2017, subject to Impact Assessment, prepare a legislative proposal on the EU free flow of data cooperation framework which takes into account the 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"*. It also stated that this framework could, in addition to taking into account these principles, address Member States' legitimate interests on secure storage of data.

The policy intervention also builds upon the **Digitising European Industry** (DEI) policy package that included the **European Cloud initiative**[14] aiming to deploy a high capacity cloud solution for storing, sharing and re-using scientific data. The free flow of data will contribute to an effective functioning of this open environment. Furthermore, the initiative builds upon the revision of **the European Interoperability Framework**[15], which aims to improve digital collaboration between public administrations in Europe and will benefit directly from the free flow of data. It contributes to the EU's commitment to an **open Internet**[16]. The policy initiative also responds to the calls from stakeholders expressed in the **REFIT Platform**[17].

1.4 Scope

The initiative concerns data storage and processing in its broadest sense, encompassing usage of all types of IT-systems, whether located on the premises of the data controller or outsourced to cloud service providers[18]. The initiative also **covers data processing of different levels of intensity**, from mere data 'storage' (Infrastructure-as-a-Service (IaaS) in cloud terminology) to the processing of data on platforms or in applications of different kinds (or, in the jargon, respectively Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS)).

The scope of this initiative is limited in order to **avoid duplication** and to ensure consistency **with existing legal instruments and other Commission initiatives**. In particular, this initiative takes into account the provisions and fields of application of different existing EU legal instruments, such as the GDPR, the e-Commerce Directive, the Services Directive, the Single Market Transparency Directive and the NIS Directive (see sections 3.3 and 8).

It will be **synergetic with the planned initiatives** on the EU ICT security certification framework, online platforms and digital innovation in health and care. It takes into account the forthcoming solutions, including legislative ones, to improve access to e-evidence in criminal matters by law enforcement authorities.

---

forcing organisations and companies to store data on servers physically located inside a particular Member State, SWD(2015) 100 final, 6.5.2015.

[13] COM(2017) 228 final, "Mid-Term Review on the implementation of the Digital Single Market Strategy", 10.5.2017.

[14] COM(2016) 178 final, "European Cloud Initiative - Building a competitive data and knowledge economy in Europe", 19.4.2016.

[15] COM(2017) 134 final, "European Interoperability Framework – Implementation Strategy", 23.3.2017.

[16] COM(2014) 72 final, "Internet Policy and Governance - Europe's role in shaping the future of Internet Governance", 12.2.2014

[17] See Figure 3 - Overview and illustration of the data localisation problem (at the end of section 2).

[18] Other data processing services include data analytics, data management systems, etc.

The territorial scope of the initiative is **limited to the European Union**. It does not address data localisation restrictions put in place by the countries outside the EU or movement of data outside of the EU[19]. This Impact Assessment acknowledges the importance of the international dynamic and of current developments around global data flows, their impacts on EU competitiveness and the importance of protecting fundamental rights[20].

The initiative **does not concern the processing of personal data[21] and the free movement of such data *as governed* by the GDPR and the proposed ePrivacy Regulation**. Specifically, since the GDPR prohibits restrictions on the free movement of personal data within the Union where these are based on reasons connected with the protection of personal data, the initiative deals with data flow restrictions imposed by Member States based on reasons other than the protection of personal data (e.g. security of storage of the data).

For instance, company laws can require local storage of certain corporate information and documents (e.g. registers of shareholders and directors). Those often include personal data, e.g. names of corporate executives. However, the reason for such localisation is to make sure that shareholders and other interested parties can get access to and review the information / documents, and not to protect any personal data. As the GDPR does not address such restrictions, the present initiative will address them.

The initiative also addresses the issue of porting data from one IT environment to another, to the extent that it constitutes a barrier to the movement of data within the EU and the ability to switch cloud service providers or move data back in-house. The initiative will take into account Article 20 of the GDPR, which gives the right to the data subject to receive the personal data concerning him or her from a data controller and the right to transmit those data to another controller. However, this provision cannot be invoked by businesses or public sector entities in B2B data porting scenarios involving personal data, e.g. where a business entity wants to get back or port to another cloud service provider (CSP) all the data sets, including personal data sets.

For instance, a cloud service provider specialising in managing application processes for universities accumulates both personal and non-personal data from the universities using its service (its customer) and stores the data with a major cloud provider (its subcontractor). At some point in time the data service provider wants to switch to another cloud service provider and port all the data it has accumulated to a new subcontractor. This data porting scenario will not fall under Article 20 of the GDPR so that specific issue will be addressed by the initiative.

In this regard the scope of the initiative also differs from the planned online platforms initiative. While the data porting element of this initiative focuses on two-party (cloud provider – cloud user) relationships and seeks to make it easier to port the data provided and controlled by the cloud user, the platforms initiative would focus on the three-party (consumer/business – platform – business) relationship. It would seek to make it easier for businesses offering products or services through platforms to obtain access to the data held by the platform, which has been provided to the platform by the customers of the business concerned while using the platform.

2 Problem Definition

2.1 Relevance of the problem

In an increasingly data-driven economy, data flows are at the core of business processes in

[19] International data flows are dealt with separately under the project team co-managed by Commissioners Jourova, Malmström and Vice-President Ansip and their respective services.
[20] Any transfer of personal data outside the EU must be in compliance with Directive 95/46/EC, which will be replaced by the GDPR on 25 May 2018.
[21] The GDPR defines 'personal data' as any information relating to an identified or identifiable natural person (Art.4.1).

companies of all sizes and in all sectors: from data-intensive ICT companies to manufacturing and agriculture processes, to hospital administration and key electricity infrastructures. In **the public online consultation "European data economy"**, a large number of respondents indicated that they process data in multiple Member States mainly for operational reasons, namely the cross-border character of their activities, the location of subsidiary companies and the satisfaction of consumer expectations in terms of proximity (see further in **Annex 2**). This is equally true for public administrations, not least in supporting data-informed policies and public services delivery within and across borders. Therefore, data is increasingly ubiquitous, supporting all sectors of industry, economy and society.

The nature and role of data in the economy is complex, however. Inherently, data 'travels' across cross-border value chains, where it is generated, collected, curated, processed and analysed, transferred and stored. Its value can increase exponentially when it is aggregated, analysed, or used in innovative ways. Data can become a competitive differentiator and an enabler for innovation and creation of new business models, for example in the fields of data analytics, text and data mining and app development.

However, in the European Union the possibility to build a data economy and to benefit from new technologies which rely on data[22] is undermined by a series of barriers to data mobility, impacting business behaviour in the Single Market.

2.2 Core problem: obstacles to data mobility in the EU single market

"Obstacles to data mobility in the EU single market" is the core problem identified.

"**Data mobility**" refers to the degree in which data can be (re-)located to different IT-systems, regardless of the physical location of such systems in the Union or the owner of such IT-systems, which might be the data holder himself or a data storage and processing service provider/CSP.

A high degree of data mobility is important for realising a European data economy to its full extent, since it is required for core activities of such an economy, for instance data collection, analysis and re-use.

2.3 Problem analysis

Making use of the Better Regulation toolbox[23], the Commission services conducted an extensive analysis of the core problem and its drivers. On the basis of evidence supplied by the public online consultation, the structured dialogues with the Member States and other stakeholders, dedicated support studies, external studies and available data[24], the Commission services have verified the existence of four underlying problems that cause obstacles to data mobility.

Problem 1: Member States' legislative and administrative restrictions

Problem 2: Legal uncertainty

Problem 3: Lack of trust

Obstacles to the movement of data across borders within the EU

Problem 4: Vendor lock-in

Obstacles to the movement of data across IT-systems

Obstacles to data mobility may lead to a large number of negative consequences for European society and economy, hindering the EU's policy objective of creating of a Digital Single Market. Following analysis, the consequences of these obstacles have been divided into four main categories.

Consequence 1: Loss of growth/innovation potential

[22] An estimate shows that 75% of the value added through the Internet (and, implicitly, data flows) rests with traditional industries, see http://europa.eu/rapid/press-release_MEMO-12-759_en.htm.
[23] Specifically, Tool #11: "How to Analyse Problems", http://ec.europa.eu/smart-regulation/guidelines/tool_11_en.htm.
[24] See Annex 1 for a full list of sources used.

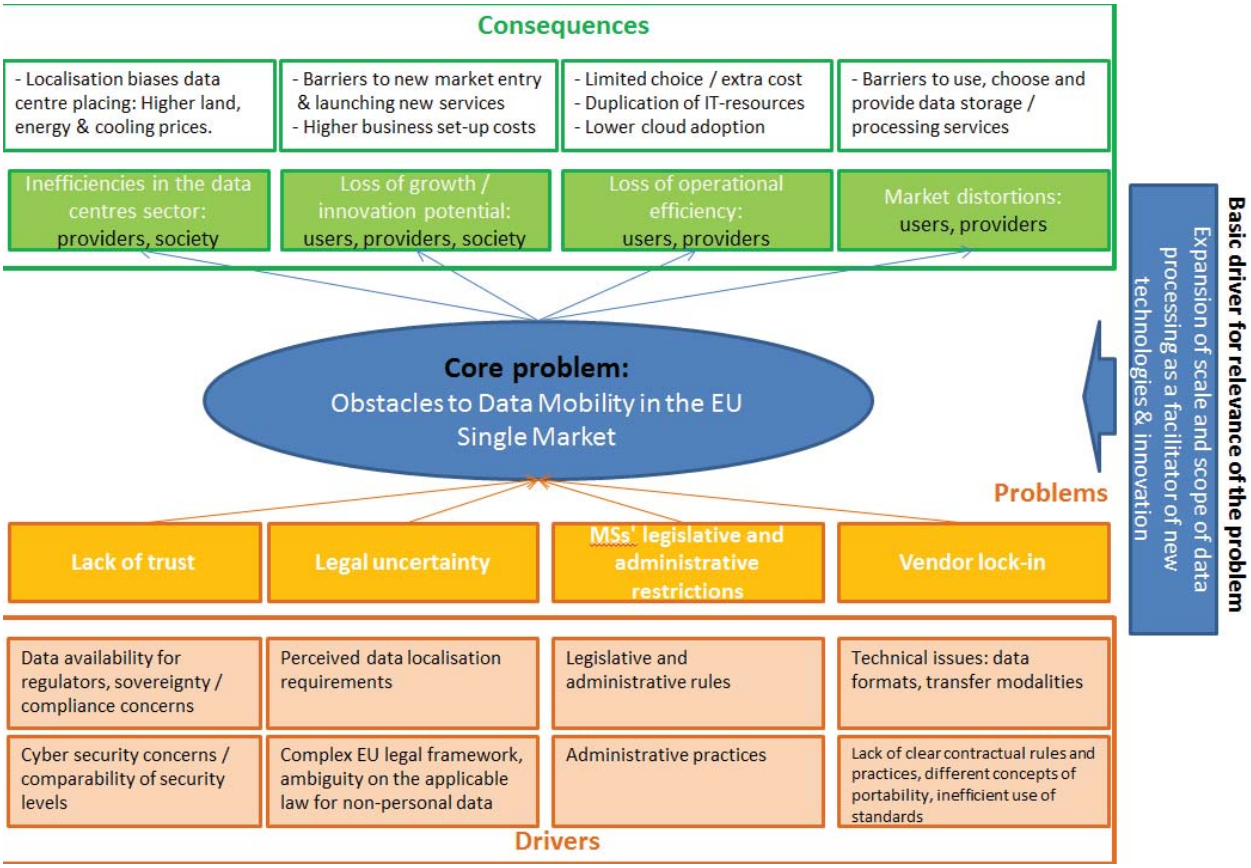
Consequence 2: Loss of operational efficiency

Consequence 3: Inefficiencies in the data centres sector

Consequence 4: Market distortion

For a visual mapping of the problem analysis, see Figure 1: the Problem Tree. In the remainder of this section, the individual problems and consequences will be briefly described, elucidating the many interrelations between them. **For the full problem analysis, comprehensive explanations, examples and extensive references to evidence, the reader is referred to Annex 5**.

Figure 1 - Problem Tree



2.3.1 Underlying problems & drivers

Member States' **legislative and administrative restrictions** form the starting point of the problem analysis, because they represent the most tangible obstacles to data mobility in the EU. To a varying degree, Member States have put in place so-called 'data localisation restrictions'. These are rules that either oblige citizens and businesses to process and store certain categories of data within the territory of the country, or have an equivalent effect. Data localisation restrictions come in many forms, ranging from 'hard law' to 'soft law' measures and administrative practices. National governments are not the only type of actor capable of raising them. Regulatory or supervisory authorities or other sector-level institutions can also do this.

The number of data localisation restrictions has been growing as a response to the digitisation of the economy as a whole and the strong development of the data economy; according to some sources, the number has at least doubled since 2006.[25]

[25] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016. Some data localisation measures included in the report fall outside the scope of this initiative.

Member States' reasons for data localisation restrictions

Data localisation measures are adopted by Member States for different reasons, which are prominently data security (in a wide sense, which encompasses concerns like confidentiality, integrity, continuity and accessibility for the controller of the data), and the availability of data for supervisory and regulatory authorities of the Member States.26 This has been confirmed by the bilateral and multilateral exchanges with Member States and private stakeholders, subsequently to the Communication of January 2017.

A study raised that security is a common driver behind data location restrictions imposed by Member States and is often used as "convenient shorthand" for national security, national sovereignty and for security as a public policy task or as a protection of private interests.27 Therefore, some legislative and administrative rules are imposed in order to keep data out of reach of other jurisdictions and limit the access of other governments to specific types of data. Those restrictions reflect concerns to protect the confidentiality of certain types of data, to control access to such data and to oversee legal proceedings in case of unauthorised access, particularly to citizens' data, national sensitive data, privileged information and industrial secrets.

Furthermore, security concerns by Member States are largely unfounded. Localisation is not a proxy for security, but the means of storage is. Contrary to concerns on cyber security, evidence suggests that data stored in large-scale data centres is actually safer than data stored on-site. The economies of scale that are inherent to data centres make it easier to invest in state-of-the-art data security. In addition, CSPs spend much more time and effort on security to be compliant with certain certification schemes as to meet customer expectations and favour demand.

For some legislative and administrative rules, Member States aim at ensuring that the data is immediately available to the national government, administrative authorities and/or law enforcement institutions. A number of the restrictions and requirements are therefore based on considerations that originated in the 'paper era', where documents needed to be physically accessible for scrutiny or where only the original paper version had legal status.

Despite these reasons and objectives, data localisation restrictions often are unjustified or disproportionate, since (i) effective alternative means to achieve the relevant public policy objective are available (e.g. requiring access to accounting and company data could replace outdated measures and obligations requiring accounting and company data to be stored locally) and/or (ii) the scope of a measure is excessive / the measure concerns non-critical data (e.g. requiring all public archives to be stored locally).

One of the main causes for this trend is presumably the attempt by regulators to transfer the given means of control and reassurance tailored for the industrial age to the digital age. According to the OECD, computer services including data storage and data processing services are sensitive to restrictive regulations affecting trade and imposing an additional time burden on companies. It is crucial for these services to be delivered in a timely and agile manner. In view of the fact that all economic activities increasingly depend on them it is understandable why obstacles to such services can generate large economic losses. [28] Therefore respective regulatory barriers have comparatively an even stronger impact on trade, and the progressive emergence of such restrictions is set to increase in gravity in light of the massive expansion of the data economy.

Evidence gathering shows that the data localisation restrictions identified are only part of the core problem. Obstacles to data mobility in the European Union are driven at least as much by market dynamics leading to localisation because of risk-averse behaviour in the face of legal uncertainty.

[26] LE Europe Study (SMART 2016/0016) and TimeLex Study (SMART 2015/0054).
[27] TimeLex (SMART 2015/0054).
[28] Nordås, H., et al. (2014), "Services Trade Restrictiveness Index (STRI): Computer and Related Services", OECD Trade Policy Papers, No. 169, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5jxt4np1pjzt-en

Public and private entities in Europe often assume that they are not allowed to store or process data across borders, while there is actually no restriction in place. This is particular harmful in view of the fact that data services are among the key inputs to any modern economic activity, and that access to such competitive services can help companies - particularly SMEs - integrate into value chains, focus on core competencies and improve productivity.[29]

This phenomenon has several causes. First of all, there is **no explicit prohibition in EU law** against localisation of non-personal data. This gives rise to a large degree of **legal uncertainty** when it comes to cross-border data storage and processing. Several existing EU legislative instruments could be interpreted as prohibiting data localisation, or at least restrictions on services that rely on use of data, but these instruments always apply only to a limited number of cases.

Nearly one quarter of the 45 localisation restrictions identified in the evidence gathering process for this Impact Assessment[30] are exempted from the E-Commerce Directive, and between one quarter and two thirds of the localisation restrictions are excluded from the Services Directive.

Besides, the complexity of applicable legislation also exacerbates legal uncertainty. Apart from the Treaty, different potentially relevant provisions can be found in, among others, the Services Directive, the E-Commerce Directive and the Transparency Directive. This legal patchwork complicates rather than simplifies the matter and does not provide for the robust foundation needed for the emergence of an all-encompassing principle. The result is that European businesses and public sector organisations often store and process their data within the borders of their own Member State.

A data localisation restriction has to be tested against 33 provisions in 5 pieces of EU secondary legislation in order to determine to what extent it is covered by existing EU law.

Legal uncertainty also originates from the manifold and diverse sector-specific guidelines and administrative practices. In highly supervised sectors, such as finance or health, users may have a preference for storing data locally because they assume that it is implicitly required by their regulators.

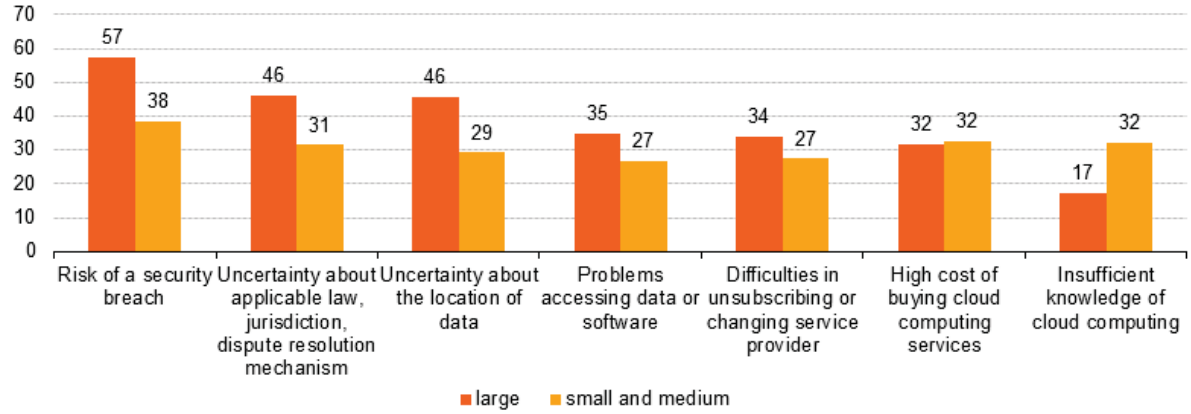
Besides widespread legal uncertainty, the problem of **lack of trust** also constrains data mobility. This lack of trust has two important pillars.

Firstly, there is the broader category of lack of trust in society vis-à-vis certain types of data storage and processing as such (e.g. cloud computing). This type of lack of trust frequently originates from concerns over data security and the protection of sensitive data. It is still rare for customers to rely completely on cloud services for storing their valuable data. Fear of the risk of a security breach is the most common concern, which directly constrains the uptake of cloud services, and which in turn leads to efficiency losses for businesses and, ultimately, society as a whole. Figure 2 below shows that the issue of lack of trust is intertwined with the legal uncertainty problem described above. The combination of both, together with vendor lock-in concerns (referred to below in this section) limits the uptake of cloud services.

[29] Idem

[30] Please refer to Annex 6 for a full list of identified data localisation restrictions.

Figure 2 – factors limiting enterprise use of cloud services



Source: Eurostat (2014)

As indicated above in the textbox on page 8, this type of lack of trust is largely unfounded as evidence suggests that data stored in large-scale data centres is actually safer than data stored on-site.

Secondly, a lack of trust can also be observed in relation to access to data for regulatory/supervisory purposes, when it is stored outside national borders. Certain data localisation restrictions are adopted to ensure the availability of data for inspection/control purposes.[31] The lack of trust surrounding jurisdictional and law enforcement challenges was also raised during the Structured Dialogues with the Member States.[32] Yet, the localisation restriction can be replaced with a functional requirement to ensure data availability for the supervisor, as the data can be made readily available for inspection electronically.[33] This has been exemplified by the amendment to the Danish Bookkeeping Act 2015[34].

In cases where the subject of regulatory oversight does not provide data voluntarily, the Member State might have to resort to issue-specific administrative cross-border access/sharing cooperation mechanisms or judicial cooperation or seek the voluntary assistance of the IT service provider. Cooperation and assistance frameworks have been established in criminal matters, administrative matters, such as taxation, and in financial regulations[35], with different scope of information and entities/supervisors concerned in the various instruments. This variety and the potential delays in judicial cooperation, likely generate uncertainty and lack of trust as to whether a specific (including unforeseen) data availability need could be fulfilled.

Vendor lock-in actions by cloud service providers constitute a form of data localisation restrictions imposed by the private sector, targeting more specifically data mobility across IT-systems instead of data mobility across borders in the EU. This problem occurs when users of data storage or processing services try to switch cloud service providers.

[31] Time.Lex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (SMART 2015/0054) at p.43.
[32] Specifically, workshop held on 23 February 2017.
[33] See to that effect, TimLex Study (SMART 2015/0054) at p. 99: if data should be stored on a server in a specific Member State in order to ensure its accessibility to a national supervisor, then the formal data location requirements can be "recast into a functional accessibility requirement".
[34] Denmark now allows accounting records in electronic format to be stored anywhere without prior application or notification to the public authorities, subject to the requirement on the business to provide online access to the records held abroad at any time. See also Annex 5.
[35] An overview of several sector-specific cooperation frameworks available for public authorities can be found in Annex 8 to this Impact Assessment.

Cloud switching[36] can lead to **prohibitive costs** for cloud customers (and especially SMEs). This includes costs for data transport and licence fees, downtime cost and the need for concurrent services during a transition period, as well as the cost of network use. The aggregate cost can potentially be very high. Numbers vary according to the complexity of each switching scenario, but the Commission has been informed of an anonymised example in which the total costs of data egress for the cloud customer amounted to of EUR 2.700.000 (for more information on the potentially excessive costs of porting data between providers or back in-house, please refer to section 6.2.1.3, the economic assessment of the baseline scenario). Some cloud customers have also reported instances where Cloud Services Providers offer much lower prices for the above cost categories when importing the data on their own systems than when they have to export it to a new destination. Accordingly, they attract customers by offering low thresholds for entry, but 'lock them in' by making switching costly. It is often easier to switch CSPs in the Infrastructure as a Service (IaaS) context, where the services rendered are those of data storage only. Moving into more complex services such as Platform as a Service (PaaS) and especially Software as a Service (SaaS), the difficulties with switching increase. IaaS and PaaS standards can be defined using simple interfaces, but this is mostly not the case with SaaS standards, which at least require more complex interfaces to retrieve the data.

The public online consultation showed that the problem with switching providers is already prevalent, as more than 50% of SME respondents indicated that they experienced difficulties when intending to switch. At the same time, the size and intensity of the problem may become even clearer over time, when the ever-growing cloud services market reaches new stages of dynamism in terms of supply and demand. Today, however, it is already clear that users of storage and processing services are often unaware of technical difficulties, for example in terms of network capacity (bandwidth), which may arise when they want to move their data from one service provider to another or back to their own premises. Also, they often have insufficient or no knowledge of the provisions in their contracts with cloud service providers. Issues at stake here are, for example, the costs of data transfer in the case of termination of contract or what will happen with the data when the service provider ceases to exist as a result of e.g. bankruptcy.

2.3.2 Consequences

Obstacles to data mobility, such as data localisation restrictions, form 'digital border controls' within the European Union and therefore are incompatible with the (digital) single market. They hamper EU businesses that operate cross-border, because certain data would have to be stored in specific and different Member States of activity, therefore leading to multiplication of storage costs. This is disproportionately burdensome for small companies such as start-ups and SMEs. The Scale-Up Europe Manifesto makes a specific reference to this problem: "Enforced data localisation will mean higher costs for the cloud-driven services upon which so many start-ups rely. It will add further uncertainty and immensely greater regulatory burden on fast-growing enterprises, which should rather focus on developing their business…".[37] A direct consequence of this **is a loss in growth and innovation potential** as the (disruptive) innovation potential of start-ups and scale-ups is very high. Next to start-ups and scale-ups, this problem also confronts other SMEs, which in total account for nearly 60% of European GDP and 65% of European employment[38]. Any impact on them would therefore have large implications for the EU economy.

[36] SMART 2016/0032, IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (Ongoing) [IDC and Arthur's Legal Study (SMART 2016/0032)]
[37] The Lisbon Council, Nesta and Open Evidence (2016), "The scale-up Europe manifesto"
[38] Eurostat, "Statistics on small and medium-sized enterprises", September 2015, available at : http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises .

If we assume that SMEs using private cloud services store 50 TB on average and the monthly price per GB of data stored ranges between €0.0224 (low cost location) and €0.5371 (very high cost location), a SME spends between €1010 and €26855 per month.[39] This would mean that an SME would face costs of at least €12120 per year, not considering the administrative costs, if it operates in one Member State. In view of existing and emerging localisation restrictions this cost will potentially duplicate, either fully or partially, for each Member State with respective restrictions where the SME wants to operate in. In particular for start-ups this would undermine cross-border scaling up substantially.

Moreover, a loss in growth and innovation potential will also be incurred because data localisation restrictions form barriers to new types of services that are geographically distributed by design.

The deployment of IoT technologies and applications could suffer from a lack of trust, legal uncertainties or blockages brought by data localisation. With an explosion in the number of connected objects in a variety of application areas – connected cars, manufacturing, energy, agriculture, etc. – data generated by IoT is geographically distributed by design.

According to responses to **the public consultation**, the highest impacts of data localisation restrictions, next to increased costs for business, are on the provision of a service to private or public entities (69.6% of stakeholders responding identified this impact as 'high') or the ability to enter a new market (73.9% of responding stakeholders identified this impact as 'high'). The EU itself is perhaps the most compelling proof that the free provision of services in an internal market leads to growth. Making the provision of cross-border data-based services in the single market more difficult would therefore put a constraint on the European economy.

Moreover, data localisation leads to a **distorted market** for cloud service providers. An important outcome of a dedicated support study showcases that data localisation restrictions force them to make business and investment decisions that lead to suboptimal outcomes in cost, security and operational agility.[40] Already there are large intra-EU price differences for data storage, varying up to 120% between different Member States.

The problem of vendor lock-in also constitutes an obstacle to data mobility; hence it leads directly to market distortions, as it cements the position of larger cloud service providers vis-à-vis new market entrants. Accordingly, vendor lock-in curbs free competition and drives up prices.

Based on the evidence gathered, from the data service (cloud) user perspective, different degrees of impacts caused by obstacles to switching and porting data can be envisaged. These range from very high impact, e.g. where a data service (cloud) provider goes bankrupt without a data porting possibility for the user, and the data is lost; to low, medium or high impact where the possibility to port data exists, but is constrained by technical or contractual issues, and, as a result, the user incurs extra costs and/or decides to port only part of data.

This market failure then leads directly to a **loss of operational efficiency**, which is the consequence caused by, on the one hand, a low-level of cloud adoption in Europe and, on the other hand, a lower level of innovation and efficiency of those cloud services because of the lack of fully free competition in the market. The suboptimal cloud adoption predominantly results from a lack of trust because of data security concerns. Research has confirmed the link between a lack of trust in cloud security and cloud adoption.[41] Also, it may be contended that a lower-than-expected level of cloud adoption derives from vendor lock-in, as this leads to less competitors on the market and therefore

[39] https://azure.microsoft.com/en-us/pricing/details/storage/blobs/ and http://www.telekom.hu/uzleti/szolgaltatasok/informatika/szerverek-adatparkiszolgaltatasok/szerverberles/virtualis-szerverek

[40] SMART 2015/0016, London Economics Europe, Carsa and CharlesRussellSpeechlys, "Facilitating cross border data flow in the Digital Single Market", 2016 [LE Europe Study (SMART 2015/0016)].

[41] Intel and McAffee (2017), "Building trust in a cloudy sky", accessed via: https://www.mcafee.com/us/resources/reports/rp-building-trust-cloudy-sky.pdf

higher prices. To quantify the scale of this problem, one of the Commission's support studies found that all EU businesses can reduce their overall ICT-expenditure by 20% to 50% as a result of adopting cloud solutions.[42] A significantly higher cloud adoption could therefore mean a large leap in the competitiveness of European business.

Finally, **inefficiencies in the data centres sector** are already visible negative consequences of obstacles to data mobility. As a result of intervention (or sometimes: uncertainty about intervention) in the market, cloud service providers locate their data centres in countries with significant markets where data localisation restrictions are in place. If those restrictions would not have been of concern, actors would have been able to base their decisions on different parameters such as energy prices, land prices or the envisaged environmental footprint of data centres in a certain location.

The problems identified in this section have significant (but differing) impacts on various stakeholder groups (see **Annexe 3**). **Annex 2** provides a synopsis report of the public online consultation.

Figure 3 - Overview and illustration of the data localisation problem

Feedback from stakeholders	Two thirds of respondents to the public consultation said that they had knowledge of the existence of data localisation restrictions. **80%** of them stated that their organisations must comply with these restrictions. The issue was also raised in the REFIT platform in April 2017.[43]	
Scale	**Legislative / administrative requirements**	**Localisation driven by legal uncertainty / lack of trust in the market**
	- 56 identified by the studies[44] - 49 sent to MS for the structured dialogues (measures outside scope of initiative were discarded) - 9 removed or to be removed in the future by MS - 20 new measures identified by the public consultation (specific legal acts not always mentioned, some might coincide with those identified by the studies) - Approximately 60-65 known measures in place at the time of this IA - More than two thirds of the sample of 45 analysed in detail could be considered unjustified or disproportionate at the time of this IA **Further details – Annex 5 for the analysis and Annex 6 for the list of measures per Member State**	37% of IT service providers responding to the public consultation had received requests from customers for local data storage or processing, mostly due to an assumption that they were obliged to do so. The providers stated that they duly inform their clients about the applicable rules, but are still asked by those clients to deliver local storage or processing **Further details – Annex 5**
Illustration – current examples	In a paper presented during the Roundtable 'banking in the digital age', organised by the Commission in November 2016, the European Banking Federation	A software as a service provider specialising in integrated solutions for universities has

[42] Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 (SMART 2014/0031).
[43] An opinion of the REFIT Platform is expected in September 2017).
[44] LE Europe Study (SMART 2016/0016) and TimeLex Study (SMART 2015/0054). Please note that the numbers, descriptions and categorisation of data localisation measures in the studies and this Impact Assessment might differ, since the measures identified by the studies were verified and discussed with the Member States in the context of the structured dialogues before being analysed in the Impact Assessment.

	clearly pleaded for a legal principle on free flow of data, to enable the banking sector to become more efficient.[45] During the Roundtable, a participating bank presented the Commission with the following problem it is experiencing: X bank, a top-10 EU bank, undertook an initiative to increase efficiency, lower costs and improve security through centralisation of IT infrastructures in one Member State, thereby avoiding IT duplication in subsidiaries of the bank. The project was presented to all the national competent authorities concerned for information / approval. All the Central Banks approved the project with the exception of the National Bank of Member State Y, which insisted on local storage based on considerations of distance, the possibility of change of storage configuration in the future and complexity. X bank provided documentation demonstrating low level of those risks. Still, Y National Bank repeatedly rejected the project. As a result, X bank had to maintain redundant IT operations in country Y.	reported that some of their partner universities "believe" that laws applicable to them force them to keep data in their respective countries.
Consequences	The direct consequence is a loss of operational efficiency for X Bank. IT-costs constitute on average 15% of total bank expenditure, which is the second highest cost category (after staff).[46] Moreover, 70% of this spending concerns the operational expenditure (infrastructure and systems)[47]. Research shows that centralisation of IT-systems can lead to 40% of cost reduction on IT operational expenditure.[48] Combining this information, it may be contented that X Bank misses a total cost reduction potential of 4.2% on **overall costs**, at least for the branch in country Y. Indeed, existing evidence shows that diverging data localisation restrictions in the EU lead to IT-inefficiency. 23% of national financial supervisory authorities in the EU states that cloud should never be used by financial institutions, regardless of the type of activity concerned.[49] Nevertheless the ECB mentions that there is large room for improvement of IT-expenditure by EU banks, as the average EU ratio of cost to total assets is 1.4% whereas in the best performing Member State, Sweden, it is just half of that: 0.7%.[50]	The provider deprived of the possibility to scale-up in an important EU market and the ensuing reduction in competitiveness on global markets.

[45] European Banking Federation (2016), "Innovate. Collaborate. Deploy. The EBF vision on banking in the Digital Single Market"
[46] Zeb (2017), "Cutting IT costs in a smart way", accessed via: https://www.bankinghub.eu/banking/operations/cutting-costs-smart-way-swim-aid-cios-pressure
[47] Ibid,
[48] CIO 2010, "Ensure a smooth transition to centralised IT delivery": http://www.cio.co.uk/it-strategy/ensure-a-smooth-transition-to-centralised-it-delivery-3430109/. Examples from banking show that figures can be comparable when migrating systems to the cloud, as the Commonwealth Bank of Australia saved an estimated 30 to 40% through using Cloud: W Kuan Hon and Christopher Millard (2016), "Use by banks of cloud computing: An empirical study"
[49] ENISA (2015), "Secure use of cloud computing in the finance sector"
[50] ECB (2017), accessed via: https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp170614.en.html

Illustration – future examples	The Commission is working on a new initiative to promote digital innovation in health and care[51]. One of the 3 pillars is "Connecting and sharing data and expertise to advance research, personalise health and care, and better anticipate epidemics". Specifically, the diagnosis of rare diseases could be substantially improved by applying analytics to large pools of data gathered from all over the EU, including the use of artificial intelligence technologies. Data localisation restrictions in the health sector are likely to undermine such pooling of data.[52]	Blockchain is a promising new technological approach to data storage and processing. Instead of relying on huge data centres, it distributes data storage and processing to a large (and potentially unlimited) number of computing resources called "nodes". Blockchain already underpins crypto-currencies (bitcoin, ether). Numerous start-ups are working on ways to deploy blockchain in other areas, e.g. recording identities of and operations associated with things connected to the Internet, organising land registries, etc. Widespread market assumption that data localisation is required is likely to be an obstacle to innovations based on the multiple-location blockchain approach.
Consequences	The realisation of the full potential of digital technologies in health and care inhibited.	The realisation of the full potential of technological and business innovation inhibited.
Possibility to solve the problem under the existing framework(s)	Very limited as confirmed by the structured dialogues with Member States and the Commission's own analysis. **For further details, please refer to section 6.3.1.1, Annex 5 and Annex 7**	Limited in view of the challenges identified during the structured dialogues with Member States, complexity of existing frameworks and absence of a clear free movement of non-personal data principle. **For further details, please refer to Annex 5**

3 Why should the EU act?

3.1 Does the EU have the right to act?

Article 114 of the Treaty on the Functioning of the European Union (TFEU) confers on the EU the power to adopt measures, including regulations, which have as their object the establishment and functioning of the internal market.

Removing obstacles to the movement of data across borders and obstacles to the movement of data across cloud service providers / in-house IT systems as well as preventing the emergence of the new

[51] European Commission – Press Release, "Commission launches public consultation on Health and Care in the Digital Single Market", http://europa.eu/rapid/press-release_IP-17-2085_en.htm .

[52] As explained in section 1.4 above, if these restrictions are based on reasons connected with the protection of personal data, the prohibition under the GDPR applies. However, if they are imposed for reasons other than the protection of personal data (e.g. security of storage of the data), the free movement of data provisions of this initiative would apply.

ones would contribute to stimulating a competitive and innovative EU single market for data storage and processing services.

3.2 What would be the added value of action at EU level?

An EU level initiative would address the problem of legal uncertainty by establishing a clear free movement of data principle covering the whole Union and fostering common approaches to and awareness of the legal possibilities to store and process data at the location and using the service or IT system chosen by an enterprise or a public sector organisation.

As demonstrated above, both obstacles to the movement of data across borders and obstacles to the movement of data across cloud service providers / in-house IT systems are widespread in the EU. They concern different economic sectors and have been detected in many Member States.

Therefore, the initiative is a precondition for the development of an innovative and competitive European data economy. It is an enabler of efficient allocation of resources and exploitation of the economies of scale. It is an important factor in creating an environment that attracts foreign investment to the EU. Furthermore, the initiative will give an impulse to economic growth in the EU, leading to GDP gains of up to EUR 8 billion or 0.06%) per year, as a dedicated study estimated.[53] To put these benefits in perspective, they would be on par with recently concluded free trade agreements (FTA), such as the FTA between the EU and South-Korea. EU intervention through this initiative would therefore answer directly to the Commission's overall policy objective of creating jobs and growth for the EU.

EU intervention would also contribute to the development of a safe and trustworthy data space, while avoiding the proliferation of potentially different and conflicting requirements to ensure data availability for regulatory control or security of data storage and processing. This is particularly necessary because data value chains are not bound by territorial borders and are increasingly in operation across different Member States.

A survey on the data economy by Noerr LPP (119 replies covering 20 Member States) revealed that a majority consider that "any regulation must be European, not national".

3.2.1 Subsidiarity

The initiative is fully in line with the subsidiarity principle, because there is no possible action at national, regional or local level that could be more effective than EU-intervention.

Obstacles to cross-border data mobility constitute the core problem underpinning the proposed EU-action. As the cross-border element is obviously a fundamental aspect of this problem, the initiative should be supranational in nature and cannot be tackled at Member State-level.

Member States are able to reduce the number and range of their own data localisation restrictions, but are likely to do so to different extents, at different rates and in different ways or not at all.

Similarly, Member States could take initiatives at national level to set the conditions for switching cloud service providers and porting data between providers and/or users' own IT systems. However, none of these separate actions would induce EU-wide principles. Therefore, they would lead to multiplication of regulatory requirements across the EU single market, hence fragmentation, and tangible additional costs for enterprises, especially SMEs. As stated above, the only way to credibly confront these problems is by introducing general legislative principles at European level. This would provide legal certainty regarding the different intervention areas of this initiative, vis-à-vis both Member States public authorities and the private sector.

[53] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016.

3.3 Consistency with other EU policies and with the Charter of Fundamental Rights

The initiative pursues the objectives set in the DSM Strategy, its recent mid-term review, as well as the Political Guidelines for the current European Commission - "A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change".

Together with the GDPR, the initiative would put in place a comprehensive and consistent EU framework enabling free movement of data in the EU single market as well as movement of data between data cloud service providers and in-house IT systems.

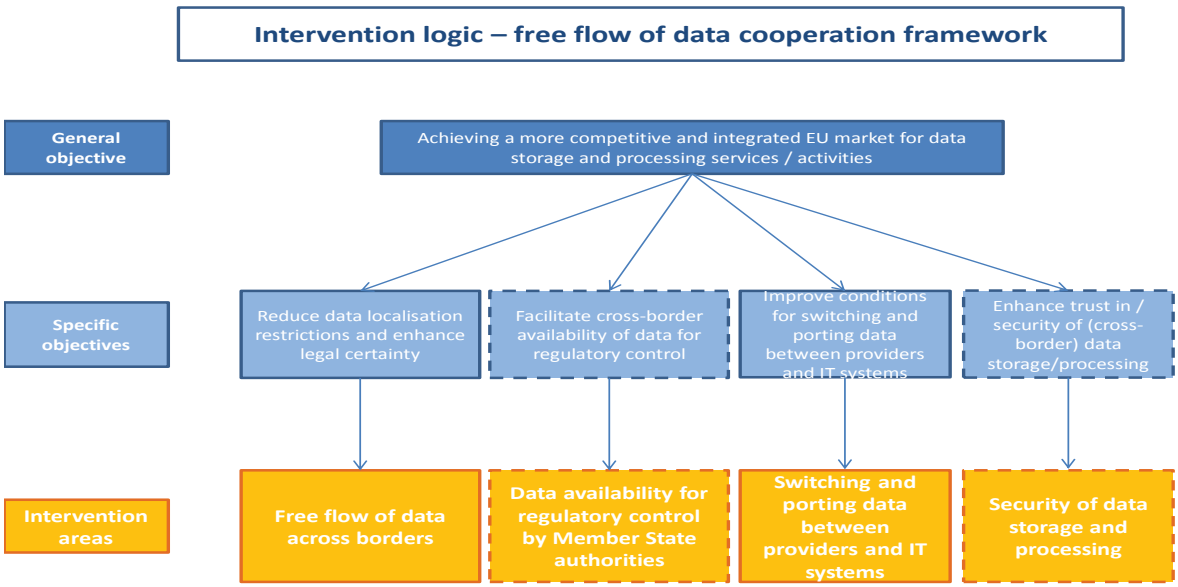
The initiative is consistent with the E-commerce Directive, Services Directive and the Transparency Directive: it pursues the ambition to create an effective EU single market for data-based services, just as those Directives aim at a comprehensive and effective EU single market for services. It is also consistent with the NIS Directive: the NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU; this initiative aims to enhance cyber resilience of cross-border storage and processing of data, relying on the NIS Directive.

The initiative would promote rights enshrined in the Charter of Fundamental Rights. In particular, it would promote the freedom of information (Article 11), since enhancing transparency is an important element of the initiative. The freedom to conduct a business (Article 16) would also be promoted since this initiative would contribute to eliminating and preventing unjustified or disproportionate barriers to the use and provision cloud services as well as configuration of in-house IT systems.

4 What should be achieved?

The following diagram summarises the intervention logic that inspired the proposal, providing the necessary links between the general objective of the intervention, its specific objectives and the intervention areas.

Figure 4 – Intervention logic of the initiative



4.1 General policy objectives

The general policy objective of the initiative is to achieve a more competitive and integrated EU market for data storage and processing services and activities.

4.2 Specific policy objectives

1) Reduce the number and range of data localisation restrictions, enhance legal certainty and transparency of remaining (justified and proportionate) requirements;
2) Facilitate cross-border availability of data for regulatory control purposes, specifically when that data is stored / processed in another Member State, reducing the propensity of Member States to impose data localisation restrictions for that purpose;
3) Improve the conditions under which users can switch data storage and processing (cloud) service providers and port their data to a new provider or back to their own IT systems;
4) Enhance trust in and the security of (cross-border) data storage and processing[54], reducing the propensity of market players and the public sector to use localisation as a default safe option.

The four specific objectives identified are closely linked to the problems described in section 2. In particular:

- The first specific objective targets concrete and existing legal and administrative data localisation restrictions, as well as localisation restrictions that may be adopted by Member States in the future. This would create a more efficient and environmentally friendly data centre sector and effectively address the problem of legal uncertainty as to the existence and scope of application of data localisation restrictions and the extent to which the existing EU rules mandate the free movement of data.
- The second specific objective facilitates the achievement of the first one and is focused on reducing the lack of trust in the free movement of data stemming from Member States' concerns about data availability for regulatory control purposes or data sovereignty.
- The third specific objective targets vendor lock-in situations on the data services (cloud) market.
- The fourth specific objective also facilitates the achievement of the first one. It focuses on enhancing trust through enhanced cyber resilience levels of cloud services in Europe.

4.3 Intervention Areas

To achieve these objectives, four **areas of intervention** have been identified, taking into account the results of the structured dialogue with the Member States and the results of the public consultation:

- Free flow of data across borders;
- Data availability for regulatory control by Member State authorities;
- Switching and porting data between providers and IT systems;
- Security of data storage and processing.

5 What are the various options to achieve the objectives?

Options projecting different levels of intervention are considered: from no EU policy change to low-intensity non-legislative intervention to high-intensity legislative intervention. The nature of the area / objective (core or supportive) is taken into account when formulating and describing the options.

The no change/baseline scenario is being used as the benchmark against which the alternative options should be compared, in line with the provisions in the Better Regulation Guidelines.

[54] In line with but separate from horizontal ICT security frameworks and initiatives.

Discarded options are also mentioned. As prescribed by the Better Regulation Guidelines, section 5 is merely descriptive, while the impacts of the policy options are presented in section 6.

5.1 Discarded options

The option of revising existing EU sectorial legislation (e.g. the INSPIRE Directive[55]) with a view to limiting the scope for unjustified data localisation has been discarded. This is because it would not be able to overcome the significant problem that some data localisation restrictions might not fall within the scope of this legislation, and eventual revisions might not take the free flow of data dimension into account. Limiting the intervention to specific sectors would also ignore the evolving nature of the problem and the need to offer an innovation-friendly legal environment in an expanding data economy.

Other options would be to revise the E-commerce Directive[56], the Single Market Transparency Directive (SMTD)[57] or the Services Directive[58].

However, amending the E-commerce Directive or the Services Directive to introduce the free flow of data provisions would be disproportionate and ineffective. This is because many provisions would have to be modified with the data issue in mind, meaning that such revision would go beyond mere technical adaptation. Secondly the lists of sectors/services excluded from the scope of these Directives, for example important sectors such as transport, telecommunications or healthcare in the case of the Services Directive, would need to be reviewed.

Amending the SMTD would not address data localisation restrictions effectively as the Commission cannot, under that Directive, adopt legally binding decisions requesting the Member States to refrain from adopting the notified requirements.

The GDPR provisions addressing data portability covers only personal data.[59] Provisions would have to be expanded in scope to also cover switching of cloud services providers, which is a different kind of portability as it concerns a change of data processors, which often concerns in practice large volumes of business data. The technical conditions under which portability could take place are therefore distinct in the case of switching cloud providers. Furthermore, cloud services are used in almost every sector. Introducing the principle of switching cloud services providers in sectoral legislation would mean amending a large amount of legislation, and this has not been deemed feasible.

As regards the intervention area of security of data storage and processing, addressing it by means of additional legislative provisions has been discarded in view of the recent adoption of the NIS Directive and the planned initiative on the EU ICT security certification framework.

5.2 Option 0: Baseline scenario - no EU policy change

This option would imply:

- Relying on the Member States to progressively replace data localisation restrictions with less intrusive measures and not to introduce new (unjustified and disproportionate) data localisation restrictions. In practice, notifications under the Transparency Directive would be examined and - although unlikely - infringement proceedings could be launched on a case by case basis where

[55] Directive 2007/2/EC (OJ L 108, 25.4.2007, p. 1–14). The Directive established the Infrastructure for Spatial Information for the purposes of Union environmental policies. See the 2016 Report and REFIT evaluation: http://inspire.ec.europa.eu/news/commissions-inspire-report-and-refit-evaluation-published.
[56] Directive 2000/31/EC (OJ L 178, 17/07/2000, p. 1-16).
[57] 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 (Text with EEA relevance) (OJ L 241, 17.9.2015, p. 1).
[58] Directive 2006/123/EC (OJ L 376, 27.12.2006, p. 36–68).
[59] GDPR, Article 20.

strong evidence can be gathered to show that the restriction has a direct and significant impact on the cross-border provision of a service.

- That Member State authorities seeking data stored or processed in another Member State would continue to rely on (i) requests addressed to the subject of regulatory oversight / holder of the data as well as (ii) formal judicial cooperation requests and / or (iii) other cooperation / assistance frameworks where these exist, and which are of varying scope and degrees of effectiveness / efficiency.

- Relying on market players to introduce technical and contractual conditions progressively to enable data portability and facilitate the switching of data (cloud) service providers.

- Relying on the NIS Directive and related instruments to provide a benchmark for a common level of security of data storage and processing.

5.3 Option 1: Non-legislative initiatives to promote trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

This option would:

- Provide guidelines on the existing EU instruments relevant to data localisation restrictions, their scope of application, applicable provisions and exceptions as well as best practices in addressing the functional requirements underpinning data localisation (including guidelines on data availability for regulatory control by Member State authorities and security of data storage and processing).

- Imply a strengthened enforcement of existing EU legislation vis-à-vis different categories of unjustified or disproportionate data localisation restrictions imposed by Member States, e.g. by giving priority to the preparation of this type of cases.

- Encourage Member States, e.g. by means of transparency mechanisms under existing legislation, to enhance the transparency of (justified and proportionate) data localisation restrictions as well as any requirements concerning data availability for regulatory control by Member State authorities and security of data storage and processing.

- Foster regular discussions between Member State representatives and the Commission on issues that may be identified regarding the availability of data for regulatory control by Member States' authorities and ways to resolve them, using existing (sectoral) guidelines, and cooperation mechanisms such as these listed in **Annex 8**.

- Provide EU-level guidelines on best practices in facilitating switching cloud service providers and porting data to a new provider or back to users' own IT systems.

- Encourage self- and co-regulation by market players to work out the technical and contractual conditions of switching / data porting, as well as data security.

5.4 Option 2: Principles-based legislative initiative and cooperation framework to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

This option would:

- Lay down the principle of free flow of data within the EU requiring Member States not to put in place unjustified or disproportionate data localisation restrictions. Under this Option, in principle all data localisation restrictions for reasons other than protecting public security would be considered unjustified or disproportionate restrictions. It would require Member States to notify any new data localisation restriction they intend to put in place by means of the existing notification scheme of the Transparency Directive and to carry out a review of / notify existing measures during a transitional period; ensure transparency and proportionality of remaining (justified) data localisation restrictions.

- Lay down the principle whereby a user of a data storage and/or processing service that is subject to regulatory oversight or regulatory compliance obligations shall not deny access to data to a competent authority of a Member State that has the right to obtain the data for regulatory control purposes when the data is stored and/or further processed in another Member State. It would provide for cooperation between the Member States on obtaining access to the data where existing cooperation / mutual assistance frameworks cannot be relied on as well as an implementing act laying down details of the procedures for the cooperation on obtaining access to data.

- Lay down the principle that data storage and/or processing service providers should facilitate data porting for switching providers or porting data back to users' own IT systems; require that cloud service providers explain in a sufficiently detailed, clear and transparent manner (including in contracts) the processes (e.g. scope, exit plan and support services), technical requirements (e.g. data formats and supports), timeframes and charges that apply in those situations as well as the extent of a data return guarantee in the case of bankruptcy; encourage self-regulation to work out the detailed technical and legal conditions of switching / data porting.

- Identify and develop reliable common standards and/or requirements for the security of storage and/or processing of data. In particular, a cloud-specific EU-level set of binding requirements could be established in an implementing act. In practice, the Commission would work with the DSM cloud stakeholder platform[60] to prepare ground for the future cloud-specific requirements.

- Envisage the designation by each Member State of a single point of contact, who shall be responsible for coordinating the application of this Regulation in the Member State and, specifically, coordinate the cooperation on access to data.

- Establish an expert group composed of the single contact points. The group could advise on a consistent application of the principles in all Member States. It could exchange experience and good practice regarding the removal of data localisation requirements and the cooperation of competent authorities for the purpose of ensuring data availability for regulatory control purposes as well as give opinions on, and develop model contracts or guidelines facilitating data availability. It could meet and coordinate with data protection and cyber security authorities and sectoral regulators as needed. It could discuss and engage in raising awareness of the free movement of data principle.

The principles-based legislation would be detailed and made operational using several instruments: the notification and transparency requirements, implementing acts (in all the intervention areas of this initiative except for the free flow of data across borders), advice and opinions of the expert group and self-regulation.

Sub-option 2a

In view of the different nature of the various intervention areas of this initiative (as defined in section 4.3), a sub-option to Option 2 was developed to allow for the assessment of a combination of binding substantive provisions establishing the free flow of data principle and ensuring access to data for regulatory control purposes on the one hand, and softer measures for data porting and security of data storage and processing on the other hand.

Specifically, this sub-option is based on the elements described above for Option 2, except that:

- for data porting upon switching providers or porting data back to users' own IT systems, it would not put a legal obligation on data storage and/or processing service providers to facilitate data

[60] The recently created Digital Single Market cloud stakeholder platform will provide for a stakeholder engagement platform with the purpose of interacting with the broadest possible collection of stakeholders in order to ensure valuable and multi-perspective participation and commitment on the various current and emerging issues along the cloud computing value chain. The objective of the DSM cloud stakeholder platform is to contribute to the development of a European cloud ecosystem and provide input for imminent EU policies in the context of the Digital Single Market. Its main workstreams envisaged are data (cloud) security and certification, and portability/switching of cloud providers. The preparatory meeting took place on 29 June 2017. See further http://netfuturesconference.eu/cloud-stakeholders-kick-off-meeting/

porting, but it would require the Commission to encourage service providers to develop self-regulatory codes of conduct.

- for the security of data storage and/or processing, it would merely provide for the clarification that any existing security requirements for companies continue to apply to them, regardless the location in the EU where their data is stored or processed and also when this is subject to outsourcing to a cloud service provider.

5.5 Option 3: Detailed legislative initiative to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

This option would:

- Establish pre-defined (harmonised) assessments of what constitutes (un)justified and (dis)proportionate data localisation restrictions as well as a detailed mechanism to ensure transparency of white-listed data localisation restrictions (dedicated platform).

- Establish a horizontal, cross-sector mandatory cooperation framework to enforce access rights of public authorities to data when it is stored and/or processed in another Member State: competent authorities, deadlines, common request / response templates would be specified.

- Establish both the obligation to facilitate switching / porting and harmonise the key technical and legal conditions (e.g. concerning types of data, usable formats / structures, timeliness). It would require cloud service providers to explain in a sufficiently detailed and accessible manner (including in contracts) the processes (e.g. scope, exit plan and services), technical requirements (e.g. data formats and supports), timeframes and charges that apply in those situations.

- Develop common standards and a European certification scheme for the security of storage and processing of data and mandate its use.

- Envisage implementing acts in all the intervention areas of this initiative and a dedicated Committee[61].

Figure 5 - Summary of measures envisaged by the options in the four intervention areas:

Intervention areas / Options	Free flow of data across borders	Data availability for regulatory control by Member State authorities	Switching and porting data between providers and IT systems	Security of data storage and processing
0-Baseline	-	-	-	-
1- Non-legislative initiatives	Guidelines, enforcement, transparency	Guidelines	Guidelines, self/co-regulation	Guidelines
2- Principles-based legislative initiative and cooperation framework	Legal principle, notification, review, transparency, awareness	Legal principle, MS cooperation, comitology, awareness raising	Legal principle, transparency, self/co-regulation, , comitology,	Standards, cloud-specific requirements, comitology, awareness

[61] As defined by Regulation No. 182/2011 of 16 February 2011, laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

	raising		awareness raising	raising
	← *single contact points, expert group* →			
2a	Same as 2	Same as 2	Self/co-regulation, comitology, awareness raising	Enhancing legal certainty on applicable security requirements.
3- Detailed legislative initiative	Harmonisation, transparency, comitology	Mechanism, comitology	Legal principle and conditions, transparency, comitology	Standards, certification, comitology

5.6 Choice of legal instrument

The realisation of Option 0 does not require a new legislative instrument.

Option 1 could take the form of a new Commission Recommendation(s).

Options 2, 2a and 3 could take the form of either a Directive or a Regulation. They would be best implemented through a Regulation, since it would ensure that the new rules are applicable in all Member States at the same time as well as a uniform approach in the EU's entire single market, which is particularly important to guarantee the legal certainty to enterprises and public sector organisations concerned.

Also, as demonstrated before, at least two of the three drivers to the basic problem of obstacles to data mobility (legal uncertainty and lack of trust) are underpinned by important psychological elements. Therefore, these problem drivers can best be solved by introducing clear principles in a Regulation and subsequently raising awareness about them.

A Directive, while also representing a legislative approach, could solve the lack of trust to a certain degree, maintain some flexibility as regards implementation and would fit with a principles-based approach. However, it would bring less legal certainty, and the time period between adoption and the start of implementation would be longer due to the need to transpose a Directive into the national laws of Member States.

The public consultation showed that a majority of participating stakeholders (55.3% of respondents) believe that legislative action is the most appropriate instrument to tackle unjustified localisation restrictions, with a number of them calling explicitly for a Regulation[62]. IT service providers of all sizes, both from the EU and abroad, show the highest support for regulatory action. In a written answer to the public consultation, one of them explained its position: "Without a concrete legislative instrument, Member States may not be incentivized to change laws to remove existing data localization measures. Worse, they may continue to enact new ones."

Most respondents see a combination of a legislative instrument and increasing the transparency of justified restrictions as the most appropriate option. They generally make the same argument, referring to increased legal certainty and trust.

Respondents also took the view that a Regulation would send the strongest signal to the international community, showing that the EU takes leadership on the free movement of data. As

[62] 289 stakeholders participated in this multiple-choice question of the public consultation. Respondents were not asked about *the type of* legislative action, but 12 stakeholders, on their own initiative, took the possibility to explicitly call for a Regulation in a written comment. This stakeholder group was of a diverse nature, consisting of 2 Member States, 3 business associations, 6 IT service providers and a law firm.

there are already data localisation restrictions currently in place, a number of these respondents also call for transparency on the approach to those existing restrictions.

6 What are the impacts of the different policy options and who will be affected?

6.1 Approach and impact categories

The following impact analysis is based on the results of the public consultation, the structured dialogues with the Member States and other stakeholders, studies funded by the European Commission, several analytical tools developed by the European Commission[63] and publicly available information. Most of these sources provide qualitative rather than quantitative insights. The sections below will assess the impacts of the policy options presented in section 5, considering the following impact categories:

1. Economic impacts
2. Environmental and social impacts
3. Impacts on Member States' public authorities

For each category, impacts are also reflected from stakeholders' points of view, on the basis of feedback received during the various steps of assessment (a more detailed assessment of impacts on specific stakeholder categories is provided in **Annex 3):**.

4. Stakeholder views

6.2 Option 0: Baseline scenario - no EU policy change

6.2.1 Economic impacts

6.2.1.1 Free flow of data across borders

Under this option, Member States would have **wide discretion to put in place new data localisation restrictions and maintain the existing ones**. This discretion is constrained by (i) the Treaty provisions on the free movement of services and the freedom of establishment; (ii) relevant EU secondary legislation, notably the e-Commerce Directive and the Services Directive and (iii) the Commission's actions to ensure the effective implementation of the Treaty provisions and the legislation, notably through infringement proceedings.

These **legal constraints are only partially effective**, since they either (i) do not cover all the types of data storage or processing activities addressed in this Impact Assessment (e.g. many are excluded from the scope of application of the e-Commerce Directive and/or the Services Directive) or (ii) could only produce tangible results in the long term. For example, infringement proceedings take on average 4-5 years[64] until they result in a court ruling. Before such judicial clarification legal uncertainty would prevail, leading users of data-based services to demand local data storage and/or processing from the service provider (60% of European IT service providers who participated in the public consultation of 2017 indicated that their customers have demanded local storage of their data) and harming the prospects of the fast-developing data economy. **See section 6.3.1.1 (infringements text box) and Annex 5 for more details**.

Outcome of the structured dialogues with Member States:

[63] *e.g.* the "Institutional Cost Estimation tool" used to calculate Full Time Equivalent cost parameters, developed in the the support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005).

[64] From the launch of the proceeding to the EU first instance court ruling. See http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/infringements/index_en.htm and https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-02/cp170017en.pdf

In the case no substantial EU-level policy action were undertaken, as would be the case under Option 0, some Member States that believe in and support free movement of data across borders can remove some data localisation restrictions, possibly even unilaterally. For instance, Denmark changed its Bookkeeping Act already in 2015 to replace the requirement to obtain an individual authorisation to keep data abroad with a functional requirement to provide an online access to Danish supervisory authorities.

Nevertheless, as a result of the structured dialogues, only a few Member States are expected to do so without any EU-level policy action, depending on their national policies. This would lead to an unequal regulatory landscape and an unequal level playing field for businesses in the EU.

In addition, Member States may have different views on which categories of localisation are unjustified. For example, the same Member State as mentioned above, Denmark, maintains some other localisation restrictions concerning public sector data / registries.

Option 0 implies that when making business decisions about data storage or processing activities (notably, their location) **cloud service providers** have to take into account data localisation restrictions as opposed to a market-driven approach. In particular, cloud service providers have to (i) build local data centres even if the provider could serve its users from a data centre located elsewhere or (ii) choose less ideal locations for planned data centre infrastructures or (iii) outsource processing activities to more expensive local service providers. These factors have a **direct effect** on the choice of location and could result in additional costs for cloud service providers, posing a constraint for the **operational efficiency** of the industry.

Deploying cloud data centres beyond the needs dictated by the market, or limiting choices for the location of a planned data centre can have serious **cost implications**. The table below shows a comparison of typical data centre lifetime[65] costs in the EU 28 Member States (excluding land costs and capital costs associated with servers and other equipment)[66]. The EU average is 276.9 million €, the most expensive location is Belgium (421.4 million €), and the cheapest location is Bulgaria (81 million €). This additional cost cascades down the value chain to the consumer eventually.

Figure 6 - Ten year lifetime costs for cloud data servers in EU28 Member States

	Construction and ten years of operating costs €m	Rank
EU28 average	276.9	
Austria	350.8	7
Belgium	421.4	1
Bulgaria	81.0	25
Croatia	145.0	19
Cyprus	n/a	
Czech Rep.	185.1	16
Denmark	356.9	5
Estonia	144.0	20
Finland	318.4	10
France	339.1	8
Germany	324.8	9
Greece	187.9	15
Hungary	164.9	18
Ireland	356.9	4
Italy	301.3	12
Latvia	127.9	22

[65] The typical lifetime of a data centre is 10 years, with servers being replaced every 3 to 5 years

[66] time.lex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (SMART 2015/0054).

Lithuania	116.8	23
Netherlands	356.8	6
Poland	130.2	21
Portugal	213.1	13
Romania	88.0	24
Slovakia	178.8	17
Slovenia	205.7	14
Spain	306.2	11
Sweden	389.8	2
UK	359.4	3

(Source: Timelex, Spark 2016)

The proliferation of data localisation restrictions would mean that organisations carrying out data processing activities in several Member States and using in-house IT systems for that purpose would need to set up dedicated data storage or processing IT systems for those Member States imposing restrictions.

It could be argued that Option 0 would protect (small) cloud service providers operating in Member States with data localisation restrictions from foreign **competition**. However, the competitiveness of all cloud service providers operating in multiple territories would be curtailed by the lack of possibility to benefit from economies of scale.

Clearly, a much more likely outcome in terms of competitiveness, especially in the medium term, is that large cloud service providers active in multiple territories will serve some of the markets of the Member States imposing data localisation restrictions.[67] The real reduction in competitiveness will be seen by **smaller providers and SMEs** that have spare capacity to serve foreign users and export their services but are not able to do so due to data localisation restrictions.

As regards organisations using in-house data storage or processing IT systems, the reduction in competitiveness is likely to affect those organisations that are based in the Member States where the costs of installing and running such IT systems is relatively high and that compete with market players from other Member States (e.g. banks).

The public consultation highlighted that localisation restrictions drive up the **cost of setting up a new business**. Several respondents maintained that if scaling across Europe is more expensive than scaling globally, start-ups will continue moving to other parts of the world to scale there. A recent study procured by the Commission indicates that 1 out of 7 European scale-ups move their headquarters abroad. 83% of them choose the United States, of which a majority ends up in Silicon Valley.[68] Option 0 would not be able to counter this trend and would therefore lead to a loss of growth and innovation potential for the European economy.

6.2.1.2 Data availability for regulatory control by Member State authorities

The economic impacts of this option are expected to be mostly of qualitative and indirect nature. Option 0 does not foresee any type of cooperation mechanism or legislative action so it is likely to reiterate some of the problems highlighted in section 2 concerning the causes and effects of lack of trust.

Even in the absence of any type of intervention the data market will continue to evolve and cross-border data flows will continue to increase, only at a slower pace. IMF data from 2008 to 2012

[67] See London Economics Europe, "Facilitating cross border data flow in the Digital Single Market", 2016 (SMART 2015/0016), pp..35-36 and this overview http://uk.advfn.com/stock-market/NASDAQ/GOOGL/share-news/U-S-Tech-Firms-Dominate-Cloud-Services-in-Western/72136481

[68] Europe Direct 2017, "Study on transatlantic dynamics of new high growth innovative firms" accessed via: http://ec.europa.eu/research/innovation-union/pdf/expert-groups/rise/transatlantic-dynamics_final-report.pdf

present cross-border information flows as the fastest growing component of US as well as EU trade[69]. For more information on the magnitude of cross-border data flows see **Annex 9**. Governments are likely to face an increase in requests for access to data aimed at other jurisdictions, resulting in increased **administrative burden**.

Under Option 0, the lack of trust via-a-vis cross-border storage would persist, altering market dynamics and the choice of market operators and having an indirect effect on their **operational efficiency**. This lack of trust will foster market fragmentation for data storage, **hampering innovation and competitiveness** of the companies in the market. The upstream market structure (cloud service providers) would be distorted by the survival of less efficient companies exploiting localisation restrictions in order to be able to maintain higher prices. The costs would be passed on to the **downstream market** (business users).

If Option 0 leads to high administrative burdens, the impact on economic operators will be cost inefficiency, suboptimal allocation of resources and hence limited growth and competitiveness.

Switching and porting data between providers and IT systems

Vendor lock-in practices have several economic impacts, as cited in the survey on switching cloud providers[70] and in the responses to the public consultation[71]. These would persist under Option 0.

Macro-economic impacts
In the dedicated study 'Switching Cloud Providers'[72] that was conducted on behalf of the Commission, the possible effect on the growth of cloud computing in Europe is described for Option 0, forecasting demand for public cloud to grow by 18.7 % Compound Annual Growth Rate during the period 2018-2025, and reaching €64.9 billion in 2025. That is less than the baseline market prediction of an authority in the cloud computing sector, projecting a CAGR of 23% annually until 2020 for cloud services.[73] Still, the study predicts this even **lower than baseline growth scenario** under Option 0, as SMEs would continue to lag behind larger companies in the take-up of public cloud, resulting in an unequal level playing field. National governments could also take independent action to support data portability in cloud switching, creating fragmentation in the EU cloud market.

Impacts on business users of data storage and processing services
In the situation currently existing on European markets, which Option 0 leaves unchanged, the technical and contractual difficulties with switching can lead to **excessive portability costs** for business users of cloud services**.** As evidenced by the dedicated study mentioned above, these costs are relatively much heavier for smaller business users, sometimes even higher than the total annual runtime cost of the cloud service itself.

There are different categories of portability costs, such as – but not limited to:

- Data egress cost (i.e. the amount charged for data traffic out of the premises of the CSP);
- Transport fees for transporting the data to its new location;
- Cost of downtime;
- Cost of concurrent cloud use (during the porting process);
- External expertise and/or internal resource costs.[74]

[69] Aaronson, Susan Ariel, "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", 2015.
[70] IDC and Arthur's Legal, "Switching Cloud Service Providers", 2017 (SMART 2016/0032).
[71] Public Online Consultation on Building a European Data Economy (10 January 2017 – 26 April 2017).
[72] IDC and Arthur's Legal, "Switching Cloud Service Providers", 2017 (SMART 2016/0032).
[73] IDC, Cloudview 2016
[74] IDC and Arthur's Legal, "Switching Cloud Service Providers", 2017 (SMART 2016/0032).

Whereas the exact portability costs always depend on, firstly, the complexity of the digital architecture used and, secondly, the amount of data stored, one element does not change: the cloud customer is completely dependent on the cloud service provider regarding the technical capabilities of the provider to export the data from its premises. The method of data egress does not only affect the transport costs, but also the costs of downtime and concurrent cloud use, because exporting the data of a mid-sized company, when using 'ordinary' internet-browsing speeds, can take months.

The study provides estimations of the height of these costs, modelled to three different use cases: a **simple** case (a relatively simple application of an entrepreneur running the equivalent of under ten PCs and some simple office programs in the cloud), a **medium-complex** case (a commercial application (cloud capacity of the equivalent of <100 PCs, running a large database such as a CRM system) and a **complex** case (an enterprise application landscape of approximately 350 equivalent PC's with distributed data sources). The following figures extracted from the study's analysis show that the 'simple' case users – representing typically smaller business users such as start-ups or SMEs – relatively face the highest portability costs:

	Portability cost (p.c.)	**Yearly runtime cost (y.r.c.)**	**p.c. relative to y.r.c.**
Simple	18.800 EUR	15.000 EUR	125%
Medium Complex	119.400 EUR	120.000 EUR	99.5%
Complex	231.400 EUR	600.000 EUR	38.6%

This example shows that portability costs may become prohibitive, especially for smaller business users, because they can amount to higher than the yearly runtime cost of the service itself. It can be concluded that this in practice leads to a **high degree of vendor lock-in**.

6.2.1.3 Security of data processing

The baseline scenario in the area of security of data processing entails relying on the NIS Directive and related instruments to provide a benchmark for a common level of security of data storage and processing. The evidence that was gathered points to data being more secure when kept in the larger data centres of cloud service providers, as these are often much better equipped in terms of security systems. Therefore, the negative indirect effect from the status quo is linked to the assumption that companies (especially SMEs) that are affected by data localisation restrictions may choose not to store data in the cloud.

When data is stored on-site, the security risks for business end-users are higher, while at the same time more expensive as well[75]. The NIS Directive provides a risk-based approach to security but does not address the cost problem. Some cloud service providers in more closed economies may therefore exploit the existence of data localisation restrictions to raise their prices, at the expenses of business users in the downstream sector.

Moreover, existing legislation and policy does not address security concerns of data storage/processing specifically, for instance by introducing certification. This would not solve the current uncertainty about the security of cloud use.

Therefore, the presence of data localisation restrictions and the limited degree of collaboration in security matters in the baseline scenario looks unlikely to solve the problems discussed in the problem definition section.

The respondents to **the public consultation** have highlighted the importance of allowing free flow of data without restrictions for keeping data storage and processing secure. As one respondent

[75] London Economics Europe, "Facilitating cross border data flow in the Digital Single Market", 2016 (SMART 2015/0016) and EC Consultation on the regulatory environment for data and cloud computing, May 2016.

noted: "*We deliver two major updates a year and smaller updates on a weekly basis, with all of our customers always on the same version. Enabling cross-border data flows enables greater adoption of cloud computing, with these benefits that are lost with multiple instances or hybrid solutions. Having a single privacy and security model and having everyone on the same version makes it easier to protect data, add new functionality, and reduces complexity enhancing ease of use for customers"*. It seems unlikely that a no-action scenario will help to improve the security of the data processing.

6.2.2 Environmental and social impacts

6.2.2.1 Free flow of data across borders

No positive **environmental impacts** are to be expected under Option 0.

In general, a free flow of data has positive **environmental impacts**, because it will allow cloud service providers to locate their data centres in locations where there are substantive energy efficiency gains to operate such infrastructures. These locations are typically locations in lower temperature zones[76], as they allow energy savings on cooling servers. [77] Cooling may account for up to half of a data centre's power expenditures, so this issue of large importance for the sector and may therefore have sizable impacts in terms of environmental footprint. [78]

It is true that many factors play a role in the decision on where to situate a data centre (such as proximity to clients and access to a pool of human resources who have the skills to operate the data centre). Still, it is important to highlight that data localisation restrictions may have an impact on the location choice, skewing it towards less environmentally optimal locations.

Because the baseline option would allow for the persistence of data localisation restrictions by Member States and through market dynamics, it would therefore have a negative impact on the environment.[79]

Proliferation of data localisation restrictions could also hamper the development of innovative approaches energy optimisation or efficiency in data centres, e.g. maximising the use of renewable energy by shifting the loads of data processing to a data centre where renewable energy is available at a particular moment.

In terms of **social impacts**, the baseline option would lead to an increase in employment in Member States that have introduced or will introduce data localisation restrictions, because of supervision or operating needs of new infrastructure. The positive impact of such jobs is likely to be limited, since cloud service providers deploy only the limited capabilities needed to serve customers in those Member States.

In addition it must be noted that the data skills gap is expected to increase to more than 16% over the next four years totalling a number of unfilled positions of almost 770,000. In particular some of the largest and most advanced EU economies will face a considerable skills gap whereas smaller and less developed economies will witness an oversupply of data workers.[80] Therefore, it can be presumed that non-effective policy measures not sufficiently addressing either, existing or

[76] Time.Lex Study (SMART 2015/0054), Economic analysis of costs for cloud data providers in meeting data location restrictions, p.9

[77] In general, data centres situated in Nordic countries with abundant renewable energy are more environmentally-friendly than the data centres situated within cities in countries with a lot of "brown" energy in the energy mix.

[78] Cooling may account for up to half of a data centre's power expenditures, see Oxford Research "A springboard for green data centers in Southern Norway", p.8. Water is another resource used for cooling, see Justin Morton, "Data Centers' Water Use Has Investors on High Alert", Bloomberg, 5 August 2016, available at: http://www.bloomberg.com/news/articles/2016-08-05/data-centers-water-use-has-investors-on-high-alert

[79] Electricity use by data centres is one of the fastest-growing sources of greenhouse gas emissions globally, see Susanne Goldenberg, "Social media explosion powered by dirty energy, report warns", The Guardian, 2 April 2014, https://www.theguardian.com/environment/2014/apr/02/social-media-explosion-powered-dirty-coal-greenpeace-report

[80] Idem, p.198

potentially emerging limitations to the free flow of data would promote directly or indirectly a concentration of data skills demand. This will consequentially also affect negatively the data skills gap.

Another possible negative social impact could incur on the freedom to conduct a business provided for by Article 16 of the European Charter of Fundamental Rights, since it would result in (a growing number of) limitations constraining (i) business choices regarding the location of data storage or processing infrastructures and (ii) the opportunities for cloud service providers to serve customers in other Member States.

6.2.2.2 Data availability for regulatory control by Member State authorities

As there would be no significant action to improve data availability for regulatory control by Member State authorities envisaged by this option, no change in cross-border data mobility can be expected and consequently, no positive environmental impacts. Through inaction, it would mean a missed chance in terms of improving the environmental footprint of data centres.

As explained in section 6.2.2.1 above, a free flow of data is beneficial for the environment through increased liberty for service providers to locate their data centres in more environmentally optimal locations. Policy action on improving data availability to Member State authorities for regulatory control purposes would increase cross-border data mobility because of raised levels of trust, both by market participants and by Member States authorities.

Therefore, the reader is referred to section 6.2.2.1 as it applies similarly for the intervention area of availability.

6.2.2.3 Switching and porting data between providers and IT systems

The baseline option would leave it to the market to implement energy efficient solutions. If the lack of interoperability between cloud services is allowed to persist, this would make it necessary for companies wanting to switch providers to spend more resources and processing power to migrate their data, which could have a negative environmental impact.

Apart from the issues of continued market distortion, and leaving SMEs and start-ups in a weaker position, there are no social impacts of this option, although certain negative regional policy effects of localisation can be quite important on a local level, such as the lack of scaled investments because of fragmented service provision.

6.2.2.4 Security of data processing

Cyber threats pose significant environmental and social risks. As more and more data of critical infrastructure or industry working with dangerous substances are moved to the cloud, state-of-the-art security of data processing and storage facilities is of utmost importance to keep environmental and social dangers to a minimum. In this respect, security breaches could lead to accidents in manufacturing processes and/or the release of dangerous or polluting substances. The policy options presented in this area do not cause direct environmental or social impacts. Nevertheless, it can be argued that because it is most likely that this option will not lead to a higher level of security (through better coordination between Member States' authorities and the establishment of common standards), it will not have the potential positive social and environmental impacts that the other policy options constitute.[81].

[81] Examples of potential environmental impacts are:

- Cyber intrusions that lead to contaminant releases, resulting in damage to human health and the environment
- Cybercrimes causing catastrophic spills, waste discharges and air emissions that result in bodily injury, property damage, environmental remediation expense and significant legal liability claims

See XL Catlin Group, "Environmental Risks: Cyber Security and Critical Industries" (Whitepaper), 2013.

Social impacts concern the disclosure of information that can pose harm to individuals.

As the baseline option does not foresee the development of cloud-specific security guidelines, it may be argued that of all policy options, this option constitutes the highest environmental and social risks.

6.2.3 Impacts on Member States' public authorities

6.2.3.1 Free flow of data across borders

The baseline option would not produce specific impacts on Member States' public authorities in the intervention area of free flow of data across borders (in particular, potential infringement proceedings relating to data localisation restrictions could be dealt with in the context of existing administrative arrangements).

6.2.3.2 Data availability for regulatory control by Member State authorities

There are several inter-state cooperation mechanisms in existence, allowing Member States to exchange information in relation to specific administrative/judicial procedures, and specific data types, subject to various conditions.[82] For scenarios not covered by these instruments, Member States can engage in bilateral or multilateral interaction, with potentially diverging procedures to follow in different exchanges, and multiplied administrative efforts. As outlined above with regard to the economic impacts, without establishing and strengthening obligations on private actors to make the data available and promoting Member States' cooperation, a projected rise in cross-border data services and requests for access to data would exacerbate such administrative burden.

6.2.3.3 Switching and porting data between providers and IT systems

As the baseline option relies on market players to progressively introduce technical and contractual conditions facilitating switching data of cloud service providers, it is not expected to incur direct administrative burden on national public authorities under the baseline option.

However, relying completely on market participant to introduce such conditions could constitute a lack of guidance and therefore cause disproportionately dominant market positions for large tech companies. This could lead to indirect administrative burdens in the form of an increased number of cases referred to Member States' competition authorities.

6.2.3.4 Security of data processing

The baseline scenario does not lead to direct burdens for Member States' public authorities, as it relies on existing instruments like the NIS Directive. It is likely that such existing instruments will not establish specific security benchmarks for cloud services, as their necessary purpose is to create a generic framework. However, if such common security criteria would not be instituted this could in the future lead to burden for Member States authorities as a result of the collective risk this poses to their societies.

6.2.4 Stakeholder views

6.2.4.1 Free flow of data across borders

The majority of stakeholders voiced its support for a legislative principle on the free flow of data. They did so by means of the online public consultation, during the structured dialogues organised by the Commission or by submitting position papers for scrutiny. 61.9% of respondents to the public consultation indicated that data localisation restrictions should be removed and, as mentioned in section 5.6, 55.3% argued for a legislative approach in doing so. Moreover, stakeholders have

[82] Please refer to Annex 8 for a detailed list and analysis of these cooperation mechanisms.

indicated their concern about data localisation restrictions that are currently in place or that are perceived by the market.

As Option 0 would rely on Member States to progressively replace data localisation restrictions with less intrusive measures, this option would not address either of these two concerns raised by stakeholders. It does not propose actions to remove existing and perceived data localisation restrictions, and it would also be unable to avoid the emergence of new data localisation restrictions, following the trend witnessed in the European Data Economy communication of the European Commission.

6.2.4.2 Data availability for regulatory control by Member State authorities

Concerning the intervention area of data availability, stakeholders hold that national competent authorities uphold data localisation restrictions for the objective (in itself legitimate) of keeping data available for supervision or control purposes. In **the public consultation**, 77.4% of respondents indicated that localisation demands were rooted in compliance concerns vis-à-vis local legal or administrative requirements.

As Option 0 neither includes clear EU-level guidance on the abatement of data localisation restrictions, nor provides guidelines or tools for Member States authorities to ensure availability of data processed in another Member State, there is no reason to conclude that these (frequently defined by sector) localisation restrictions would be mitigated by Option 0.

6.2.4.3 Switching and porting data between providers and IT systems

56.8% of SME respondents who intended to switch providers indicated in **the public consultation**[83] that there are important barriers to data portability. This is echoed also by participants from the 18 May 2017 workshop on cloud switching[84], which included representatives of the cloud industry and their business customers. It is evident from the stakeholder engagement that there is an expectation for the EU to act to improve data portability in order to facilitate switching of cloud services providers. Option 0 would not meet this expectation.

6.2.4.4 Security of data processing

Stakeholders have expressed considerable concerns about the security of data processing. The main argument made by stakeholders[85] is that security of data processing would benefit from a free flow of data legal principle. There were zero stakeholders arguing the opposite. The reason behind this is that hosted cyber security services are typically provided remotely, from operation centres located in strategic places around the globe to be able to benefit from 24/7 security incidents reporting. In the case incidents are detected, these services will typically upload security updates at once on IT-systems of many users worldwide.

Considering that stakeholders' views were not conflicting on this issue, their judgment suggests that Option 0 is suboptimal, as it would not include any policy action to ensure enhanced data mobility in Europe.

[83] See Annex 2
[84] Ibid.
[85] This argument was expressed mainly by specialists on the topic, like cyber security service providers, but also by business users.

6.3 Option 1: Non-legislative initiative – guidelines, strengthening enforcement of existing EU rules and enhancing transparency

6.3.1 Economic impacts

6.3.1.1 Free flow of data across borders

The economic impacts of this option **would not vary much compared to the baseline scenario**, as the intervention in this case would be based on a non-legislative and little binding policy action. It does not guarantee any change in data localisation by business actors driven by market dynamics through legal uncertainty and does not promote consistency of treatment across the single market.

Option 1 would foresee strengthened enforcement of existing legal instruments to minimise negative effects of data localisation. However, this would not solve the problem of legal uncertainty and still leave gaps for new localisation restrictions. One IT service provider specifically mentioned this in a written answer to **the public consultation**: "*Only a legislative instrument can remove these barriers; ensure they are not re-instated and that new ones are not introduced; and provide sufficient certainty to providers and users in the longer term. While there are already some relevant legislative instruments in place (e.g., the Services Directive and the E-Commerce Directive), none of these set forth a comprehensive prohibition on the maintenance of unjustified obstacles to the free flow of data. Guidance, or mere identification of the data localisation measures, while helpful, will not be as effective.*"

Also, it would largely **preserve Member States' discretion to put in place new data localisation restrictions and maintain the existing ones**.

Outcome of the structured dialogues with Member States:

Soft approaches could persuade some Member States to lift some data localisation restrictions. For instance, France revised Act number 2002-303 and the French Public Health Code which oblige hosting service providers to be approved by the Shared Healthcare Information Systems Agency within the Ministry of Health in order to be allowed to undertake hosting activity for patient data. From 2019 the strict prior authorisation requirement will be replaced by a certification requirement. In Germany, the initial draft "social network" law contained data localisation restrictions, but those were taken out as deliberations on the draft law progressed.

In particular, as explained below, it would still be **difficult to pursue infringement proceedings** targeting data localisation restrictions.

Factors making infringement proceedings against data localisation restrictions difficult to pursue

The Commission has recently announced that it would pursue infringements "in a strategic way to focus and prioritise its enforcement efforts on the most important breaches of EU law affecting the interests of its citizens and business."[86] In particular, economic and systemic (cross-EU) significance of a particular case are among the factors to be taken into account.

In this vein, the following categories of cases would be easier to pursue:

(i) where a case is underpinned by provisions of EU law clearly targeting the infringement at hand (e.g. the Services Directive clearly precludes Member States from imposing an obligation on the provider to obtain an entry in a register or registration with a professional body or association in their territory); and

(ii) the infringing provisions of laws or practices of Member States are easy to identify (e.g. infringing laws are generally easy to identify).

[86] C(2016) 8600 final, "EU Law: Better Results through Better Application".

In this regard the structured dialogues with Member States point to significant confusion as to how (if at all) the data localisation restrictions identified fall within the scope / could be addressed under the provisions of different existing EU legal instruments (**Annex 5 presents a detailed overview**). Moreover, many restrictions are hidden in outsourcing guidelines, circulars and similar administrative documents.

Also it appears from the structured dialogues with Member States and the Commission's own assessment that it would be more difficult to pursue infringement proceedings against localisation restrictions concerning public data or sensitive private data, such as health data.

Considering the potential cases targeting different categories of data localisation restrictions against the criteria mentioned above, very few cases would satisfy the threshold of addressing "the most important breaches of EU law" while being, at the same time, easy to pursue. For instance, cases targeting restrictions in the financial sector could be said to have sufficient economic significance, however the sector is excluded from the scope of the E-Commerce Directive and the Services Directive. Moreover, the restrictions typically stem from administrative requirements and practices rather than easily identifiable Member States' laws. Cases targeting restrictions in the health sector or those concerning public data could also be regarded as economically important, but the type of data at hand would make such cases difficult to pursue.

In view of these difficulties, it is not surprising that no infringement proceedings against data localisation restrictions imposed by Member States have been launched yet.

Finally, even if proceedings were to be launched, the fact that many data localisation restrictions are context-specific means that several court judgements would be required in order to cover all aspects of such restrictions and establish a cross-cutting set of principles. Since, as explained in section 6.2.1.1 above, infringement proceedings take on average 4-5 years until they result in a court ruling, this would indeed lead to **a long period of legal uncertainty.** As a result, users would continue to demand local data storage and/or processing from the service providers, and the prospects of the fast-developing data economy would continue to be harmed.

This option could have a marginally positive impact on **costs associated with the analysis of the regulatory environment**, at least for SMEs and could also have a marginally positive impact on the **choice and cost of data services** for the organisations using them. This would for instance be the case if an organisation that had erroneously assumed it has to store and/or process data in a particular Member State (i) found out, thanks to transparency measures, that there was no such localisation restriction and (ii) contracted a cheaper (foreign) data service.

Putting in place guidelines and transparency measures is **not expected to affect the competitiveness** of cloud service providers or organisations using in-house data storage or processing IT systems.

6.3.1.2 Data availability for regulatory control by Member State authorities

The introduction of guidelines on data availability for regulatory control by Member State authorities would reduce the negative economic impacts and costs deriving from the **administrative burdens** present in the baseline scenario. Member States will find it useful to have a framework for discussion and a forum where best practices can be discussed and eventually adopted. This could result in a degree of procedural convergence and reduce the human resources cost, thereby increasing **cost efficiency** for public administrations. This remains, however, a simple discussion forum which is not likely to lead to specific improvements or results.

In addition, option 1 is likely to have only **limited impacts on the downstream sector**. Many negative impacts identified for the baseline scenario are likely to persist. A persisting lack of trust could alter **costs and choice** of market operators and have an indirect effect on their **operational efficiency**. **Market fragmentation** would also persist, hampering **innovation and competitiveness**

of the companies in the market as business end-users of data services would in some case be obliged to stay in less competitive markets with **higher prices**.

The impacts on the **upstream market structure** (cloud service providers) would be similar to those envisaged in the baseline scenario.

6.3.1.3 Switching and porting data between providers and IT systems

The development of the EU cloud market is forecast to be somewhat stronger under the Option 1 than under the baseline option[87], putting the **growth in demand for public cloud at 19.7 % Compound Annual Growth Rate between 2018-2025** (6 percentage points higher than in the baseline scenario), amounting to a €68.8 billion market by 2025. This is due e.g. to growing awareness and involvement from industry and increased momentum to build trust and confidence in cloud and reduce the fear of vendor lock-in. Exit strategies by design might be implemented by cloud service providers.

This option would require service providers to explain in a sufficiently detailed and accessible manner the processes, timeframes and charges that apply to switching. The economic impacts of this option therefore include an **increase in variable costs** for the service providers.

Costs in data transmission are already high and sometimes prohibitive[88]. **Transparency** on this type of cost could be helped under this option, e.g. by explicitly stating the cost of bandwidth for data outbound and data inbound in contractual agreements in guidelines or self/co-regulation. This can help cloud customers plan their costs related to migration. This could be **beneficial for SMEs** that have lower bargaining power against cloud service providers, and it could incentivise switching by removing uncertainty.

6.3.1.4 Security of data processing

This option would result in guidelines concerning security of data storage and processing, but would not be binding for the Member States. Nevertheless, clarity would be shed on the security provisions on data storage, and contribute to alleviate the lack of trust and the uncertainty.

Because of enhanced levels of trust, this option would have a positive indirect impact on the business sector, including both upstream (cloud service providers) and downstream markets (business end-users of cloud services). The magnitude of the impact will depend on the uptake and effective implementation of guidelines by Member States. However, it is likely that this impact will be modest because of the voluntary nature of the guidelines, which will configure against a background of a myriad of different voluntary certification schemes.[89] Therefore, Option 1 will not lead to a high degree of clarity.

6.3.2 Environmental and social impacts

6.3.2.1 Free flow of data across borders

As explained in section 6.2.2.1, a free flow of data is beneficial for the environment through increased liberty for cloud service providers to locate their data centres in more environmentally optimal locations. Option 1 would slightly reduce the need to deploy infrastructure in environmentally sub-optimal locations and could have a (limited) positive impact on the environment.

[87] IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (SMART 2016/0032).
[88] Ibid.

[89] Tecnalia SMART 2016/0029, Tecnalia, "Certification Schemes for Cloud Computing" (Ongoing)

Its social impact is likely to be negligible due to (i) the option's non-binding nature and (ii) the absence of a strong link between setting up data storage and processing infrastructures and employment in general.

6.3.2.2 Data availability for regulatory control by Member State authorities

As the option would mostly include discussions / exchange of practices under a non-legislative approach to improve data availability for regulatory control by Member State authorities envisaged by this option, there would be only limited positive environmental impacts in this intervention area.

6.3.2.3 Switching and porting data between providers and IT systems

The impacts would be similar to those under the baseline option. However, with a stronger push from the Commission for market players to cooperate on interoperability, and especially open APIs, a further increase in the efficiency of data migration may be seen.

6.3.2.4 Security of data processing

Guidelines on security of data processing and storage would mean an improvement in terms of cyber security compared with the baseline option. Therefore, potentially negative environmental and social impacts of cyber-attacks, as described in 6.2.2.4 would diminish under Option 1.

6.3.3 Impacts on Member States' public authorities

6.3.3.1 Free flow of data across borders

A strengthened enforcement of existing EU legislation, combined with enhanced transparency on existing data localisation provisions, could lead to administrative burden for Member States, particularly in terms of human resources. As Option 1 is not legislative, the impact would depend greatly on the modalities of its implementation in particular Member States (from low-scale implementation to full-scale implementation) and the degree to which existing mechanisms set up under the *acquis* would be relied on. Any quantitative estimation would also depend on the number of existing data localisation restrictions in a particular Member State. Under this option, therefore, administrative burden is expected to vary greatly by Member State.

Moreover, this option does not provide an avenue for problem resolution regarding data localisation not covered by the existing mechanisms. As such, it is not future-proof and it does not allow for tailoring/further deliberations or implementing rules on issues relating to the free flow of data.

6.3.3.2 Data availability for regulatory control by Member State authorities

Option 1 would have similar implications for burdens on public authorities to those described in 6.3.3.1.

6.3.3.3 Switching and porting data between providers and IT systems

As Option 1 encourages self/co-regulation by the market to establish common conditions for switching cloud service providers, it would pose no direct administrative burden to Member States.

6.3.3.4 Security of data processing

The expected impacts of Option 1 on Member States' public authorities are the same as those of Option 0 for the intervention area security of data processing.

6.3.4 Stakeholder views

6.3.4.1 Free flow of data across borders

In general, stakeholders have indicated *not* to support Option 1. Instead, as argued further below in this section, a majority of different categories of stakeholders has called for a legislative approach to confront the problem.

In first instance, the strengthened enforcement of existing EU legislation vis-à-vis different categories of unjustified localisation restrictions, as foreseen under Option 1, would be welcomed if compared to the baseline option. For, a clear majority of stakeholders (61.9% of respondents to **the public consultation**) believes that data localisation restrictions should be removed. In this regard, strengthened enforcement is expected to have a moderate positive effect as compared to no EU policy change.

However, as introduced above, stakeholders from both the public and private sectors have called for a new legislative instrument. On 13 December 2016, 16 heads of governments of EU Member States sent a letter to President Tusk to call for such a legislative approach. They state "*In our view an early legislative proposal providing for the free flow of data is crucial to avoid market fragmentation and further obstacles to the development of the data economy in the EU*".

The same message appears from **the public online consultation**, in which 55.3% of respondents argue for a legislative approach.[90]

The majority of stakeholders, therefore, would be disappointed with an approach as under Option 1. The different group of stakeholders also provide more in-depth views on why they would prefer a legislative approach. Participants of the structured dialogues with the Member States, for instance, convincingly identified the issues of 'legal uncertainty' and 'lack of trust' as drivers of the problem of obstacles to data mobility. This view was confirmed by respondents to **the public consultation**, who identified the influence of market dynamics on data localisation, even without the presence of data localisation restrictions from the part of public authorities. One respondent to the public consultation referred to such 'perceived restrictions' in a written answer to an open question: "*More concerning than formal obligations are informal/perceived ones. For example, our experience is that many entities in regulated industries want data to be stored in one country. Even without a formal requirement, it is clear from these conversations that entities believe that regulators strongly disfavour or in practice prohibit storing data outside of their home country. More generally even with formal requirements, there is uncertainty as to their application and coverage which complicates market assessment*".

Option 1 would not take away this legal uncertainty, as it proposes to retain the current patchwork of EU-law applicable to data localisation. As no awareness raising campaign would be undertaken under this option, the uninformed market dynamics leading to data localisation and the 'perceived restrictions' mentioned above would retain intact. Accordingly, this approach does not tackle the sectorial administrative requirements that are still in place.

Finally, as evidenced by multiple press reactions to the Digital Single Market Mid-Term Review[91]an initiative under Option 1 could be seen as a negative appreciation of the Commission's promised actions under the Digital Single Market strategy. This is contention is reinforced by the letter of 16 heads of governments of EU Member States to President Tusk on 13 December 2016: "*we note with concern the risk of serious delay with the presentation of a legislative proposal in relation to data localisation under the European 'free flow of data' initiative. The DSM strategy set very clear expectations for presentation in 2016 on an initiative…*"

[90] 289 respondents participated in this multiple-choice question.

[91] See: Politico, http://www.politico.eu/article/digital-single-market-mid-term-report-card-tktkt-percent/ and CBR Online, http://www.cbronline.com/news/verticals/central-government/eu-failing-digital-single-market-says-techuk/.

6.3.4.2 Data availability for regulatory control by Member State authorities

Compared with Option 0, Option 1 does not comprise any significant change in the approach on the intervention area of data availability. It is unlikely that Member State discussions / exchanges of best practices would lead to tangible results in terms of trust either on the part of public authorities or the part of market players. Therefore, Option 1 would not enhance the data availability concerns that were frequently mentioned by stakeholders in their responses to the public online consultation.

6.3.4.3 Switching and porting data between providers and IT systems

There is broad agreement among stakeholders that the identified issues with data portability and switching need to be addressed. Stakeholders have generally been positive towards the different soft law measures suggested, both in the public consultation and in workshops. Especially popular measures are standards development and guidelines. However, many stakeholders have underlined the need to avoid interfering too much with contractual freedom.

Among the **Member States** who contributed position papers to **the public consultation**, the **UK** held that the EC should be careful not to promote portability through over-prescriptive common standards, or to create unnecessary cost/burden on businesses. The **Danish** government supports the development of standards which aims to promote interoperability and portability. They also view interoperability as an essential prerequisite for a competitive well-functioning digital economy.

6.3.4.4 Security of data processing

With reference to section 6.2.4.4., we may conclude that specialised stakeholders argued that security of data processing would benefit from increased data mobility. During the evidence gathering process, this insight was frequently confirmed by other stakeholders, with no opposite views voiced. Therefore, stakeholders' judgment would be that Option 1 is suboptimal but slightly better, as it would imply a strengthened enforcement of existing legal instruments to counter unjustified data localisation restrictions.

However, as a free flow of data principle would be still absent, cyber security service providers would still have to be engaged in costly processes of compliance research. This would still result in a lack of legal certainty.

6.4 Option 2: Principles-based legislative initiative and cooperation framework to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

6.4.1 Economic impacts

6.4.1.1 Free flow of data across borders

Option 2 includes the establishment of a legal principle of free flow of data within the EU (as described in section 5 and in the context described in section 2). It requires Member States to notify any new data localisation restrictions they deem justified and intend to put in place by means of notification schemes of existing EU legal instruments. During a transitional period, Member States would be obliged to carry out a review of existing data localisation restrictions. Additionally, the policy option proposes awareness raising campaigns around the free flow of data principle.

Hence, this option would **ensure the effective removal of existing unjustified localisation restrictions, and the avoidance of future ones**.[92] As more than two-thirds of the sample of 45 analysed data localisation restrictions is unjustified, this would mean the removal of most existing data localisation restrictions. The remaining restrictions are not likely to affect businesses, e.g. in

[92] Under this Option, in principle all data localisation restrictions for reasons other than protecting public security would be considered unjustified or disproportionate restrictions. The precise application of this practical rule can be debated by the expert group which is to be established under this option.

the form of restrictions on accounting data, because such restrictions would not likely be justified on grounds of public security. Additionally, the at least equally important problem of market dynamics originating from a lack of knowledge by operators of the correct legal situation concerning data localisation restrictions or on implicit localisation restrictions would be addressed by the awareness raising action foreseen, effectively mitigating legal uncertainty and lack of trust. The remainder of this section will assess the economic impacts of the removal of data localisation restrictions.

Macro-economic impacts

It is, to a certain degree, possible to estimate the macro-economic impacts following the general adoption of data-driven innovation and data technologies in the EU, as in the analysis carried out by the support study for this Impact Assessment[93]. This study concludes that a free flow of data legislative proposal taking away data localisation would be the most important factor in driving the European data economy towards the high growth scenario of 4% GDP by 2020.

However, there are also challenges in calculating the exact macroeconomic impact generated from removing data localisation restrictions in quantitative terms. The link between the different levels of regulation proposed to address the problems identified in section 2 and aggregate economic elements such as GDP, employment level or competitiveness of the sector does not allow quantifying in a high level of granularity.

Certainty for the future: creating an investment climate for a true European data economy

The most notable economic effects of this Option will be achieved through creating legal certainty and raising trust levels regarding data storage and processing. This should create an optimal investment climate, directed at the EU's future. The data economy is developing rapidly at the moment. Therefore, the proposal underlying this IA deviates from the classical situation in the sense that it is not only directed at present problems but also at preventing future ones and creating the right environment for the EU to fully grasp the benefits of the data economy.

Impact on cloud service providers

The support study by Spark, Time.Lex and Tech4i2[94] has provided some evidence on stark difference across costs in setting up and operating data centres in Europe, but relativizes the link between these costs and the existence of restrictions. The study finds that data localisation has an impact predominantly on the data centres that cloud providers build in addition to their first facilities: "It is possible to assert that having built a first round of data centres primarily in locations to meet user needs, later choices for additional data centres (being built now or in the future) might be driven more by concerns of cloud service providers about cross-border data regulations - thus they might be located in sub-optimal locations"[95].

The study asserts that data localisation restrictions could lead to the provision of more cloud data centres than cloud service providers would ideally like to deploy if they wish to provide services in Member States with more onerous cross-border data transfer compliance obligations. With each cloud data centre costing €276.9 million on average in EU Member States, overprovision of centres is costly[96].

---

[93] See IDC, "European Data Market. Data ownership and Access to Data - Key Emerging Issues", 2016 (SMART 2013/0063).

[94] Time.lex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (SMART 2015/0054).

[95] Interviews with cloud providers have confirmed that ten years ago cloud servers were built to meet the needs of cloud service providers. In recent years the situation has been reversed and now server locations are designed to best meet user needs and cross-border data compliance requirements. However, these location decisions could also include user concerns such as lower latency and/or cost factors.

[96] Moreover, the cost does not need to be reflected necessarily into pricing. Discussions with cloud providers also revealed that the price/subscription charged to users in the short-term can be independent of the cost of provision; as

Impacts on businesses

The study conducted by Deloitte[97] for the European Commission shows how important the removal of data localisation restrictions is for downstream business users. Although there is an overall net benefit, the removal could be detrimental to providers using data location as a specific competitive advantage. Deloitte compares a baseline scenario of no intervention with one where data localisation restrictions are removed. The results are illustrated by below, showing that **EUR 11.6 billion can be leveraged in terms of net present value (NPV) of revenues for cloud users**, providers and society as whole by the removal of data localisation restrictions. Being based on cloud services only, this is just a conservative proxy of what could happen in the entire data universe.

Figure 7 – Changes in NPV across stakeholders after the removal of data localisation restrictions

Stakeholders	Discounted NPVs 2015-2020	% change compared with baseline scenario
Cloud users	EUR 542.2 billion	1.36%
Cloud providers	EUR 19.5 billion	21.53%
Society	EUR 57.6 billion	1.49%
Total NPV added	**EUR 11.6 billion**	**1.90%**

(Source: Deloitte 2016))

In terms of different sectors of activity, the same study calculated that the largest benefits in relative terms would accrue to the manufacturing sector (+2.23%), followed by distribution retail and hotels (+2.12%).

ECIPE[98] estimated an overall EU-wide weighted impact on GDP is up to EUR 8 billion yearly, representing 0.06% of the current EU GDP. The true cost of today's restrictions is however likely to be underestimated given that this scenario does not take into account the regulations that are implicitly or indirectly localising.

The same report acknowledges that the impact of these price adjustments would not lead to a large-scale outsourcing of data hosting and processing services to other EU Member States. Imports of communication services by German customers from other EU Member States would increase within a range of 2-8% above the current levels. The ranges are similar or slightly higher for France. In all other cases, the import increase on communication services are limited to between zero and 3% according to ECIPE.

These results are corroborated by the results of **the public consultation**, which show how stakeholders are aware of these potential savings that could accrue in case of clear limits to data restrictions[99].

providers pursue goals such as maximizing market share. Over the long term, cloud service providers will need to obtain a return on their investment, but in the short-term, costs to users (in subscriptions and/or fees) may not reflect costs incurred by cloud service providers.

[97] Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 (SMART 2014/0031).

[98] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016, http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf .

[99] The impact that was most frequently mentioned across all participants is costs (130 times). The second most frequent answer is that of launching a new product or service (118 times). Subsequently follow entering a new market (95 times)

Also, the consultation showed the high impact (more than 70% of respondents) for the effects of data localisation restrictions on **launching a new product or service or entering a new market.**

Additional results of the public consultation are explored in more detail in **Annex 2.**

Costs of setting up a new business in the EU

Taking away data localisation restrictions and enshrining a legal principle on the free flow of data in European law would **reduce the cost of setting up a business in the EU** through the provision of cheaper and more competitive cloud services at a one-time cost for applicability in the whole EU. The cost of setting up a business in the EU is currently at EUR 300 and 3 days per Member State. In line with the Commission's Start-up and Scale-up initiative's findings, bringing this cost down would increase EU innovation and competitiveness, strengthening the economy.[100]

Quantitative impacts

It is possible to extrapolate some of the economic impacts in more quantitative terms to give an idea of the potential benefits from the free flow of data principle.

The very nature of data localisation restrictions implies that the offer of data services is reduced, at least in the short term, leading, potentially, to higher prices of such services in the markets concerned. This has an impact of **market structure** as pent-up demand in "expensive" Member States is not met and providers in "cheaper" Member States do not manage to attract all the potential clients. Also, the choice will be more limited in smaller Member States. In several countries, only data centre services that offer the lowest added value are available (e.g., Infrastructure-as-a-Service (IaaS)), while more value-adding services like Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) are not available there. This limits the options of some companies to less efficient data centre solutions. For example, the price of storage per gigabyte in case of a Hungarian cloud service provider is more ***than 25 times higher than*** the price per gigabyte per month in a larger PaaS service.

Figure 8 – Diverging data storage prices

Public cloud provider location	Price(per GB of data stored)
Azure Germany Northeast (PaaS)	€0.0224
Azure North Europe (PaaS)	€0.0202
Telekom Hungary (IaaS)	€0.5371[101]

This can have an impact on the **competitiveness of European SMEs**. If we extend as an example, the price differential of 51.69 Euro cents and we assume that SMEs store 50 TB on average using private cloud services, this would entail a saving or around EUR 26,000 per SME.

In 2015 there were around 23 million SMEs in the EU[102]. The following example assumes that only 8% of them use private cloud computing services[103]. Assuming theoretically that 50% of the SMEs

---

and providing services to private entities (81 times). Other impacts, such as on providing services to public entities or conducting research, received lower scores. Only 2,6% (16 respondents) see no impact of data localisation restrictions.

[100] COM(2016) 733 final, "Communication of the European Commission to the European Parliament and 'Europe's next leaders: The Start-up and Scale-up Initiative".

[101] Source: https://azure.microsoft.com/en-us/pricing/details/storage/blobs/ http://www.telekom.hu/uzleti/szolgaltatasok/informatika/szerverek-adatparki szolgaltatasok/szerverberles/virtualis-szerverek

[102] Annual report on EU SMEs 2015/2016

[103] Eurostat, http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Main_statistical_findings

can use a 'cheap' provider and the other 50% an 'expensive' one, then the potential savings from migration of half of them from the cheap to the extensive provider would be in the area of 23.9 million euro per month. That would amount to around 276 million euro per year. This is an estimation which has little scientific value, but can give an idea of the magnitude of lifting data restrictions that may hinder this migration in fact or in perception.

6.4.1.2 Data availability for regulatory control by Member State authorities

Option 2 foresees the establishment of the principle that the holder of data shall not deny access to data to a public authority for its regulatory control purposes. As for the previous two options discussed, the impacts on the business sector are likely to be indirect.

However, the fact that the obligations on private parties are clearly established and reinforced and a cooperation framework is established to promote the effective application of the principle of availability in cross-border data storage will **reduce the level of uncertainty** for those business users who would like to move to cheaper providers in another Member State. This has a short-term positive impact on the **operational efficiency** of the **downstream sector** (business end-users).

The impacts on the **cloud service providers** are likely to be more significant in the medium term. Under a provision and a cooperation mechanism on data availability foreseen by this option, they could compete widely across borders, which would improve the **efficiency of the data service providers' sector** and contribute to bring down the costs for its clients.

The only limited negative impact on the upstream sector from Option 2 would be linked to the costs associated with the set up and enforcement of the standard contractual clauses.

6.4.1.3 Switching and porting data between providers and IT systems

The economic impacts of this option stem from establishing the principle that cloud service providers should offer data portability to facilitate the switching of providers or porting of data back to users' own IT systems. Under this option, the role of industry will be flanked by enforceable legal principles. A possible result could be more direct compliance costs, however at the same time the option would tackle vendor lock-in issues more convincingly. As these have higher and more serious impacts on stakeholders and the economy in general, they will therefore offset any increased compliance costs through the creation of a more open and competitive market.

More transparency will remove legal uncertainty, especially regarding hidden costs which are not mentioned in the contract. However, transparency and voluntary agreements on some contractual arrangements fall short of addressing the cost problem. This has to do with the **magnitude** of the costs and its **apportioning** between the "sending" and "receiving" side. The more granular the analysis of the cost apportioning gets, the more difficult (and costly) it is to extricate the cost components, especially for data which are complex in format and not raw.

Option 2 could indirectly foster, through making switching easier, the growth **and the take-up rate of cloud services** in Europe. A forecast of the growth in the uptake of public cloud has been made in the study on Switching Cloud Providers[104], using a **Mandatory Regulation Scenario**[105]. A mandatory regulation will lead to a faster take-up of public cloud services. SMEs and start-ups are expected to be most positively impacted in this scenario. The demand for public cloud is forecast to grow by 20.5 % Compound Annual Growth Rate between 2018 and 2025, reaching €71.9 billion in 2025.

Furthermore, as reported in one of the workshops with business stakeholders organised by the support study team[106], "*Standards are used in the market in an ineffective and inconsistent manner,*

[104] IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (SMART 2016/0032).
[105] This scenario assumes the introduction of a mandatory data and application portability right, which is somewhat broader than the scenario presented in this section. However the growth forecast is still expected to be relevant.
[106] Workshop held on 18 May 2017 in Brussels.

thus, hampering the export of data from one cloud service provider and their import to another cloud service provider". High level EU principles could **encourage industry-wide initiatives**.

Although it is currently impossible to obtain a macro-economic estimate of what this option would entail at European level in terms of costs' savings, it is possible to get some insights at the **micro-level** thanks to a study by Kolb, Lenhard and Wirtz[107] who carried out and evaluated the migration process for a real-world application among seven cloud platforms. Their study shows that there are many costly and time-consuming issues to grapple with for cloud service providers when customers migrate from platform to platform. The effort put into this by cloud service providers differs considerably from vendor to vendor. Introducing a principle of data portability to enable switching would steer the efforts made by market players in the same direction, and force more cooperation and a more streamlined approach to portability solutions (both on a technical and contractual level).

At the same time, however, evidence suggests that legislative action in this intervention area **should not be too detailed**, as this could have counterproductive effects. Analysis of the written inputs to **the public consultation** indicates that some stakeholders are concerned about the introduction of a right to data portability for any kind of data held by a company. Likewise, they flag the risk of negative impacts on innovation.

The increase of switching requirements is likely to lead to a **regulatory burden and compliance costs** on the service provider. Here it could be argued that since service providers will anyway have to give effect to the portability right under the GDPR, these negative effects will be limited. Since many of the cost factors are present but quantitatively unknown, this option aims to strike the balance in regulatory intervention.

At the same time, the level of information supplied by the evidence-gathering process (e.g. the dedicated support study 'Switching Cloud Providers') is of such a modest volume, that instituting a legal right to portability and an obligation to CSPs could yield negative externalities that are not yet assessed. In this respect, the Commission should be cautious about instituting such a right.

Sub-option 2a

Sub-option 2a would rely on self-regulation by industry through the development of codes of conduct for facilitating switching between providers. Accordingly, Sub-option 2a may lead to less directly positive economic result than Option 2, because of a more modest approach to mitigating market dynamics leading to 'self-imposed localisation'. This is because it is much more effective to raise awareness around a clear legal principle than around a decentralised effort of industry to develop codes of conduct that is foreseen under Option 2a.

Option 2a would however still induce the largest amount of the positive economic effects assessed for Option 2 above, because it would provide for action by the industry to develop codes of conduct on switching and standards of information provision to users regarding the conditions under which data can be ported out of their IT environments. This would provide for better functioning of market forces to yield easier switching and porting data for customers.

What is more, the sub-option would probably result in lower compliance costs for cloud service providers than under Option 2, because self-regulation would present the cloud service industry with the opportunity and responsibility to self-regulate while minimising compliance costs.

6.4.1.4 Security of data processing

This option would facilitate the identification and development of reliable common standards and/or certification schemes for the security of storage and/or processing of data. Concretely, a specific

[107] Stefan Kolb, Jorg Lenhard and Guido Wirtz, "Application Migration Effort in the Cloud – The Case of Cloud Platforms" (2015), available at: https://www.researchgate.net/publication/303750569_Application_Migration_Effort_in_the_Cloud

cloud service providers' certification scheme could be developed through cooperation on standards by the Member States.

There will be an impact on the providers of cloud services which will be involved in the making of the **codes of conduct and standard-setting**. This is likely to entail only moderate **costs,** as participation would be voluntary and possibly devoted to trade associations and bodies. The cloud services providers may be more extensively affected by the specification of EU standards, to the extent that they would implement new standards (one-off cost and lower running cost ensuring updates).

The **benefits from standards** would be expected to outweigh the costs if an EU-wide certification and labelling scheme for the Cloud sector is established. This would enhance the **efficiency of companies** operating cross-border as industry could certify their products and services only once and against a scheme that is recognised in the whole of the EU. The existence of standards in areas such as security is likely to increase trust and hence attract more business end users of cloud services, thus fostering **growth and competitiveness** across the borders

At the same time a minimal level of common requirements would reduce uncertainty and lack of trust stemming from different levels of data security among the Member States[108] which is currently contributing to alter the market structure and the client choice[109], as has been proven by stakeholders consulted and by the support studies.

The importance of certification and standards has been quantified by Deloitte[110] calculating that cloud users are expected to experience an additional NPV creation of 0.64% (which corresponds to around EUR 3.5 billion) from the additional user uptake generated by these certifications and standards and the reassurance they provide that these cloud services can be considered safe and reliable.

Sub-option 2a

Instead of catering the possibility for a new cooperation mechanism on security standards or certification schemes, Sub-option 2a would enhance legal certainty on the already applicable security requirements. It would recall that any existing security requirements for companies will continue to apply to them, regardless the location in the EU where their data is stored or processed and also when this is subject to outsourcing to a cloud service provider.

The economic impact of security elements of the sub-option would be more positive than under Option 2, as it would lead to a higher degree of legal certainty in the market. This positive effect is attained by explicitly avoiding any overlap with existing requirements, while at the same time providing reassurance to businesses about the continued applicability, also across borders in the EU and under outsourcing arrangements, of the security provisions under which they already operate.

The actual security levels of data storage and processing in the EU would be maintained or even improved compared to Option 2, because the same EU actions on security of data storage and processing would still be provided for under Sub-option 2a, only on a different legal basis, making use of other cyber security initiatives and the NIS Directive.

[108] The Study by London Economics Europe et al., "Facilitating cross border data flow in the Digital Single Market", 2016 (SMART 2015/0016) provides clear insights and figures about how business and individuals tend to perceive or assume real **differences in the level of data security across European countries;** and use data **location as a proxy for security** (with one's own country often, though not always, seen as more secure).

[109] For example, the LE Europe study (SMART 2015/0016) notes that "For the UK, a recent study by Vanson Bourne found that 86% of enterprise customers believe it is important for business-critical data to be stored by a UK-based cloud service provider to ensure "data sovereignty"".

[110] Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 (SMART 2014/0031).

6.4.2 Environmental and social impacts

6.4.2.1 Free flow of data across borders

Option 2 would have a positive impact on the environment, since data service providers and organisations using in-house data storage or processing IT systems would receive concrete benefits. Firstly, they would be free to deploy data storage or processing infrastructures in those locations which are characterised by low average temperatures and/or abundance of renewable sources of energy, thereby achieving small environmental footprints of their activities. Secondly they would be able to adopt innovative approaches to the use of energy in data centres, e.g. maximising the use of renewables by shifting the data processing load to a data centre where renewable energy is available at a particular moment.

In **direct terms**, Option 2 would have a positive impact on social issues in terms of employment. An interview with a large European cloud service provider on the specific conditions for investment in data centre locations led to the conclusion that a moderate number of new jobs might well be created thanks to relocation of data centres to Member States with better conditions in terms of climate, energy prices or land prices. In line with EU-regional policy objectives to diversify economic activities in rural areas, this is likely to more evenly spread data centre jobs over geographical locations in the European Union. At the same time, this would not lead to loss of jobs in the locations were data centres are located before relocation, because they can be operated remotely, so current personnel would not have to be necessarily relocated. Data centres can easily service clients over larger distances, for instance 2000 kilometres between a data centre and its clients is feasible.[111] This allows for an optimal distribution of resources of cloud service providers over the EU because of the more transparent, predictable and open regulatory environment for data storage and processing activities. [112]

More generally, as illustrated in the high growth scenario by the European Data Market Study, by 2020 the overall number of data jobs is estimated to amount to 10.4 million, subject to a set of very favourable framework conditions triggering a faster take-up of data services and technologies. Apart from other factors such as the adoption and diffusion of all digital technologies, as well as the awareness and willingness to deploy them, the removal of regulatory barriers such as restrictions to the free flow of data, is critical to a favourable framework.[113] Therefore, Option 2 would have a positive impact on the overall creation of data jobs by 2020.

In **indirect terms,** however, Option 2 would have a positive impact on employment because of the added growth and innovation potential, caused by the lower costs for (i) setting up a business in the EU, (ii) entering a new market, (iii) launching a new product or service to the market and (iv) the ability to serve public and private customers, as indicated in section 6.4.1.

In **social terms**, Option 2 would reduce the number and range of limitations constraining (i) business choices regarding the location of data storage or processing infrastructures and (ii) the opportunities for data service providers to serve customers in other Member States. It would, therefore, have a positive impact on the freedom to conduct a business provided for by Article 16 of the European Charter of Fundamental Rights.

6.4.2.2 Data availability for regulatory control by Member State authorities

Policy action on improving data availability to Member State authorities for regulatory control purposes would increase cross-border data mobility because of raised levels of trust both with

[111] Latency requirements persist only for a very small number of applications, such as high-frequency trading.
[112] Discussions with a large cloud service provider, headquartered in France.
[113] See further pp.190 & 195, European Data Market, 2017 [IDC Study (SMART 2013/0063)].

market participants and with Member States authorities. Therefore, there would be significant positive environmental impacts flowing from this intervention area under Option 2.

6.4.2.3 Switching and porting data between providers and IT systems

The introduction of a legal principle of data portability to facilitate cloud switching, especially when accompanied by guidance and recommendations on the levels of interoperability needed, would force companies to improve the interoperability of their systems. With a minimum level of interoperability ensured, migration processes would need less processing power and thus have less of an environmental imprint.

As for the social impacts of this option, the assessment is the same as for the preceding options.

Sub-option 2a

Sub-option 2a does not include a legal principle of data portability. For that reason, it might lead to less directly positive environmental and social effects in terms of the decrease of processing power used for migrating data from one server (of a service provider) to another server. However, this difference in impact would be negligible as Sub-option 2a would provide for self-regulation through the development of codes of conduct, which will also lead to improved interoperability of systems.

6.4.2.4 Security of data processing

Option 2 foresees in the development of a specific cloud service providers' certification scheme. This would mean a considerable improvement in terms of cyber security, compared with Option 1. Therefore, potentially negative environmental and social impacts of cyber-attacks, as described in 6.2.2.4 would diminish under Option 2.

Sub-option 2a

Sub-option 2a would not provide for any additional actions on cyber security. However, the issue will be addressed by of other/existing EU instruments, such as the NIS Directive. As for potential environmental/social impacts of cyber security it is not important at all which instrument is used, Sub-option 2a would not lead to impacts different from Option 2.

6.4.3 Impact on Member States' public authorities

6.4.3.1 Free flow of data across borders

Option 2 would lead to moderate administrative burden for Member States' public authorities, caused by the allocation of Member States' human resources necessary for structured cooperation between Member States and the Commission by means of a 'single points of contact' expert group in the Member States. The single points of contact would be represented by civil servants who are already employed by Member States' public services, but whose responsibilities would be expanded or further coordinated.

As indicated in the description of Option 2 in section 5.4, these single points of contact would be tasked with cooperation regarding free flow of data categories (in particular in the context of the expert group) and organising awareness raising campaigns around the free flow of data principle.

The expert group would meet regularly. Accumulating the tasks mentioned above, it can be estimated that 0.5 FTE would be sufficient to fulfil these duties, because the expert group would not meet frequently. Moreover, any implementing acts could be taken by making use of the comitology procedure of an existing Committee. According to the 'institutional cost estimation' tool used for the

European Electronic Communications Code, this would result in an annual cost of EUR 33.384 for Member States. [114]

Option 2 would also put in place the notification/review procedures to verify the compatibility with the EU law of Member States' planned and existing derogatory measures as well as the transparency mechanism and could, therefore, result in administrative burden on Member States' public authorities. However, all options would include notification and review process, including the baseline option. Therefore, there are no further added costs in this respect in the higher intervention range options. As demonstrated in the section describing drivers of the problem above, the number of measures to be notified and reviewed is not expected to be very high. Assuming that a Member State would have to provide between 1 and 5 notifications per year and that an average administrative cost is around €385 per notification[115], the annual administrative burden per Member State would range between approximately €385 and €1925.

6.4.3.2 Data availability for regulatory control by Member State authorities

Although this option would slightly increase the coordination costs for the Member States' administrations as compared to the previous two options, this cost would be fixed and the effort to establish the system would be a one-off. On the other hand, the benefits of common approaches and guidelines, as well as increased cooperation on data availability in electronic format are going to be increasingly large as the volume of cross-border data availability requests increases.

As Option 2 would place any actions on this intervention area under the cooperation framework of single points of contact mentioned in section 6.4.2.1, the financial burden for this intervention area will be shared with the free flow of data area and will not generate extra costs.

6.4.3.3 Switching and porting data between providers and IT systems

Under Option 2, market participants would be required to give insights in the processes, technical requirements, timeframes and charges that apply in the situation of switching providers. So, although Option 2 would institute a legal principle on porting for switching provider, any burdens would be placed on the private sector, not the public authorities of Member States.

Sub-option 2a

This option would rely on self-regulation, to be monitored by the European Commission. Therefore, there would be no conceivable additional impact on Member States.

6.4.3.4 Security of data processing

There would be no administrative burden for Member States in the intervention area of security under this option. It envisages the development of common standards, but this could also be done by industry.

Members of the cooperation group of single points of contacts would be expected to have regular but non-frequent meetings with the data protection authorities and cyber security authorities of Member States, but because this will constitute a maximum number of two meetings annually, no extra burden in terms of HR or finance is to be expected.

Sub-option 2a

[114] The "Institutional Cost Estimation tool", used to calculate Full Time Equivalent cost parameters, was developed in the context of the support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005).

[115] Based on the data presented in the Impact Assessment accompanying the proposal for a Directive on the enforcement of Directive 2006/123/EC of 12 December 2006 on services in the internal market, laying down a notification procedure for authorisation schemes and requirements related to services, the average time spent to comply with the notification procedure analysed in the IA is 12 working hours per notification. Taking the EU average of hourly earnings of civil servants with university education of €32.10, this results in an average administrative cost of €385.20 per notification.

This option would rely completely on existing legislative instruments for security. Therefore, there would be no conceivable additional impact on Member States.

6.4.4 Stakeholder views

6.4.4.1 Free flow of data across borders

The majority of stakeholders who responded favour Option 2 for this intervention area, because it concerns a legislative approach, combined with certain non-legislative elements such as cooperation and awareness raising.

The public consultation consulted stakeholders on the type of EU-level action they consider appropriate to address data localisation restrictions. 55.3% of respondents advocate legislative action[116]. Cross-checking the multiple-choice answers to this question with the written contributions to the same question leads to the conclusion that most respondents see a combination of a legislative instrument and increasing the transparency of justified restrictions as the most appropriate option. As Option 2 foresees precisely this, it may be inferred that the majority of public consultation respondents would have chosen Option 2.The respondents' argument behind the call for a legislative instrument is that this provides clarity and legal certainty by establishing a general principle of the free movement of data.

Exemplifying this argument, in one of its responses to the public online consultation, a cloud service provider stated: "*In the cloud computing business, the most common data localisation restrictions we see target financial, health, telecom and public sector data. However, these measures are less often found in black and white legislation, but rather in sectorial guidelines by national regulators or government agencies*". As the respondent also stated, it is increasingly difficult for data storage and processing (cloud) service providers to be aware of all data localisation restrictions that are in place at a given time, because of the multitude of regulators and agencies and of their varying approaches to technology and data transfers.

Therefore, only a legislative instrument would be appropriate to solve the problems, as non-legislative initiatives would not replace the current patchwork of applicable legislation and therefore retain legal uncertainty. As was demonstrated in the previous sections, perceived localisation by the market is an important obstacle to data mobility. As the policy objective is to take these obstacles away, Options 1 and 2 would be disqualified.

According to certain stakeholders, awareness-raising around a legal principle on the free flow of data is important. The government of the United Kingdom phrased it accordingly while discussing its favoured policy option in a position paper submitted as answer to **the public online consultation**: "*The European Commission proposes a new consolidating regulation which provides clarity and legal certainty […]. To be effective, this should be accompanied by awareness raising in Member States […]*" Option 2 foresees in such **awareness raising** around the Free Flow of Data principle (awarding this task to the single points of contact group). Therefore, Option 2 would be in line with these stakeholders' views.

6.4.4.2 Data availability for regulatory control by Member State authorities

During the **structured dialogues with the Member States** the availability of data for regulatory control emerged as a key concern. During the first dialogue the fact that cross-border storage could in some cases mean that data would be unavailable for inspection, was flagged by Member States as a 'key challenge or threat' of a future free flow of data right. In the second dialogue this was reversed to a positive 'functional requirement' to flank a potential free flow of data right: Member States indicated to be willing to remove certain data localisation restrictions if availability of certain data would be guaranteed by another provision of the legal act. At the end of the dialogue process,

[116] 289 respondents participated in this particular multiple choice question, of which the outcome is that 'a legislative instrument' is the most favoured option. However, respondents could indicate multiple options.

during the third meeting, the majority of Member States agreed that data availability should be a building block of a forthcoming free flow of data proposal.

22.3% of stakeholders responding to **the public online consultation** identified the immediate availability of data for supervisory authorities as an important enough issue to keep (some form of) data localisation restrictions to safeguard it, while at the same time a majority of respondents voted for taking away data localisation restrictions in general. This clearly shows that stakeholders feel that data availability for regulatory control is an important issue that needs to be tackled.

Option 2 will address these legitimate concerns by providing certainty on private undertakings' responsibility to provide data and strengthening Member State cooperation. Appointing single points of contact in the Member States and putting in place a cooperation framework on data issues should further promote the effectiveness of the principle of data availability for regulatory control and its development via model clauses and practices. Therefore, Option 2 would correspond to the views of the majority of stakeholders.

6.4.4.3 Switching and porting data between providers and IT systems

Of the stakeholders that participated in the **public consultation**, most argued for non-legislative forms of EU intervention, such as setting standards or addressing the issue through developing model-contracts for cloud service providers.

In written contributions to the public consultation, a small majority reacted positively when asked about their attitudes towards a more general portability right for non-personal data. Although they were not specifically consulted about the introduction of data portability rights for cloud switching, many of the respondents to the public consultation were also cautiously positive towards the possible EC introduction of such rights.[117] When it comes to cloud-specific portability rights, several positive effects were cited by the respondents, such as reduced vendor lock-in, increased competition, new business opportunities, more data-driven innovation and research and better convenience for the customers. Among the negative effects cited by the respondents were increased financial and technical burdens on providers and the possible disclosure of IPR and trade secrets.

One responding organisation to this open question explained its position by drawing a comparison between portability rights for individuals regarding their personal data and the data flows that businesses deal with: "*Organisations using cloud services are no different to consumers in terms of their need for the portability of the data they collect with these systems and services, it is the history of their organisations business transactions and the portability of such data is an essential element of protecting any organisations assets and capability.*"[118]

Among the participants in the **workshop on cloud switching**[119] (who were all either cloud service providers or business customers of such services), about half considered there is need for a European regulation to ensure a right to port data in view of switching cloud service providers[120]. There was a preference among the participants for principles-based legislative initiative rather than more detailed legislation, as too much detail in the provision might hamper the development of flexible and innovative solutions.

Certain **Member States** have also shown interest in a legal right to data portability. The **French** Digital Council has announced its support of an EC initiative to introduce legal rights to portability

[117] Stakeholders from certain more industrial sectors, such as the transport, utilities and energy sectors, as well as the media sector, were generally more positive towards the introduction of a data portability right in order to facilitate cloud switching.

[118] Answer from Mydex CIC (United Kingdom)

[119] Workshop "Data and application portability in the cloud: current challenges & policy scenarios", Workshop organised by IDC and Arthur's Legal (SMART 2016/0032), 18 May 2017. Workshop report accessible via: https://ec.europa.eu/digital-single-market/en/news/stakeholder-dialogue-building-european-data-economy

[120] The polarisation observed between stakeholders calling for legal actions on portability and those opting for softer measures corroborates the input provided by Member States at the occasion of the 3rd structured dialogue.

of non-personal data[121], as discussed in the EC Communication on Building a European Data Economy. The **Estonian** government has also recently published a vision paper on the free movement of data in which they elaborate on the possible future framework for data access and portability[122]. Although no direct call is made for the development of new data portability rights, the Estonian government clearly sees the need to address the issue, claiming that "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", and that " The right to data portability is relevant both in the B2C and B2B contexts".

Sub-option 2a

As indicated above, many stakeholders that participated in the public consultation and the dedicated workshop on switching cloud providers, propagated a soft law, market driven approach to porting data and switching providers/IT-systems, as they believed that a portability right could potentially curb innovation in the market. This sub-option, relying on self-regulatory codes of conduct, would therefore better respond to the vision of the majority of stakeholders.

6.4.4.4 Security of data processing

Nearly all stakeholders with an IT background state that security of data processing would benefit from increased data mobility. Other stakeholders concur with this, or remain silent on the topic. Keeping this in mind, it could be inferred that their opinion would be that Option 2 is preferred, as it proposes to introduce a principle of free flow of data within the EU and the review of existing measures. This would enhance legal certainty to cyber security providers, meaning that they would be able to deliver better cyber security services to their customers, for instance by doing cyber security updates at once for all customers, regardless of their location in the EU.

Sub-option 2a

No significant stakeholders' views were received regarding this Sub-option, as it was not tested in the public online consultation. This is because Sub-option 2a relies completely on existing security requirements. Assuming that these requirements achieve the policy objectives in an efficient manner, stakeholders' judgment would be that the sub-option is equally positive as Option 2.

6.5 Option 3: Detailed legislative initiative to ensure trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems

6.5.1 Economic impacts

6.5.1.1 Free flow of data across borders

As this option would establish pre-defined, harmonised white or black list of localisation restrictions, as well as a dedicated platform to ensure transparency around them, it would have a large impact on data localisation restrictions and would provide legal certainty. At the same time, it can be expected that the option would **only moderately reduce the number and range of data localisation restrictions and prevent the emergence of new restrictions, since the pre-defined assessments approach would incite Member States to seek listing entire sectors or types of data as areas of justified restrictions**. Also, this option and the measures included therein would entail a higher regulatory burden for the Member States' public administrations. As the benefits of

[121] CNNum, "La consécration d'un droit a la portabilité des donneés non-personnelles", New Opinion of the French Digital Council on the Free Flow of Data in the European Union. Enshrining a right to non-personal data portability. Also: https://cnnumerique.fr/wp-content/uploads/2017/05/OpinionCNNum_FFoD_ENG-1.pdf

[122] Ministry of Economic Affairs and Communications of Estonia, "Estonian Vision Paper on the Free Movement of Data: the Fifth Freedom of the European Union", available at: https://www.eu2017.ee/sites/default/files/inline-files/EU2017_FMD_visionpaper_1.pdf

these more stringent measures could not be justified, the precautionary and better regulation principles would not be well served by this intrusive option.

In terms of **impacts on the cost and choice for users,** Option 3 would relieve organisations using external data services from negative **indirect effects**. To recall, it is reasonable to assume that under the baseline scenario and in the absence of intervention the additional costs borne by the cloud service providers due to data localisation restrictions would be passed on to users (e.g. cloud providers might charge a premium for the use of cloud data centres in particular locations). In fact, prices for the same quality of services can differ up to 50% between different Member States[123].

6.5.1.2 Data availability for regulatory control by Member State authorities

Option 3 foresees to establish a detailed cooperation mechanism to enforce the possibility for public authorities to effectively obtain data subject to detailed procedures, when it is stored or processed in another Member State. This type of intervention will require competent authorities to meet deadlines for answering the enquiries by other Member States, and common request and response templates would be specified for the implementation of the policy initiative. As for the previous two options discussed, the impacts on the business sector from provision easing data availability for regulatory control by Member States authorities are likely to be indirect.

This option would probably incur a higher increase in **coordination costs** for the **Member States' administrations** as compared to Option 2 due to the number of elements in the process that will have to be harmonised (including templates and dispute resolutions mechanisms). The evidence from the structured dialogue with the member states is not clear on whether the benefits (similar to the ones from Option 2) would overcome the costs (higher than Option 2).

The impacts on the **business sector** under this option are going to be equally sizeable as under Option 2 and of the same indirect nature.

6.5.1.3 Switching and porting data between providers and IT systems

As outlined in section 5, this option would establish both the principle of switching / porting facilitation and harmonise the key technical and legal conditions (e.g. concerning types of data, usable formats / structures, timeliness). In section 2.3 the trade-off between the regulatory burden on providers and the higher operational efficiency of the business end-users was described. This trade-off would be even more radical under Option 3, which would be more prescriptive in nature. Too invasive a regulatory intervention may also **stifle innovation and undermine growth** of the cloud data services sector in Europe.

The scant quantitative evidence currently available and the results of the support study and the public consultation do not seem sufficient to argue the case for the type of strong regulatory intervention under Option 3.

This is in line with stakeholders' concerns emerging from **the public consultation** about overly prescriptive regulation. They suggest that business models and types of non-personal data are too different to allow for full regulatory intervention. Rather, a principle-based approach is advocated.

6.5.1.4 Security of data storage and processing

This option entails developing common standards, a European certification scheme for the security of storage and processing of data. Their use would be mandated. The economic impacts are qualitatively very similar to those of Option 2, but the magnitude of their economic impact on business is likely to be wider as it would become an obligation for all companies, who would have to adopt the standards irrespective of their size and cross-border activity.

[123] *Supra*, p.14

6.5.2 Environmental and social impacts

6.5.2.1 Free flow of data across borders

Option 3 would have a positive impact on the environment, since cloud service providers and organisations using in-house data storage or processing IT systems would have more opportunities to deploy data storage or processing infrastructures in those locations which are optimal from the environmental point of view and to adopt innovative approaches to the use of energy in data centres.

The social/employment impacts foreseen by Option 3 are similar to those in Option 2, so the reader is referred to section 6.4.2.

6.5.2.2 Data availability for regulatory control by Member State authorities

Policy action on improving data availability to Member State authorities for regulatory control purposes would increase cross-border data mobility because of raised levels of trust both with market participants and with Member States authorities. Therefore, there would be positive environmental impacts flowing from this intervention area under Option 3, in line with the previous section.

6.5.2.3 Switching and porting data between providers and IT systems

The assessment of environmental and social impacts for this option is the same as for Option 2.

6.5.2.4 Security of data processing

As Option 3 contains the same provisions on security as Option 2, the impact on environmental and social issues can be considered the same.

6.5.3 Impact on Member States' public authorities

6.5.3.1 Free flow of data across borders

The administrative burden on Member States' public authorities posed by Option 3 would be significantly higher than for the other options. The reason is the proposed set-up of a new Committee under EU law. Member States' civil servants would have to travel to Brussels more frequently than in Option 2. This would result in human resources costs of 0.75 FTE, i.e. 0.25 FTE more than in Option 2 as a result of more frequent meetings and travelling by Member States' civil servants. On top of this 0.75 FTE, there would be an additional 0.5 FTE needed because of the high number of implementing acts (and the resulting comitology work) that is envisaged under this policy option. It would therefore mean a total of 1.25 FTE per Member State. Using the institutional cost estimation tool, this would mean an average annual cost of EUR 83.460 per Member State.[124]

6.5.3.2 Data availability for regulatory control by Member State authorities

As Option 3 would place any actions on this intervention area under the comitology mechanism mentioned in section 6.5.3.1, the administrative burden for this intervention area will be shared with the free flow of data area and will not generate extra burden in excess to this.

6.5.3.3 Switching and porting data between providers and IT systems

The expected impacts of Option 3 on Member States' public authorities are the same as those of Option 2 for the intervention area of switching and porting data between providers and IT systems, because this option leaves the responsibility with the private sector.

[124] The "Institutional Cost Estimation tool", used to calculate Full Time Equivalent cost parameters, was developed in the context of the support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005).

6.5.3.4 Security of data processing

The expected impacts of Option 3 on Member States' public authorities are the same as those of Option 2 for the intervention area of security of data processing, as both options contain the same policy approach to this area.

6.5.4 Stakeholder views

6.5.4.1 Free flow of data across borders

In position papers submitted to the Commission in the framework of **the public online consultation**, several stakeholders have emphasized the importance of awareness raising around the principle of the free flow of data. In their opinions, Option 3 would be probably less convincing than Option 2 because Option 3 is a purely legislative option and makes no reference to awareness raising activities. The reason is that Option 3 foresees comitology as execution mechanism, instead of a cooperation group made up of representatives of Member States' civil services. Without awareness raising, these stakeholders could argue, it is not efficient to adopt legal principles on the free flow of data as this would insufficiently address the legal uncertainty and lack of trust problems that were identified by nearly all stakeholders.

6.5.4.2 Data availability for regulatory control by Member State authorities

As indicated above, stakeholders identified data availability for regulatory control as an important issue in their responses to the public online consultation.

Option 3 would meet stakeholders' views in this respect, as it would develop a detailed cooperation mechanism to enforce the possibility for public authorities to effectively obtain data in a timely manner, when it is processed in another Member State.

6.5.4.3 Switching and porting data between providers and IT systems

Although around 60.6% of stakeholders participating in the public consultation support the introduction of a specific right to ensure the possibility of switching between providers and IT systems, almost all stakeholders have pointed to the risk of being too specific in proposed legislation.

Stakeholders emphasize that being over-prescriptive is a risk regarding multiple elements of a switching right, but technical standards were mentioned most in this context. As one respondent put it: "*Rebuilding IT solutions entails high costs. Imposing similar demands on machine-generated data would mean enforcing technical solutions, which would hardly benefit innovation and competitiveness in Europe*."[125]

Also in the cloud switching workshop[126] many participants were positive towards the establishment of a legal principle of data portability to facilitate switching, however many explicitly noted that any such right should not be too detailed, as too many prescriptive solutions in law might prevent the industry from coming up with good solutions.

6.5.4.4 *Security of data processing*

As Option 2 and 3 contain the same policy approach to this area, stakeholder views for security of data processing would here be the same as for Option 2. Therefore, the reader is referred to section 6.4.4.4.

[125] IBEC Position Paper submitted to the Public Online Consultation 'European Data Economy'
[126] Workshop, "Data and application portability in the cloud: current challenges & policy scenarios", 18 May 2017, for Study SMART 2016/0032, IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017.

7 How do the options compare?

This section presents a comparison of the options in the light of the impacts identified. The options are assessed against the criteria of efficiency of reaching the policy objectives, potential impacts in terms of economy, environment, society and financial burden, as well as taking into account the support expressed by the different stakeholders. *For each of the different categories, the options*[127] *receive scores on a scale from -2 to +2, taking into account the following rules:*

-2: directly negative impacts
-1: indirect negative impacts
0: neutral
+1: indirect positive impacts
+2: direct positive impacts[128]

In the descriptions below, an explanation of the scoring will be provided. The calculated total scores per option are displayed in the last row of the table below summarising the findings.

Effectiveness

In this comparison exercise, effectiveness is defined as the ability of the options to reach the specific policy objectives of this initiative.

Option 1 would use non-legislative initiatives and a strengthened enforcement of existing legislation to promote the stated policy objectives. Such an approach could persuade Member States to remove certain existing data localisation restrictions, as was indicated by the structured dialogue with the Member States. Moreover, a strengthened enforcement approach could be an improvement on the baseline scenario. However, there would be no clear legal framework for discussions with Member States and the impact of infringement procedures would be limited and likely to take considerable time to deliver results. This leads to an overall indirect negative scoring for effectiveness **(Option 1: -1).**

Option 2 would prevent Member States from putting in place unjustified data localisation restrictions, requires the review and evaluation of all existing data localisation restrictions and foresees a notification mechanism in case Member States intend to put in place new (in their view justified) data localisation restrictions. It would also introduce the principle of switching and porting data between cloud service providers and back in-house, but it avoids prescriptive and technical legislation in the first instance. The same method applies to the area of security of data processing and storage. This option would therefore achieve all four policy objectives **(Option 2: +2)**. **Sub-option 2a** also receives a positive scoring for effectiveness, as the policy objectives of easier switching and porting of data and security of data storage and processing can also be attained by relying on existing instruments and self-regulation. More specifically, the reassurance provided by Sub-option 2a that the legal proposal would avoid any overlap with other EU security instruments, would lead to a higher level of legal certainty **(Sub-option 2a: +2).**

Effectiveness-wise, **Option 3** would be less likely than Option 2 to realise the policy objectives set out in section 4 of this Impact Assessment. By enshrining detailed provisions in law on what constitutes (un)justified data localisation restrictions, and forbidding the existence of all unjustified data localisation restrictions along these lines, it would significantly lighten up the existing situation. But it would also risk inciting Member States to list entire sectors or types of data as areas of justified restrictions and therefore only moderately reduce the number and range of data localisation restrictions and prevent the emergence of new restrictions. The positive impact in terms of reaching the policy objectives is therefore less predictable **(Option 3: +1)**.

[127] Sub-option 2a will only be described when its scoring deviates from Option 2.
[128] As 'coherence' is not a scalable issue but of a binary nature (something *is* or *is not* coherent), the following scoring method will be used for coherence: -2: 'coherence problems' / 0: 'no coherence problems'.

Economic impacts

As **Option 1** would not change the more fundamental problem of localisation by the market as a result of legal uncertainty and a lack of trust, it is not deemed to generate positive economic effects **(Option 1: 0)**.

By establishing a clear legal principle accompanied by cooperation between and with Member States as well as self/co-regulation, **Option 2** will enhance legal certainty in the short term, while staying relevant and effective in the long term. This option would have a much stronger impact in addressing the problems related to legal uncertainty and lack of trust, which is needed for a true change in market dynamics, removing 'self-imposed' localisation. Evidence gathered for this Impact Assessment shows that this would have the most significant economic effects **(Option 2: +2). Sub-option 2a** may lead to less effective mitigation of market dynamics leading to 'self-imposed localisation'. This is because, it is harder to successfully conduct awareness raising campaigns around self-regulation (e.g. on switching and porting data) than around a new legal right (e.g. the right to switch and port data). On the other hand, as indicated in section 6.4.1.3, the introduction of a portability right could lead to significant compliance costs for cloud service providers. Self-regulation, however, would present the cloud service industry with the opportunity and responsibility to self-regulate while minimising compliance costs. Also in the area of security of data storage and processing, Sub-option 2a yields positive economic effects, as it will enhance legal certainty for businesses, clarifying that any currently applicable security requirements will remain applicable to them regardless of the location of the storage or processing in the EU and also under potential outsourcing of these activities. Therefore, sub-option 2a receives a positive scoring for economic impact as well (**Sub-option 2a: +2).**

Option 3 could also lead immediately to significant burden for businesses, through very detailed technical specifications for switching between providers. Therefore, although it will likely reduce the number of data localisation restrictions to a degree, it will only get an indirectly positive score in terms of economic impacts **(Option 3: +1).**

Environmental & social impacts

Because **Option 1** envisages the use of existing legislation to eliminate unjustified data localisation restrictions at least to a certain degree under this option, it can have indirectly positive effects in terms of environment and employment **(Option 1: +1)**.

Because **Option 2** is expected to achieve all four policy objectives efficiently, this will yield positive economic and social impacts, as explained in section 6.4.2. However, as these impacts will be of indirect nature (e.g. through the relocation of data centres), the scoring is kept at +1 **(Option 2: +1)**. This would be the same for Sub-option 2a **(Sub-option 2a: +1).**

As **Option 3** would also decrease the number of data localisation restrictions, there will also be positive environmental and social impacts, As in Option 2 these will be of an indirect nature **(Option 3: +1).**

Coherence with existing legislation

As **Option 1** concerns a soft-law approach, the option will however not lead to problems of coherence with existing EU-legislation **(Option 1: 0)**.

Option 2 is nearly consistent with all existing EU legislation, because its principles merely complement the provisions in existing legislation, such as the General Data Protection Regulation. Its scope explicitly does not overlap with this regulation. However, the Option would run the risk of overlapping with other EU instruments on security of data storage by providing for cloud specific certification schemes, notably with the NIS Directive **(Option 2: -2)**. **Sub-option 2a** ensures full coherence with existing EU legislative instruments, because it is consistent with the GDPR in the

same way as Option 2, but leaves any EU policy actions on security to the scope of other/existing EU instruments, such as the NIS Directive **(Sub-option 2a: 0).**

As regards coherence, **option 3** would risk overlapping with existing mechanisms, for example in the area of data availability for regulatory control, because currently there are already many sectoral cooperation mechanisms in place **(Option 3: -2)**.

Administrative burden on Member States' public authorities

Option 1 will lead to a higher administrative burden for both the Member States and the Commission, because of the strengthened enforcement of existing legislation. This, however, will be in placed in the category of indirect costs **(Option 1: -1).**

Since **Option 2** does not envisage prescriptive detailed provisions it will achieve the objectives of the initiative at a limited and reasonable cost to the public authorities and market players. It would however lead to direct costs for the Member States in terms of human resources **(Option 2: -2).** This would be the same for Sub-option 2a **(Sub-option 2a: -2).**

Option 3 will result in direct higher burdens for Member States public authorities, because of the likelihood of many implementing procedures. **(Option 3: -2)**.

Stakeholder support

Stakeholders across the spectrum have strongly advocated legislative action to ensure free flow of data in the EU. Therefore, **Option 1** receives a -2 as it relies entirely on soft measures. However, on the intervention area of switching and porting data between cloud service providers, they were less in favour of legislative action. Therefore, in this area it receives a 0. Therefore, the overall score for stakeholder support will be averaged out to -1 **(Option 1: -1).**

Option 2 combines measures that are supported by stakeholders as best ways to foster the free movement of data in the EU single market **(Option 2: +2)**. **Sub-option 2a** will also obtain a positive scoring in this category, many stakeholders that were in favour of a legal right for the free flow of data, propagated a soft law approach to porting data and switching providers/IT-systems, as they believed that a portability right could potentially curb innovation in the market **(Sub-option 2a: +2).**

For **Option 3**, stakeholders' views were of diverging nature across the different intervention areas. As indicated before, most stakeholders see legislative intervention as suitable to introduce a free flow of data principle. However, they have not advocated a *detailed* legislative initiative. This results in a score of +1 for stakeholder support in this intervention area. Regarding switching for porting data, however, the majority warned the Commission for being too prescriptive in terms of prescribing technological standards, as this could be a barrier for innovation, leading to a -2 on this intervention area. Therefore, the stakeholders support is averaged to -1 **(Option 3: -1)**

Impacts	Option 0: Baseline Option – no EU policy change	Option 1: Non-legislative initiatives to promote free flow of data	Option 2: Principles-based legislative initiative and Sub-option 2a: Combination of principles-based legislation and self-regulation	Option 3: Detailed legislative initiative
Effectiveness	**0**	**-1**	**Option 2: +2** ***Sub-option 2a:* +2**	**+1**
Economic	**0**	**0**	**Option 2: +2** ***Sub-option 2a:* +2**	**+1**
Environmental & Social	**0**	**+1**	**Option 2: +1** ***Sub-option 2a:* +1**	**+1**
Coherence with existing legislation	**0**	**0**	**Option 2: -2** ***Sub-option 2a:* 0**	**-2**
Burden on MS authorities	**0**	**-1**	**Option 2: -2** ***Sub-option 2a:* -2**	**-2**
Stakeholders' support	**0**	**-2 (free flow of data)** **0 (switching & porting data)**	**Option 2: +2** ***Sub-option- 2a:* +2**	**+1 (free flow of data)** **-2 (switching & porting data)**
Total	**0**	**-2**	**Option 2: 3** ***Sub-option 2a:* 5**	**-2**

For each of the different categories of consideration, the options received scores on a scale from -2 (direct negative impacts) to +2 (direct positive impacts). The calculated total scores are displayed in the last row.

8 Preferred option

Based on the above comparison, it appears that on balance Option 2a is the option that would best achieve the objectives of the initiative, taking into account the criteria of effectiveness, economic impacts and stakeholder support.

By combining clear legal principles, transparency requirements, clarifying the applicability of current security requirements, cooperation between and with Member States through the establishment of an expert group and self-regulation, the option will enhance legal certainty and raise trust levels, deliver tangible results in the short term (especially compared with the baseline option and option 1), while leaving substantial flexibility for the framework to evolve and adapt. Option 2a also combines measures that are supported by stakeholders as best ways to foster the free movement of data in the EU single market.

Subsidiarity, proportionality and coherence of the preferred option

The preferred option complies with the principle of subsidiarity, as the EU digital single market in this field cannot be accomplished by Member States acting nationally.

In particular, Option 2a would result in an effective and coherent framework in all the four intervention areas of this initiative:

(i) The combination of a legal free movement of data principle, notification, and review and transparency requirements would give appropriate incentives to remove and prevent data localisation restrictions across the EU single market.

(ii) Strengthening the commitment of market players to provide data for regulatory control even if it is stored in another Member State (legal principle) and a complementary administrative cooperation between the Member States where needed, would reinforce the case for the free movement of data in the single market.

(iii) Self-regulation and codes of conduct would induce a market-driven progress towards free movement of data across data cloud service providers and/or in-house IT systems in the single market.

(iv) Clarification that existing security requirements remain applicable to data storage and processing in other Member States and under outsourcing agreements would foster trust and facilitate a single market for this type of services and activities.

The preferred option does not go beyond what is necessary to solve the identified problems and is proportionate to achieve its objectives. Firstly, **Option 2a will rely to a high degree on the existing EU instruments and frameworks**: the Transparency Directive for notifications of data localisation restrictions and different existing frameworks ensuring data availability for regulatory control by Member States, thereby limiting additional administrative burdens on Member States. Secondly, the approaches to the movement of data across borders and across cloud service providers / in-house IT systems would seek balance between EU regulation and the public policy interests of Member States as well as balance between EU regulation and self-regulation by the market.

As regards switching / data porting, Option 2a would also be coherent with the IPR protection mechanisms of the Database Directive and the Trade Secrets Directive - it would not require any disclosure of IPR-protected information. Secondly it would not preclude foreign operators from accessing the EU market, would not treat foreign providers differently from EU providers or other foreign providers.

9 How would actual impacts be monitored and evaluated?

The Commission will ensure that the action selected in this IA contributes to the achievement of the policy objectives defined in Section 4. The monitoring process could consist of two phases:

The first phase would concentrate on the short-term and start right after the adoption of the legislative act. During this phase the Commission would engage with Member States (e.g. groups of experts) in order to increase their awareness and understanding of the new rules and stimulate the adoption of pro-active approaches when it comes to notifying data localisation restrictions and ensuring their transparency. The Commission would also engage with the relevant stakeholders in order to increase their awareness and understanding of the new rules.

The second phase would focus on the mid-to-long-term and would address direct effects of the rules contained in the legislation. The table below presents the **operational objectives** corresponding to the identified specific policy objectives, the indicators that would be used to monitor progress towards meeting the objectives as well as the possible sources of information. The information-gathering would start immediately after the beginning of application of the legislation and then continue every year (every second year in the case of the number and use of dedicated information channels).

9.1 Monitoring of the preferred policy option

The preferred option selected above will be monitored by the indicators listed in this section. Different indictors and sources of information are listed for the different operational objectives.

Figure 9 – Operational objectives for the preferred option

Area	Operational objectives	Indicators	Sources of information
Free flow of data	Prevent the adoption of unjustified and/or disproportionate national measures, eliminate existing unjustified and/or disproportionate national measures	The prevention indicator developed to measure the ability of the procedures provided by Directive 2015/1535 (the Transparency Directive) to prevent barriers to trade[129]	Internal: Commission services Single points of contact/ expert group
	Stimulate dissemination of information on data localisation restrictions by Member States, aggregate the information at the EU level	The number of dedicated information channels (websites, applications, etc.) To the extent the relevant data is available - the effective use of the information channels	This information would be obtained from publicly available sources or directly from Member States or the Single points of contact expert group
	Foster the adoption of data storage services	Increase in the % of European companies using cloud (hosting companies	Eurostat survey Single points of contact

[129] The ratio of the sum of the comments and detailed opinions of one year, divided by the total number of notifications which is then filtered to eliminate double counting due to the fact that more than one Member State can have a detailed opinion on the same notified draft law and/or that a Member State and the Commission may file a detailed opinion on the same draft law. For further details see the Impact Assessment accompanying the Proposal for a Directive on the enforcement of the Directive 2006/123/EC of the European Parliament and of Council of 12 December 2006 on services in the internal market, laying down a notification procedure for authorisation schemes and requirements related to services and CEPS Policy Brief, Anabela Correia de Brito and Jacques Pelkmans, "Pre-empting Technical Barriers in the Single Market", No. 277, 11 July 2012.

		database or CRM)	expert group
Data availability for regulatory control by MS	Stimulate exchange of information among MS and collaboration on data request	Number of consultations among MS	EDPR Single points of contact expert group
	Provide clarity on applicable law and jurisdiction	Decrease in the % of companies (large or SMEs) worried by unclear jurisdiction / applicable law	Eurostat survey Single points of contact expert group
Switching and porting data	Lower switching barriers for users	Decrease in the % of companies (large or SMEs) worried by the difficulty to unsubscribe or change cloud service provider	Eurostat survey Single points of contact expert group
Security of data storage and processing	Improving the level of actual and perceived security linked to data storage	Decrease in the % of companies (large or SMEs) worried by the risk of security breach Decrease in the number of incidents involving data centres	Eurostat survey Single points of contact expert group Industry ENISA Annual Threat Landscape

9.2 Sources of monitoring

9.2.1 Single points of contact expert group

The legislation will require Member States to designate a single high-level contact point to coordinate and facilitate the application of the measure in their respective jurisdictions. These contact points will serve collectively as an expert group that would allow for the exchange of information and for a process of constant monitoring by the Member States and the Commission. Furthermore, the experience of the expert group will serve as a valuable source of information during the ex-post evaluation phase of the legislation, which should take place five years after its application.

9.2.2 The Eurostat survey and its indicators

Eurostat tracks indicators on enterprises' use of cloud computing services in the EU[130]. Eurostat also conducts a bi-annual survey of the companies operating in the market tracking the factors limiting the enterprises' use of cloud computing-related services. This data can be used to determine a benchmark and to monitor the impact on the business sector of the provisions adopted.

9.2.3 DESI and the European Digital Progress report

The **European Digital Progress Report** (EDPR) covers 28 Member States and provides comprehensive data and analysis of market, regulatory and consumer developments in the digital economy. It is based inter alia on DESI[131] **(Digital Economy and Society Index**) combining the quantitative evidence from the DESI with country-specific policy insights. DESI is based on data

[130] http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises The survey is carried out every two years on a sample of almost 2000 firms in the EU

[131] DESI reports available here: https://ec.europa.eu/digital-single-market/en/desi

from Eurostat and various studies and surveys[132], and is structured in five dimensions: Connectivity, Human Capital, Use of Internet, Integration of Digital Technology and Digital Public Services. DESI already tracks the degree of take-up of cloud services, but more specific indicators may be designed.

Insights on national policies come directly from the in-house expertise and research of country teams and daily policy work on data policy issues and the input from Member States. The information provided will be complemented by information collected through country visits.

9.2.4 The ex-post evaluation

A comprehensive evaluation could take place 5 years after the start of application of the rules. This evaluation will be executed in close cooperation with and relying on the information provided by the single points of contact of the Member States.

Since the principle of free flow of data is a pre-condition for the emergence of innovative virtualised and/or distributed data storage and processing technologies, as well as an enabler of data-driven innovation in general[133], this evaluation will have to assess the impact that the policy initiative suggested in this IA had on the capacity of businesses and the public sector to innovate as a consequence. It may seek synergies with the evaluation of other data policies.

Taking into account that data storage and processing are features of numerous services provided by both private and public sectors, the hurdles (extra costs and administrative burden) associated with (proliferating) data localisation restrictions could lead, indirectly, to negative impacts on consumers and citizens as users of those services. For example it could lead to no service being provided where otherwise it could have been provided - such as cross-border digital public services - or less attractive terms and conditions of a service[134]). The evaluation will have to cover these aspects and assess the extent to which the option chosen had an impact on the development of the Digital Single Market. It would need to examine whether it contributed to reducing the number and range of data localisation restrictions and to enhancing legal certainty and transparency of remaining (justified and proportionate) requirements, which is the **first specific objective** pursued by this initiative. Moreover, repercussions could be on the **fourth specific objective** concerning trust in / security of (cross-border) data storage and processing, since often localisation is driven by legal uncertainty / lack of trust in the market, as emphasised by the results of the public consultation. The evaluation will also have to assess whether the policy initiative has contributed to improve the trust in free flow of data from the Member States and whether they can reasonably have access to data stored abroad for regulatory control purpose (**second specific objective**). The evaluation shall be accompanied by an ad-hoc industry survey to assess progress in the area of switching (**third specific objective**), pricing and take-up of cloud services. A special edition of Eurobarometer may be considered for this purpose.

[132] Indicators and sources are available here: http://digital-agenda-data.eu/datasets/desi/indicators

[133] E.g. data localisation restrictions make it complicated for a researcher to aggregate data from various sources and use advanced data analytics tools.

[134] Localisation tends to reduce services and increase prices for domestic consumers: http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf

GLOSSARY

Acronym	Meaning
API	Application Programming Interface
CAGR	Compound Annual Growth Rate
CNNum	Conseil National du Numérique – French Digital Council
CRM	Customer Relationship Management
CSP	Cloud Service Provider
DEI	Digitisation of European Industry
DESI	Digital Economy and Society Index
DLR	Data Localisation Restriction
DSM	Digital Single Market
ECFR	European Charter of Fundamental Rights
EDPR	European Digital Progress Report
EIO	European Investigation Order
ENISA	European Network and Information Security Agency
FFD	Free Flow of Data
FTA	Free Trade Agreement
FTE	Full Time Equivalent
GDPR	General Data Protection Regulation
IA	Impact Assessment
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IoT	Internet of Things
NIS	Network and Information Security
NPV	Net Present Value
PaaS	Platform as a Service
QoS	Quality of Service
R&D	Research and Development
SaaS	Software as a Service
SMTD	Single Market Transparency Directive
TFEU	Treaty on the Functioning of the European Union

EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 304 final

PART 2/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

ANNEXES TO THE IMPACT ASSESSMENT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

on a framework for the free flow of non-personal data in the European Union

{COM(2017) 495 final}
{SWD(2017) 305 final}

ANNEX 1: PROCEDURAL INFORMATION

The initiative is led by DG CONNECT. The agenda planning reference is PLAN/2016/164.

The Impact Assessment was prepared by a project team of DG CONNECT and was closely coordinated with the Inter-Service Steering Group (ISG). Following its meetings in 2016, the ISG held two meetings, on 30 June 2017 and on 20 July 2017, to discuss the revised Impact Assessment. The following DGs and services participated: SG, CNECT, COMP, DIGIT, ENER, ENV, ESTAT, FISMA, GROW, HOME, JUST, JRC, MOVE, OP, REGIO, RTD and TRADE. Comments and written input from the other DGs and services were duly considered and taken into account in this Impact Assessment. Numerous bilateral meetings also took place with the relevant DGs and services to discuss specific aspects and improve the diversity and pertinence of evidence and references provided, as well as the overall quality of the text.

1. Recommendations of the Regulatory Scrutiny Board

1.1. Response to negative opinion of the RSB of 25 August 2017

The Regulatory Scrutiny Board (RSB) of the European Commission examined the draft Impact Assessment and issued a negative opinion on 25/08/17. This is the RSB's second opinion and is in principle final. In its opinion, the Board identified a number of shortcomings that needed to be addressed. These issues have been addressed in this revised version of the Impact Assessment, which is the final published version. The shortcomings and the adjustment requirements have been addressed in this new version as follows:

RSB comment	Modification of the IA report
Cloud services portability. **The report fails to make a case for a new right of cloud services portability. It does not show that switching costs are excessive. The proposed portability solution would not address the obstacles to switching that the report identifies, including standardised data formats and data transfer logistics. The report does not estimate compliance costs of such portability requirements for cloud service providers. Overall, the evidence seems to point toward less stringent options.** As regards the vendor lock-in problem, the economic analysis and methodology to assess impacts should be substantially revised to better reflect the business model of cloud services, the competitive and innovative nature of the market, the views of stakeholders on obstacles to switching providers and the prerogatives of private law contracting. The report relies on two studies which are not available yet, but references to these studies in the report suggest that this does not reflect a comprehensive cost-benefit analysis. For	In response to these concerns raised by the RSB, the **IA now identifies Option 2a as the preferred option instead of Option 2.** This means the **elimination of a new right of cloud services portability** and the replacement of the prior legal obligation for service providers to facilitate switching **by a self-regulatory approach**, taking the form of codes of conduct. The objective of this change is to make sure that service providers will not be faced with excessive requirements and that the competitive and innovative nature of their market will be preserved. As the RSB clearly identified, and despite several dedicated support studies, it remains difficult to estimate accurately the compliance costs of a portability right for cloud service providers (CSPs). Self-regulation leaves the responsibility with the industry itself to make switching and porting of data easier. In this way, compliance costs will be minimised. On

instance, what about the impact of portability obligations on the cost of cloud services? In view of stakeholders' feedback, the report should explain why the option of soft law (option 2a) is not considered more effective.	the other hand, an information/transparency objective for CSPs still figures in the preferred option, in order to ensure full transparency for professional users. This should encourage the market to move to easier switching and porting for cloud customers. The Commission should assess if the development of self-regulatory measures such as codes of conduct on transparency requirements will be sufficient in facilitating the switching of providers or porting data back to users' IT systems. For a description of the revised preferred option 2a, **the reader is referred to sections 5.4 and 8 of the IA.** Also, and as requested by the RSB, the report now contains a considerably revised and expanded passage on the excessive costs of data portability under the baseline scenario. This information is to be found **in the section on the economic assessment of the baseline option for portability (6.2.1.3) and the problem section of the IA (2.3.1.)**.
Data localisation restrictions. **The report does not establish the size of location restrictions on data. It acknowledges that there is limited evidence of such restrictions and does not explore the reasons for such restrictions, or analyse their merits. The report also does not analyse the strength of observed customer preferences for local storage.** The report draws extensively on conclusions from several structured dialogues with Member States. But it does not say whether the dialogues provided support for the methodology to identify those restrictions that are unjustified and assess the proportionality of remaining restrictions.	Despite two studies, the macro-economic analysis of the impact of data localisation restrictions remains a difficult exercise. As the RSB rightly points out in its Opinion, the IA does not succeed in projecting an all-encompassing macro-economic analysis of the 45 identified data localisation restrictions. It does provide, in section 6.4.1.1., an analysis of different economic consequences of the preferred option. It is impossible to give hard figures on the impacts of identified localisation restrictions , mainly because data localisation restrictions have many different economic effects, some of which are difficult to measure (e.g. the spin-off effect on the use of innovative data technologies that are geographically dispersed by nature (such as IoT, now mentioned in section 2.3.2. of the IA). Moreover, the business case to build a data centre in a particular country relies on several factors.

	In response to these comments by the RSB, the report now stresses more clearly **(in section 6.4.1.1)** that it is directed also at future developments, **acting for the purposes of trust and legal certainty.** This should create the essential investment climate the EU needs for becoming a true data economy. In earlier changes, the problem analysis has been fundamentally reviewed, and now gives a clearer and more systematic analysis of the different types of problems, their magnitude and the reasons why they cannot be adequately addressed under existing EU law. **See IA sections 2.3.1 and 2.3.2.**
The description of policy options. **The policy options leave open a number of issues and the role of the new policy group in addressing them. Open issues include:** **- How certification would work in practice;** **- How to define portability;** **- What geographical restrictions are unjustified or disproportionate;** **- The process to make the principles-based legislation operational.** The report should define the options more precisely. Both certification and the policy group touch on issues which are common to the ENISA proposal in the same policy package. The report should justify the need for specific measures not covered in the new ENISA proposal. For certification, it should explain whether the common standards and labelling scheme for cloud service providers should be developed by the industry or by Member States. It should also assess the potential costs of the proposed solution (cf sections 6.4.1.4 and 6.4.3.4). The policy group seems to be a hybrid body. It combines committee competence, advisory and administrative cooperation functions, and responsibility for certification. The report should clarify the role of the single points of contact in Member	The RSB rightly comments that in the previous version of the IA, detailed information is missing regarding the practicalities of security certification, the definition of portability, the justification of data localisation restrictions and the process of bringing the principles-based proposal into force. The reason is that, as described in **section 5.4,** the substance of these issues is left to the discretion of an expert group, consisting of the single points of contact designated by the Member States. There is a better regulation consideration behind this choice, giving principles-based guidance on EU level but leaving practicalities to the Member States. This was also a response to calls for a cooperation framework by the Member States. In response to the RSB comments, the report now contains an extra section on broad definitions of justified vs. unjustified geographical restrictions in **section 2.3.1,** (problems) **section 5.4** (the preferred option) and **section 6.4.1.1.** (assessment of the preferred option). The RSB is correct in asserting that the relation between the cyber package, the NIS Directive and our proposal could have been formulated in a clearer way than before.

States and their policy group.	Therefore, in response to these RSB comments, the new IA adopts a new approach to ensure that the FFD proposal will provide for extra synergies between the initiatives and no overlap whatsoever with the cyber package and the NIS Directive. In response to the RSB comment on the missing cost estimation of EU action under this intervention area, it must be contended that this will depend on the possible implementing acts under the NIS Directive.

1.2 Response to negative opinion of the RSB of 28 September 2016

The RSB had previously examined an earlier draft version of the Impact Assessment and issued a negative opinion on 28/09/16. The Board made several recommendations. These were addressed in the revised version of the IA submitted to the RSB for its second opinion, as follows:

RSB recommendations	Modification of the IA report
Context and timing. **The report should establish a clearer link and coherence between the FFDI and other policy initiatives concerning data. It should more clearly demonstrate the pertinence and urgency for additional regulatory action in this policy area.** The Commission's 2015 Communication on the Digital Market Strategy for Europe outlined several policy issues that are closely related to the FFDI. These include ownership of data, access to data, interoperability of data, and liability of the use of data. The report should better explain the links between these various initiatives and show their complementarity. It should then explain the reasons for tackling the FFDI separately rather than covering it together with other related issues.	The report now explains in greater detail the links as well as the differences between the envisaged EU free flow of data cooperation framework and other data-related policy issues (such as data ownership, transfer and liability), as also explained in the Data Economy Communication of 10/01/2017. The issue of porting business data for the purpose of switching cloud service providers is now also addressed as part of this initiative. **See IA sections 1.1 and 1.2** Two **key arguments** are the following: - Effective and efficient cross-border functioning of data storage and processing, in particular through the establishment of the free movement of data principle, should be ensured before taking the other EU data policy initiatives. This would be a timely response to the growing data-intensity of economy and would constitute the foundation upon which future cross-cutting (e.g. re-use of data across borders) and sectorial (e.g. banking and finance, manufacturing,

	connected and automated driving, smart grids) data policies can be built. - For the obstacles to the movement of data, the cause is forced storage or processing of certain types of data in electronic format within a geographical zone. The main issue is therefore the removal or the prevention of data localisation restrictions which are not objectively justified on grounds of national security. The other data issues, in particular those relating to ownership, transfer and liability are not yet sufficiently clear and need further assessment before any decisions can be taken on further regulatory action.
Problem definition. **The report should present more evidence to establish the magnitude of the problems. It should also elaborate on underlying drivers to relevant restrictions on data location, such as security or law enforcement concerns. It should describe the limitations or gaps of the existing legal framework and its enforcement. On this basis, the report should substantiate the need and scope for (legal) action.** The report should provide more evidence to demonstrate the relative magnitude of the problem and its underlying drivers. There is more scope to draw on the existing external studies as well as on stakeholder input and anecdotal evidence. For instance, the report should clarify the nature of the restrictions targeted by the FFDI and confront them with Member States' concerns, for example in relation to security issues. The report should further explain the extent to which it accepts Member States' concerns with regards to data security as legitimate. Moreover, the existing legal framework (i.e., Articles 16, 26, 49, 56, 114 TFEU and at least 6 directives, notably the services, e-commerce and transparency directives) should be described and analysed in more detail. The analysis should chart existing limits in tackling the identified issues and whether these stem from enforcement problems or legislative gaps. This should strengthen the argument for new	The report now explains in much greater detail the magnitude of the problem and its underlying drivers. Specifically: - The problem analysis has been fundamentally reviewed, and now gives a clearer and more systematic analysis of the different types of problems, their magnitude and the reasons why they cannot be adequately addressed under existing EU law. **See IA sections 2.3.1 and 2.3.2.** - The report systematically gives examples of different types of data localisation restrictions. **See IA section 2.3.2 Figure 3; Annex 5 ('Driver 1' and 'Driver 2'**) - The report differentiates between potentially justified and potentially unjustified data localisation restrictions, based on the results of the structured dialogues with the Member States, studies and the Commissions own internal assessment. **See IA section 2.3.2 Figure 3; Annex 5 ('Driver 1'**) - The report analyses in greater detail to what extent the potentially unjustified data localisation measures could be addressed using the existing regulations / directives. **See IA section 2.3.2 Figure 3 and section 6.3.1.1; Annex 5 ('Driver 4')** - The report devotes more attention to legal uncertainty as a key driver of data localisation. **See IA section 2.3.1 and section 2.3.2 Figure 3; Annex 5 ('Problem**

legislation in this area. How is it expected to simplify rather than make the situation more complex, in particular when proposing a reversal of the burden of proof and setting conditionality to Member States to justify restrictions? To what extent will it be "future proof" to allow further development of the digital single market?	**2')** - The report analyses in detail the main concerns of the Member States that underpin data localisation: concerns about data availability for regulatory control/data sovereignty and concerns about the level of security of data storage and processing. The initiative will provide co-operation mechanisms between Member States and the Commission to respond to these concerns. **See IA section 2.3.1; Annex 5 ('Driver 5')** - In elaborating the potential solutions (options) the report pays considerably greater attention to the fact that the initiative should clarify the existing legal situation. The solutions would also ensure relevant technological developments are taken into account as regards possibilities to port or move data and as regards security of data. Specifically, the preferred legislative option is based on a simple and clear free movement of data principle as well as transparency requirements for any remaining justified restrictions and relies on an existing notification mechanism. The proposed cooperation mechanisms between Member States and the Commission will ensure that the free flow of data principle takes into account Member States' concerns about data availability for regulatory control and appropriate levels of security of data storage and processing. **See IA section 5.4 and section 8**
Stakeholder views and assessment of impacts. **Stakeholder views should feature more prominently throughout the report. The assessment of impacts should be better substantiated, drawing on available qualitative and quantitative evidence. The expected impact of the preferred option should be further detailed.** The potential winners and losers from this initiative need to be better identified and stakeholder views better reflected throughout the impact assessment. More quantitative and qualitative evidence from the external studies and stakeholders consultations would help	- The report now refers to the stakeholder views much more systematically and to a greater extent. In particular, the results of the 2017 online public consultation and the structured dialogues with Member States and other stakeholders, which took place from February 2017 to May 2017, are two new important sources of stakeholder views. **See numerous references in IA sections 1, 2, 5.6, 6; Annexes 2 and 5** - The report also builds on further evidence stemming from external studies and other external sources, notably the completed study SMART 2015/0054, the new IDC and Arthur's Legal study SMART 2016/0032

policymakers to accurately weigh the relative impacts of the different options. For example, with regard to Option 2, the impacts on the environment, on employment and on fundamental rights need to be more firmly based on available evidence. With regard to administrative burden, the report needs to more clearly spell out both potential new burdens (such as costs to run the new EU information platform) as well as synergies with existing procedures (such as drawing on existing notification procedures).	"Switching between Cloud Service Providers" and the new Tecnalia study SMART 2016/0029 "Certification Schemes for Cloud Computing". **See references in IA sections 2 and 6; Annexes 3 and 5** - The report now assesses systematically and in greater detail the potential administrative burden and clarifies that an existing procedure should be used for notifications. **See IA sections 6.2.3, 6.3.3, 6.4.3 and 6.5.3; Annex 3** - The report now also expands on the costs and benefits of the initiative to different categories of stakeholders. **See IA section 6; Annex 3**

2. Evidence Base for the Impact Assessment

The Impact Assessment was prepared on the basis of diverse sources, including:

- stakeholder consultations (please see Annex 2);
- publicly tendered external studies (below);
- market reviews, statistics (*e.g.* Eurostat), and desk research;
- external expertise.

a) External Studies commissioned for the Impact Assessment

i. SMART 2016/0032, IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (Ongoing) [IDC and Arthur's Legal Study (SMART 2016/0032)]

ii. SMART 2015/0054, TimeLex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions" (Ongoing) [TimeLex Study (SMART 2015/0054)]

iii. SMART 2014/0031, Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 [Deloitte Study (SMART 2014/0031)]

iv. SMART 2015/0016, London Economics Europe, Carsa and CharlesRussellSpeechlys, "Facilitating cross border data flow in the Digital Single Market", 2016 [LE Europe Study (SMART 2015/0016)]

v. SMART 2016/0029, Tecnalia, "Certification Schemes for Cloud Computing" (Ongoing)

vi. SMART 2015/0086, CRIDS (University of Namur), "Report on the public consultation on data and cloud"

b) Other external studies relied on in the Impact Assessment

i. SMART 2013/0063, IDC and Open Evidence, "European Data Market. Data ownership and Access to Data - Key Emerging Issues", 1 February 2017 [IDC Study (SMART 2013/0063)]

ii. SMART 2011/0045, IDC, "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake" (July 2012)

iii. SMART 2015/0018, TimeLex, Spark, "Clarification of Applicable Legal Framework for Full, Co- or Self-Regulatory Actions in the Cloud Computing Sector" (Ongoing)

iv. SMART 2013/43, IDC, "Uptake of Cloud in Europe. Follow-up of IDC Study on Quantitative estimates of the demand for Cloud computing in Europe and the likely barriers to take-up ", 2014, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742

c) Expert consultation

Prof. Joachim Beck was engaged as a consultant and was consulted on the structure and quality of the analysis of the Impact Assessment.

d) Other external sources / publications

Aaronson, Susan Ariel, "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", 2015.

Albright Stonebridge Group, "Data Localisation : A Challenge to Global Commerce and Free Flow of Information", September 2015, available at: http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf

Cybercrime Convention Committee (T-CY), "T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime", T-CY(2013)17rev, December 2014, available at : https://rm.coe.int/16802e726c

Directorate-General for the Internal Market and Services (European Commission), "Handbook on Implementation of the Services Directive", 2008, available at: http://publications.europa.eu/en/publication-detail/-/publication/a4987fe6-d74b-4f4f-8539-b80297d29715

ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016.

ENISA, Report "Secure Use of Cloud Computing in the Finance Sector", December 2015

ENISA, Report "Cloud Computing Risk Assessment", November 2009, available at https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

European Commission, "A guide for legal practitioners – Judicial cooperation in civil matters in the European Union", available at: http://ec.europa.eu/justice/civil/files/civil_justice_guide_en.pdf

European Commission and European Judicial Network for Civil and Commercial Matters, "Practical Guide for the application of the Regulation on taking of evidence", available at: http://ec.europa.eu/justice/civil/files/guide_taking_of_evidences_en.pdf

European Judicial Network and Eurojust, Joint Task Force Paper "Assistance in International Cooperation in Criminal Matters for Practitioners European Judicial Network and Eurojust", 6 May 2014, available at : http://eurojust.europa.eu/doclibrary/eurojust-framework/ejrelationswithpartners/ejn-eurojust%20paper%20on%20judicial%20cooperation%20in%20criminal%20matters%20%28may%202014%29/ejn-ej-paper-on-judicial-cooperation-in-criminal-matters_2014-05_en.pdf

Eurostat, "Factors limiting enterprises from using cloud computing services, by size class, EU-28", 2014 (% enterprises using the cloud); http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

Eurostat, "Statistics on small and medium-sized enterprises", September 2015, available at:http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises

The Evidence Project, Deliverable D3.1 Overview of existing legal framework in the EU Member States, Collaborative Project EVIDENCE "European Informatics Data Exchange Framework for Courts and Evidence", FP7-SEC-2013.1.4-2. Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet" (Part 2), International Journal of Law and Information Technology (2010) 18 (3): 227-247

Jonah Force Hill, "The Growth of Data localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders", Lawfare Research Paper Series, 2014, available at: https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf

Mandel, Michael, "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security", 2013

Nordås, H., et al. (2014), "Services Trade Restrictiveness Index (STRI): Computer and Related Services", OECD Trade Policy Papers, No. 169, OECD Publishing, Paris. available at http://dx.doi.org/10.1787/5jxt4np1pjzt-en

Anna-Maria Osula, "Transborder Access and Territorial Sovereignty", Computer Law and Security Review 31 (2015) 719 – 735Oxford Research, "A springboard for green data centers in Southern Norway"

Oxford Research, "Finland's Giant Data Center Opportunity",available at: http://www.oxfordresearch.fi/media/241351/finland_s_giant_data_center_opportunity_final_version.pdf

Stefan Kolb, Jorg Lenhard and Guido Wirtz, "Application Migration Effort in the Cloud – The Case of Cloud Platforms" (2015)

Trusted Cloud Europe Survey, "Assessment of Survey Responses", 15.07.2014, available at: https://ec.europa.eu/digital-single-market/en/news/trusted-cloud-europe-survey-assessment-survey-responses

XL Catlin Group, "Environmental Risks: Cyber Security and Critical Industries" (Whitepaper), 2013.

ANNEX 2: STAKEHOLDER CONSULTATION

The **initial assessment** was based on the following activities:

- Review of literature pointing to the importance of cross-border data flows for economic development, and the detrimental effect of data localisation restrictions at European level.[1]

- Data localisation restrictions were identified as a barrier to the development of cloud computing in Europe by the steering board of the European Cloud Partnership[2] in the context of the Cloud Computing Communication[3]. In a small-scale survey that was launched following the publication of the European Cloud Partnership's report, a large majority of respondents (68%) agreed on the need to review data localisation restrictions and assess alternative approaches.[4]

- Preliminary activities aimed at the identification of data localisation restrictions on the basis of stakeholder involvement.[5]

The **first round of evidence gathering** (from the 2nd half of 2015 until the 2nd half of 2016) was based on the following activities:

- In 2015 and 2016 the Commission ran two studies aimed at identifying data localisation restrictions in Member States and quantifying the impact of those restrictions on the functioning of the internal market.

- A public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy was launched on 24 September 2015.

- One study on the economic impact of cloud computing in Europe.

- Other information gathering activities (e.g. meetings and events, targeted workshops with key stakeholders and dedicated workshops in the context of the studies).

Following the negative opinion of the regulatory scrutiny board upon the first submission of the impact assessment, the **second round of evidence gathering** (from the end of 2016 until the 2nd half of 2017) was based on the following activities:

- A public consultation on Building a European Data Economy was launched on 10 January 2017.

---

1 De Brauw Blackstone Westbroek, "EU country guide: data location & access restrictions", 2013; Kommerskollegium (Swedish National Board of Trade), "No transfer, no trade: the importance of cross-border data transfers for companies based in Sweden", 2014.

2 European Cloud Partnership Steering Board, "Establishing a Trusted Cloud Europe: A policy vision document by the Steering Board of the European Cloud Partnership", March 2014. Available at https://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 27 September 2012, "Unleashing the Potential of Cloud Computing in Europe", COM(2012) 529 final.

4 European Commission, "Trusted Cloud Europe Survey: Assessment of Survey Responses", July 2014, available at https://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe-survey-assessment-survey-responses

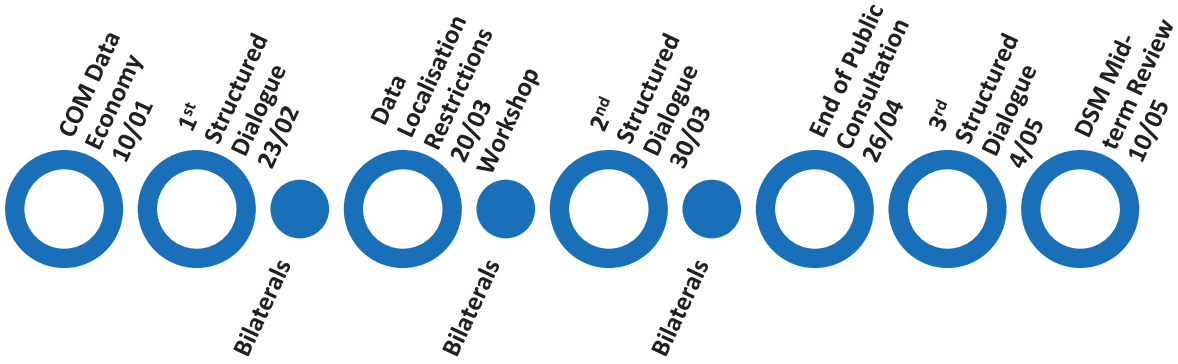
5 Workshop "Facilitating cross border data flow in Europe – on data location restrictions", March 2015, meeting minutes available at http://ec.europa.eu/digital-agenda/en/news/workshop-facilitating-cross-border-data-flow-europe-data-location-restrictions-outcome-workshop

- Three collective structured dialogue meetings with Member States to reach a common understanding of the challenges and opportunities at hand.
- Bilateral meetings with Member States to verify data localisation restrictions identified and address individual concerns.
- A dedicated study on the issue of switching of cloud providers / data porting.
- A dedicated study on cloud certification schemes and security.
- Engagement with stakeholders during the DSM Cloud Stakeholder meeting.
- Other information gathering activities (e.g. meetings and events, targeted workshops with key stakeholders and dedicated workshops in the context of the studies).

1. Overview

Structured dialogues with Member States on the Free Flow of Data

The Communication of 10 January 2017 on Building a European Data Economy announced structured dialogues on a Free Flow of Data, between the Commission and the Member States as well as other stakeholders, taking as a starting point the localisation restrictions identified so far. Three structured dialogues and bilateral meetings/calls with 16 Member States have taken place since the publication of the Communication.



Key conclusions of the structured dialogues:

The **first structured dialogue** workshop constituted an exploratory first meeting with Member States, the Commission facilitated an interactive and constructive discussion on the benefits and challenges, as well as the issues and needs of MS in view of the FFD. The key benefits and opportunities identified were economic growth; higher level of competition and innovation in the EU; better "cross-border" use of public sector services; and to promote and advance legal clarity in the EU. Whereas, the key challenges and threats outlined were a lack of mutual trust and legal uncertainty on scope of FFD.

The **second structured dialogue** workshop was an opportunity to discuss the current applicable EU legal frameworks concerning free movement of data and to further elaborate on the data localisation measures identified so far in that context. In general, participants found it very difficult to navigate through all the existing legal instruments. Some participants mentioned that the identified and anonymised rules were lacking legal clarity and that their objective was not clearly stated, which makes the proportionality test difficult.

The **third structured dialogue** facilitated a discussion on the possible building blocks of a free flow of data approach, and to collectively identify possible policy scenarios for the free flow of data in the EU. There was a sense of emerging consensus on the possible building blocks for a common FFD approach: general FFD principle; data security; data availability/cross-border access to data by authorities; data portability. Member States preferred the option of hard law with regard to a FFD principle, guidance/soft law with regard to data security and hard law and/or guidance when it comes to data availability/cross-border access to data by authorities and data portability.

Organisation and approach:

The three structured dialogue meetings with Member States have taken place and primarily aimed at promoting a common understanding of the issues at hand undermining a Free Flow of Data within the EU. For this purpose the Commission resorted during all three meetings to a *participatory leadership approach*[6] allowing for interactive and inclusive process towards a common conception of the obstacles to a Free Flow of Data and its underlying issues, and necessary steps to be taken at EU level in order to address these.

Participants to the structured dialogues

The Member States were represented by attachés and representatives from the respective national ministries and/or authorities.

1st structured dialogue workshop:

22 EU Member States + Norway were represented by 1 to 3 representatives. Luxembourg, Croatia, Latvia, Italy, Greece and Cyprus did not attend the meeting.

2nd structured dialogue workshop:

25 EU Member States + Norway were represented. Greece, Cyprus and Romania did not attend the meeting.

3rd structured dialogue workshop:

22 Member States + Norway were represented. Greece, Cyprus, Italy, Slovakia, Hungary and Bulgaria did not attend the meeting.

Bilaterals with MS

In addition to the collective structured dialogue meetings the Commission held 16 bilateral meetings/calls to discuss and verify the identified individual restrictions as well as promote a common understanding of the issue at stake. Such engagement occurred with all willing MS for which localisation requirements were previously identified (UK, LU, SLV, DE, NL, AT, ES, FI, CRO, PL, BE, BG, PT, DK, FR), or not (IT). HU, SE and IE have provided written statements instead. Romania could not respond on substance yet.

[6] The Participatory Leadership is an approach to leadership that scales up from personal to systemic usage of dialogue, facilitation, collaboration and co-creation of new solutions to address complex challenges that we face in our organizations today. It's a structured set of practices for facilitating group conversations of all sizes, supported by principles that maximize collective intelligence, welcome and listen to diverse viewpoints, maximize participation and transform conflict into creative cooperation. Participatory Leadership is increasingly used in many organizations around the globe for: Supporting the organizational change and development by engaging and empowering the collective knowledge and innovative capacity in all staff; Developing knowledge and solutions within business and services by strengthening relations and co-creating with internal and external stakeholders (collaboration across levels and departments, working across silos); Building advanced leadership capacity in the organization by training and nurturing personal leadership, collective learning and self-organization for staff to step in and take charge of the challenges facing them.

There were 8 Member States that did not receive an email with identified restrictions and therefore we have not proactively requested bilateral meetings with these countries (SLK, MAL, LV, GR, EE, CZ, CY, LT).

Public Consultation on Building a European Data Economy

The stakeholders targeted by the consultation were businesses of all sizes and from all sectors, including specifically manufacturers and users of connected devices, operators and users of online platforms, data brokers, and businesses commercialising data-based products and services. Public authorities, non-governmental organisations, researchers and research organisations and consumers were also invited to contribute.

The online survey received a total of 380 responses, including 332 responses from businesses / organisations, 6 responses from self-employed individuals, and 42 responses from citizens. Contributions mainly came from private organisations, which could be expected, since most of the issues concerned B2B contexts.

In addition, some 15 standalone contributions (i.e. not complemented by replies to the questionnaire) were received. These are available online [link to be inserted]. The authors of these contributions represent national authorities, companies, national or European business associations, insurance associations, and lawyer representatives in EU and the US. Most of these papers tackle the different sections of the consultation, with a strong focus on the access to and transfer of data.

The European Political Strategy Centre (the EPSC) has also organised a public hearing, the transcript of which serves as a contribution to the public consultation.

The Synopsis Report of the public consultation and its Annexes are available here [link].

REFIT Platform

Submission of the Royal Norwegian Ministry of Trade, Industries and Fisheries to the REFIT Platform (April 2017)[7]:

Norway points out that there is a need for a harmonized EU-law to allow for storing accounting documents in all member states, including all EEA-countries. As long as enforcement bodies have sufficient access to documentation, it should make no difference if a business keeps paper documents stored in a cabinet in their headquarter office in one European Member State, or chooses to store the same documents electronically in a cloud service with servers located in another European country.

Stakeholder Consultation Workshop for the SMART Study on Data Portability and Switching Cloud Provider

The ongoing study on 'Switching between Cloud Providers' (SMART 2016/0032) is being undertaken by IDC and Arthur's Legal. The objective of the study is to gather evidence concerning the practices of cloud service providers in relation to data and application portability within cloud ecosystems. In this context, the analysis defines portability as follows: 'Data portability is the ability to easily transfer data from one cloud service to another cloud service without being required to re-enter the data; similarly, application portability is the ability to easily transfer an application or application components from one cloud service to a comparable cloud service and run the application in the target cloud service'.

Considering the series of technical, legal and economic issues identified in the study as well as their impact on portability for different cloud stakeholders, the report elaborates on 3

[7] An opinion of the REFIT Platform is further expected in September 2017.

different policy options to facilitate portability. First, it expands on the introduction of a mandatory right for portability under EU law identifying its main components. Second, it discusses existing soft law instruments for portability reflecting on their effectiveness to address the portability issues occurring in the cloud context. Third, it explains what abstinence from any action at EU level entails. Finally, an examination of the possible economic impacts of the policy measures that could be taken at EU level to increase cloud portability shall take place, by describing the possible effects of these on demand for public cloud services.

The workshop "Data and application portability in the cloud: current challenges & policy scenarios" on 18 May 2017 had two (2) separate yet related goals: a) to present of the existing barriers limiting - or even preventing - data and/or application portability within cloud ecosystems identified in the context of the aforementioned study creating a high risk for customer lock-in and b) to identify a set of potential measures to address the barriers discussed, including the potential introduction of a new right to data portability that would not be limited only to a specific type of data.

The Workshop targeted representatives of public and private sector users (including SMEs), ICT service providers, and governmental authorities as well as Member State representatives. Over 40 participants joined for the Workshop.

Furthermore, the participants were involved in highly interactive sessions allowing them to exchange views on the challenges identified by the study and to discuss the draft set of preliminary measures captured by the workshop materials to stimulate the workshop discussion.

Stakeholder Consultation for the SMART study on Cross-border data flow in the digital single market: study on data location restrictions

The 'Cross-border data flow in the digital single market: study on data location restrictions' (SMART 2015/0054) was undertaken by time.lex, Spark Legal Network and Tech4i2. The objectives of the study were to identify and analyse legal and non-legal barriers that hinder the free flow of data within the EU, and quantify the impact of these barriers for private and public sector users, and suppliers of cloud computing services. Consequently, the final report shall contain: the identification of compliance obligations across the EU; examples of barriers which complement the analytical framework, results of a survey and in-depth interviews with stakeholders; an analytical framework that allows for the definition of concepts of barriers to the free flow of data, defining a common understanding of data requirements in the EU; the results of an economic analysis of the costs and benefits of data location restrictions and recommendations for functional requirements and future policy concepts, to facilitate cross border data flow within the EU.

The data collection for the study was done via a network of local legal and policy experts in 20 Member States, who were invited to report on at least three observed barriers that applied to at least three different types of data. Furthermore, the study team has conducted a survey and a series of interviews with selected stakeholders in order to identify non-regulatory compliance barriers.

The objective of the workshop which took place on the 31 March 2017 was to present the provisional results of the study commissioned by the European Commission on cross border data flows, and facilitate a discussion on these results, providing an opportunity for stakeholders to contribute to the legal and policy discussion in the field. In particular stakeholder feedback was sought on the formulation of recommendations on how to scope the free flow of data, and how to implement those. This enabled the study team to better appreciate the needs of all stakeholders when finalising the study and providing

recommendations for future policy action to the European Commission. The workshop was also part of a series of structured dialogues between the European Commission and the Member States and other stakeholders, as announced in the Communication on "Building a European Data Economy".

The Workshop targeted representatives of public and private sector users (including SMEs), ICT service providers, and governmental authorities. Over 90 participants registered for the Workshop.

Stakeholder Consultation for the SMART study on Facilitating cross border data flow in the Digital Single Market

The study on 'Facilitating cross border data flow in the Digital Single Market' (SMART 2015/0016) was undertaken by LE Europe, Carsa and Charles Russell Speechlys. The study investigated the prevalence of restrictions of the free flow of data within the EU, based on primary and secondary (covering CZ, FR, DE, IT, LT, LU ES and UK).

The study consulted stakeholders and gathered evidence through an online, predominantly multiple choice survey of businesses, distributed by industry associations and network, which elicited 53 responses from businesses; a survey of local legal experts in the eight member states from the Charles Russell Speechlys network; consultations with stakeholders including industry associations, service providers, legal professionals, businesses and government bodies; contributions from key stakeholders at the DG Connect consultation workshop on the Free Flow of Data (18 May 2016)

The study concluded that absolute prohibitions outside areas of core national interest (security and defence) are rare. Furthermore, compliance obligations were found to be typically aimed at ensuring regulatory oversight and access. In addition, some businesses seemed to have strict ‘data residency’ requirements that are not based on formal legal restrictions. Furthermore, the study stressed that location is seen by many market participants as a proxy for security, despite the fact that technical security is not enhanced by local data storage. However, functional requirements for data storage and processing within national boundaries arise from legitimate concerns about illegal access; accessibility of services and support (including language barriers); and latency and bandwidth. According to the study these cannot be dismissed and may justify location preferences. Another important finding was the widespread misinterpretation of the existing legal framework. Many market participants assume data storage and processing within national boundaries is mandatory or advised where it in fact is not. A lack of reliable ‘digital trade’ statistics means that the economic impact of restrictions on the free flow of data is difficult to assess.

Stakeholder Consultation for the SMART study on the Data Economy

The study on the 'European Data Market' (SMART 2013/0063) undertaken by IDC and Open Evidence presents a set of indicators measuring the European population of data workers, the value of the data market, the number of data user enterprises, the number of data companies and their revenues, and the overall value of the impact of the data economy on EU GDP. All indicators are presented for the years 2013 through 2016 and forecasted to 2020, exploring three alternative potential scenarios of evolution for the European Data Market: Baseline, High Growth and Challenge scenarios.

The study consulted a number of stakeholder categories identify the basis of their role in the data value chain. Both the supply side and the demand side of the data market were investigated through a field research survey of data companies and data users. The actual sample size was composed of 1,437 completed interviews conducted in selected Member States (the U.K., Sweden, Czech Republic, France, Germany, Spain, Poland and Italy). In addition a number of webinars were organised with the purpose of sharing information or community building.

Digital Single Market Cloud Stakeholder Meeting

During the meeting on the 29 June 2016 group discussions and an exchange took place on how to build best on the past, such as the previous work on a data protection code of conduct for cloud providers, cloud service level agreement standardisation guidelines and standardisation as well as certification. The interactive group discussions addressed current and future priorities in the context of a wider and broader stakeholder engagement.

This meeting was attended by a broad and wide mix of stakeholders with an interest in Cloud computing, including equally cloud providers and users, either public or private, and respective associations as well as organisations.

The four key topics discussed were:

- The twin topics of **data portability/switching of cloud providers**, i.e. ensuring that cloud customers can easily get their data back or move it to another provider, thus encouraging competition and higher quality services.
- Addressing any remaining and emerging concerns around **Cloud Security and Certification,** ensuring that the certification landscape becomes clearer and more consistent for cloud customers and providers alike.
- Creating an **SME-friendly cloud ecosystem**, ensuring that all past and future policy measures are accessible and beneficial to SMEs, both from the provider perspective and from the user perspective.
- Recognising and tackling **sector specific cloud uptake challenges,** including particularly for the public sector and financial services markets, but also for other markets that may have specific concerns due to their specific security, confidentiality or quality requirements.

Consultation workshop on the Free Flow of Data

The workshop on 18 May 2016 included presentations for active discussion with experts in relevant areas for the free movement of data within the EU, such as legal barriers to the free flow of data and on how the patchwork of national rules on company data fragments the EU Single Market. The Digital Single Market Strategy committed the European Commission to propose a Free Flow of Data Initiative. This workshop was scheduled for participants to actively discuss their own perspective of issues related to the free movement of data within the EU.

The Workshop targeted representatives of public and private sector users (including SMEs), ICT service providers, and governmental authorities as well as Member State representatives. Over 80 participants joined for the Workshop.

The discussion on the first issue demonstrated clear support for the abolition of unjustified data location restrictions in the light of technological developments and costs. In relation to access and ownership of data, a clear divide could be observed and scepticism in relation to potential regulation was expressed even though most participants confirmed that access to data must somehow be granted. In relation to liability it was generally acknowledged that the current regime needs to be adapted to emerging technologies and future challenges, whereas with regards to interoperability and portability caution with regards to premature standardisation was expressed. In conclusion, cost and a lack of trust were identified as two critical considerations framing the FFD discussion.

Public Consultation on Regulatory Environment for Data and Cloud Computing

A public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy was launched on 24 September

2015, and ended on 6 January 2016. The consultation included questions on data location restrictions, 'data ownership', (re)usability and access to data, and liability. In accordance with the better regulation guidelines, an Inter Service Steering Group (ISSG) approved the consultation questions.

The public consultation on the regulatory environment for platforms, on liability of intermediaries, on data and cloud and on the collaborative economy received 1034 replies, 1005 of which were submitted through the EU-Survey, and 29 through the functional mail box set up exclusively for the consultation. Not all respondents replied to all four sections. Over 650 responses were received on the data and cloud section plus over 50 written submissions. The Commission prepared a synthesis report of the results. Given its scope and the level of response, the public consultation was considered to be sufficient to inform the Commission's analysis of the options mentioned above.

Cloud computing – Eurostat statistics on the use by enterprises

The survey by Eurostat provides for recent statistics on enterprises' use of cloud computing services in the European Union. The main findings of the survey are figures on the use of cloud computing; cloud computing as a service model for meeting enterprises' ICT needs; enterprises using cloud computing; enterprises' dependence on cloud computing; types of cloud computing: public and private cloud; factors limiting enterprises' use of cloud computing (2014 survey); and factors preventing enterprises from using cloud computing (2014 survey).

The data are based on the results of the 2014 and 2016 surveys on ICT usage and e-commerce in enterprises. The statistics were obtained from enterprise surveys conducted by national statistical authorities. The survey covered enterprises with at least 10 persons employed. In 2016, 148 000 of the 1.6 million enterprises in the EU-28 were surveyed. Of the 1.6 million enterprises, approximately 83 % were small enterprises (10-49 persons employed), 14 % medium (50-249) and 3 % large (250 or more).

Stakeholder Consultation for the SMART study on Measuring the economic impact of cloud computing in Europe

The study on 'Measuring the economic impact of cloud computing in Europe' (SMART 2014/0031) was undertaken by Deloitte. It provides an overview of the development of cloud computing in Europe in absence of policy measures, and of the most important barriers for its further development. It provides an assessment of the likely impacts (costs and benefits) of policy measures supporting cloud computing to be implemented consistently with the free flow of data initiative recently launched by the Commission, i.e. introduction of security certifications and removal of data location restrictions. The study developed a model for the cost-benefit analysis based on a large literature review, on available datasets and statistics, and on primary data collected via stakeholders' consultation.

The study collected inputs (both quantitative and qualitative) from stakeholders' consultation via interviews172, online surveys (a cloud computing professional users' survey173 and a cloud computing providers' survey174) and ad-hoc sessions at two C-SIG plenary meetings (one held on October 29 2015 and the second on June 27 2016). Equally, the demand side and supply side were consulted.

Stakeholder Consultation for the SMART study on Uptake of Cloud in Europe

The study on 'Uptake of Cloud in Europe' (SMART 2013/0043) was undertaken by IDC and constituted a follow-up of the IDC Study on 'Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up'. This study was carried out from January 2014 to November 2014. The objective of the 'Uptake of Cloud in Europe' study was to undertake a comprehensive economic analysis and provide quantitative estimates of the

impact of cloud computing on the EU economy. The previous study was carried out for the Commission by IDC in 2011-2012.

The study consulted per interview CIOs, IT directors, or IT managers of medium/large organizations and the IT managers or owners for small organizations. In total 361 interviews were conducted for the U.K., France, and Germany and 253 for Italy and Spain. The sample frame was obtained from a list source representative of the entire local market, regardless of computerization.

The study looked at the potential economic impact of the EU28 resulting from the adoption of Cloud based computing solutions by the Public and Private Sector. It provided updated data of Cloud adoption in the EU28 by industry, company size, and country. It estimated the level of substitution by Cloud spend of IT spend. In undertaking the assessment of the economic impact IDC prepared three scenarios, termed baseline, optimistic and pessimistic, reflecting a range of outcomes that reflect "most likely", "best case" and "worst case" respectively. The study also looked at how competitive the EU owned IT industry is in meeting the demands and opportunities that Cloud Computing presents.

Cloud Select Industry Group Plenary Meetings

The Cloud Select Industry Group (C-SIG) was established by the Directorate-General for Communications Networks, Content and Technology, Software and Services, Cloud Unit, for the purpose of providing independent validation and advice on proposals.

It was a stakeholder group open to all organisations, groups and individuals having a professional interest in cloud computing matters and are active in the European cloud market. The main representatives were from major European and multinational companies and organizations with significant involvement in cloud computing, in particular the supply side of the cloud value chain.

During the plenary on the 15 February 2017 the questions were raised on whether the European Commission is looking at intra- or extra-European data flows and in particular the differing nature of the identified restrictions. The European Commission clarified that they are now looking at intra-European data flows and outlined the categories of restrictions at issue.

During the meeting on 27 June 2016 cloud computing policy and related issues in the context of the Digital Single Market, in particular the Free Flow of Data were discussed with the participants. The discussion was nourished by the presentation of the results of the study "Measuring the economic impact of cloud computing in Europe" by Deloitte and led discussion on the potential economic impact of a removal of data location restrictions. It is clear that contractual and jurisdictional issues are major reasons for a lack of uptake in cross-border cloud computing services with consideration for issues of latency and redundancy. The impacts on important stakeholders lead to lively debate on the business benefits for SMEs vs. large companies.

2. Structured Dialogues with the Member States: summary report

Reports from the three structured dialogues

First structured dialogue workshop & set-up

On 23 February2017, the Commission held the first structured dialogue with Member States on the Free Flow of Data (FFD). It constituted a first exploratory meeting with Member States where the Commission facilitated interactive and constructive break-out discussions in various rounds on the benefits and challenges, as well as the risk and threats to MS in view of the FFD. This opportunity helped to effectively gather information on the shared as well as dissent views, concerns and questions raised by Member States in relation to the FFD. In addition the MS had the chance to collectively address their views on the most important issues, next steps to be taken and how to best address MS needs and concerns in order to enable a FFD in Europe.

At this occasion DG CNECT presented the ongoing public consultation and promoted participation by Member States and industry and user groups to the consultation. The presentation of two Commission studies on the study "Power of Data for European Growth" by IDC and the study "on the European Data Market set the scene and illustrated the benefits of, and/or the costs of not having, a single European Data and Cloud Market in Europe.

Furthermore, three Member States representing different positions, ranging from a strong support (PL), a pragmatic approach (DK) further to a substantial initial scepticism (FR), were given the opportunity to present their perspectives on the Free Flow of Data in the EU

The presence of a Cabinet member of Vice-President Ansip ought to underline the high political importance of the FFD initiative.

Key conclusions

The intervention by some MS on the expectations for this meeting on their behalf which pointed out the significant differences in understanding of the Free Flow of Data and its scope, in particular in relation to the questions: intra-EU vs. global flows; personal vs. non-personal data and the role of the GDPR; and terminology used (e.g. access to data vs. availability of data for regulatory purposes).

The key benefits and opportunities, and the key challenges and threats identified by the MS representatives during their discussions among each other were:

Key benefits & Opportunities	Key challenges & Threats
Economic growth o cost cutting - for companies, in particular SMEs - environmental costs o better/greater market access for SMEs - easier to scale up cross-border	Lack of mutual trust o Lack of common "high" security standards - certification/labels - standardisation Jurisdictional and enforcement issues - availability of data by authorities
Higher level of competition and innovation in the EU o better services and security for consumers/users o a globally more competitive EU Data market	Legal uncertainty on scope of FFD o terminological issues - personal/non-personal data o contextual issues - applicability of/relation to current EU and national legislation

	- justified data localisation restrictions – e.g. national security
Better "cross-border" use of public sector services	
Promote and advance legal clarity in the EU o overcome wrong perceptions on data localisation restrictions o foster mutual trust in relation to security	

The common understanding on possible ways to address the issues, as well as MS' needs in order to allow free flow: share best practices, issue guidance and application of/resort to existing applicable legislation (e.g. Service Directive, NIS Directive, GDPR etc.); clarify and raise awareness in order to address wrong perceptions; provide a wider and deeper economic impact assessment; promote trust through common security certification and standards; and regulate where necessary.

The Commission acknowledged and committed to: clarify on terminology and establish a common language to work with; provide clarity in relation to applicable laws and current legal gaps; foster further discussion to better understand the security and trust challenge, and the issue of cross-data availability of data by public authorities.

In conclusion the Commission presented a roadmap and timeline to the Member States.

The overall reaction by Member States on the first structured dialogue was positive. The interactive method that was used ensured that the Commission listened to the Member States and that a common approach towards the FFD could be created in joint effort.

Second structured dialogue workshop & set-up

On 30 March 2017 the Commission held the second structured dialogue with member States on the Free Flow of Data. This meeting served as an opportunity to discuss the current existing and applicable EU legal frameworks concerning free movement of data and to further elaborate on the data localisation measures identified so far in that context.

Based on bilateral discussions that the Commission had had with a few MS, there seemed to be a positive trend to remove identified legal provisions which result in forced data localisation. However, the EC was still in the discovery phase as regards to local practices. Several participants agreed that at this stage we only saw the tip of the iceberg.

The Commission started by summarising the first structured dialogue and the workshop of 20 March 2017 and received positive feedback from the participants on the constructive and cooperative approach of the EC. The relevant legal instruments (including TFEU – provisions on the freedom of establishment and the free movement of services, GDPR, Services Directive, e-Commerce Directive, Transparency Directive, NIS Directive) were presented by DG CNECT E2, JUST, CNECT F2 and GROW. Colleagues from SG, TRADE and CNECT D3 also attended the dialogue.

Participants were asked to identify prima facie and in small groups divided per category of data (health data/financial data/public archives/accounting data):

- whether they think that the identified and anonymised restrictions fall under the scope of any existing EU law;

- whether these restrictions are subject to any possible exemption (legitimate objective); and

- to make a proportionality test.

Key conclusions

In general, participants found it very difficult to navigate through all the legal instruments. Austria showed some sensitivity around the flow of health data and in response to Germany's question, it was clarified that there is no single FFD principle in the current legal instruments.

Some participants mentioned that the identified and anonymised rules were lacking legal clarity and that their objective was not clearly stated, which makes the proportionality test difficult. More specifically:

Public archives: conclusion that the restrictions are coming from the pre-digital era. The objectives behind the restrictions seem to relate to the availability and continuity of records, possibly to security and confidentiality of data as well.

Health data: Healthcare services are explicitly excluded from a number of instruments. Some of the restrictions might fall under the GDPR, the transparency Directive and the TFEU. For some obligations (e.g. obligation that the doctors must comply with specific recommendations established by the order of physicians), it is not clear cut whether this will infringe the free movement of personal data principle established by the GDPR as the obligation imposed on doctors may be imposed for other reasons than the protection of personal data.

Taxation and accounting data: Taxation is explicitly excluded from a number of instruments. It is also difficult to define whether it relates to personal data and whether the GDPR applies. The ECD might apply if the restriction affects the provision of information society services. It could be argued that restrictions on taxation and accounting data rely on public policy objectives and relate to the prosecution of criminal offenses (i.e. tax fraud). Some restrictions, like storing business letters in a particular Member State or at the company registered office, were nevertheless seen as disproportionate. In this case, the availability of documents should be a sufficient measure.

Financial Data: Financial data are explicitly excluded from a number of instruments. It could fall under the TFEU. The ECD might apply if the restriction affects the provision of information society services.

Functional requirements identified by participants as a possible alternative to data localisation requirements were:

For archives and for accounting documents: guarantee of the availability of data to auditors at any time (instead of storing the information in a single physical place).

For health data : certification to guarantee the integrity and authenticity of data; guarantee of the availability of data; mandatory contractual clauses (instead of having a mandatory local accreditation scheme in place for ICT providers processing health data).

For financial data : availability of data (instead of a mandatory local back-up once a month).

CNECT E2 held a short presentation on portability. The question on how to make FFD practical to companies when they are transferring data from one provider to another was specifically raised. This can drive further competition in Europe. Data portability was however not listed by the participants during the round tables as a major concern or a possible way forward to facilitate FFD, possibly in view if the nature of particular restrictions discussed. The increase of trust in cloud services was however mentioned.

Third structured dialogue workshop & set-up

On 4 May 2017, the Commission held the third structured dialogue with member States on the Free Flow of Data. The third structured dialogue was a constructive meeting with the opportunity to discuss the possible building blocks of a free flow of data approach, and to identify possible policy scenarios for the free flow of data in the EU.

The EC summarised the previous structured dialogues, the study workshop of 20 March 2017 and bilateral discussions with the MS so far. Next to this, a quick preliminary overview of the results of the public consultation on the free flow of data and data portability was presented.

The French Conseil National du Numerique gave a presentation on their recent opinion on FFD and the data economy. It focused on the need for a "data infrastructure", the portability right beyond GDPR to avoid vendor lock-in and enhance competition as well as incentives pooling of data. The German BMWi (Federal Ministry of Economic affairs and Energy) representative gave a presentation on their recent White Paper on Digital Platforms: Digital regulatory policy for growth, innovation, competition and participation. The paper reflects the state of stakeholders discussions in Germany. Regarding free flow of data, legal uncertainty and fear of new restrictions seem to be the main issues. The representative from Tecnalia (the contractor of the cloud certification study) gave a presentation highlighting the proliferation of security standards and certification schemes and outlining their further work on the topic.

The MS discussed the possible building blocks for a common free flow of data approach and their suitability to address the issues identified. They also engaged in break-out discussions to identify different possible policy scenarios (hard law, soft law, infringement procedures, business as usual, etc.) suitable for the FFD approach and its building blocks.

Key conclusions

There was a sense of emerging consensus on the possible building blocks for a common FFD approach: general FFD principle; data security; data availability/cross-border access to data by authorities; data portability.

The MS break-out sessions where they had to identify different possible policy scenarios (hard law, soft law, infringement procedures, business as usual, etc.) suitable for the FFD approach and its building blocks, resulted in the following preferences:

- Hard law with regard to a FFD principle,

- Guidance/soft law with regard to data security,

- Hard law and/or guidance when it comes to data availability/cross-border access to data by authorities and data portability.

ANNEX 3: WHO IS AFFECTED BY THE INITIATIVE AND HOW

In line with the 'Better Regulation' and 'Think Small First' principles, this annex assesses the possible impacts that the free flow of data legislative initiative is expected to have on the most important stakeholder categories. The estimations are made on the basis of the preferred policy option (Option 2 in the accompanying Impact Assessment).

Possible effects will be considered of all intervention areas envisaged in the legislative initiative, respectively: the free flow of data, data availability for regulatory control purposes, switching and porting data between providers and IT systems and security of data processing. To enhance readability, subcategorization of the text will be limited to costs and benefits per stakeholder type. Every time a specific intervention area is mentioned, it will be printed in bold.

Business users of data-based services

Costs

Business users of data and data-based services in general will not be presented with additional costs as the result of this legislative initiative (under the preferred option).

The only costs that could be connected to the legislative initiative for them would be costs for porting data when switching providers, but these costs would be lower than when no EU policy action would be undertaken and they would be agreed to in contractual agreements between business users and cloud service providers on a case-by-case basis.

Benefits

The initiative would lead to the reduction of existing costs for business users. These cost reductions can be divided into the following categories:

1. Cost reductions for businesses making use of cloud computing, or intending to do this in the future.

By enhancing open market competition for cloud services within the single market, the initiative would make cloud services more accessible to business users. At the same time, the nature of available cloud services will improve in terms of efficiency and innovation.

A support study by Deloitte estimates that the removal of data localisation restrictions would lead to an additional net benefit of 7.2 billion Euros for professional Cloud users (or 1.36%) compared to the baseline scenario.[8] These benefits are produced mainly by a reduction in prices of cloud services.[9]

The study also considers sector-specific benefits, leading to the conclusion that the manufacturing sector would achieve the largest benefit, with a generation 2.23% of additional revenue, followed by the distribution, retail & hotel sector (2.12%), finance (1.77%) and government, education and health (also around 1.77%).

[8] SMART 2014/0031, Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 [Deloitte Study (SMART 2014/0031)].

[9] The evidence cited here only considers the effects of removing data localisation restrictions. The study foresees even higher benefits if 'the promotion of existing relevant certifications and standards' by the Commission would be taken into account. However, the preferred option expects even more of the Commission, with regard to the intervention areas of data availability, data security and switching and porting data between providers and IT systems. Therefore, the benefits could be higher than predicted.

2. Cost reductions for businesses operating across borders, or intending to do this in the future.

The initiative would take away the (perceived) need for businesses to deploy a multiplication of data storage/processing facilities in multiple Member States of activity. Therefore, businesses that already operate across borders would be able to cut costs. Companies who would like to initiate a cross-border activity would be able to do so easier and cheaper, making use of only a single cloud service contract. For businesses who would want to keep their data in-house, the initiative would bring even greater benefits, as these would not be required to buy and operate multiple servers in different Member States. This would be inefficient not only because of a multiplication of purchasing costs but also of overhead costs resulting from energy use, server insurance, server space, the installation of VPNs, leased lines, et cetera. But these costs and, potentially, additional efforts for maintaining domestic routing when transferring data, are not the only costs that can be avoided for cross-border businesses supporting their data infrastructure in-house. The legislative action proposed will also take away costs in terms of administrative burden, legal assessment and compliance with the location restrictions set by some Member States, and the possible multiplicity of these costs over different borders.

Moreover, the initiative will make it easier for businesses to enter new markets. The public consultation clearly indicated that this would be one of the highest impacts of removing unjustified data localisation restrictions.

3. Cheaper to launch new products or services

Similarly, the public consultation identified the increased ability to launch new products and services in the EU single market as another high impact effect of taking legislative action. Predominantly the increased legal certainty, decreased compliance costs and rapid scalability of more widely available cloud services, are reasons for this contention.

Also the establishment of a principle of **data availability for regulatory control purposes** would have a short-term positive impact on the operational efficiency of business end-users of data-based services, through the reduced level of uncertainty for those business users who would like to move to cheaper providers in another Member State but are currently unsure whether their regulator or supervising entity would concur with such a switch.

On the intervention area of **security of data processing,** the preferred option for the free flow of data legislative initiative entails the development of an EU-wide certification and labelling scheme for cloud services. Such a system would benefit all cloud users, creating 0.64% of additional net present value (corresponding to around 3.5 billion Euros) from the additional user uptake generated by these standards and the reassurance they provide.

Start-ups, scale-ups and SMEs

The costs and benefits identified above for general business users are generally also applicable to smaller businesses like start-ups, scale-ups and SMEs. However, for these categories of businesses there are some additional considerations to make. In line with the 'Think Small First' principle, the Commission has scrutinised any possible impacts on them in a separate effort.

Costs

The initiative under the preferred option would not create costs for start-ups, scale-ups and SMEs. The initiative poses no new rules for these businesses to comply with, neither in terms of the systems they use, nor in terms of administrative or compliance requirements. Therefore there will be no increase of costs foreseen.

Benefits

The main benefits of the initiative for smaller companies will be enhanced competition on the IT services market and lower costs and barriers for market entry. But also raised security levels and higher cloud uptake would benefit this category of companies. As the Scale-up Europe Manifesto put it in words: "The real interest of startups – and of the European economy in general – is in reliable, safe and affordable data storage".[10]

Removing unjustified data localisation restrictions is a first considerable benefit, because when 'micro-multinationals' are active across national borders, especially early in their development, and conduct their business mainly online, data localisation measures would hinder the development of such fast-growing companies and their innovative potential. This is fully in line with the outcomes of the public consultation, identifying high impacts on launching new products and entering new markets.

Of specific importance to smaller companies is the possibility to run a company's data infrastructure from one Member State instead of having to duplicate storage and processing facilities. Companies with smaller budgets would be disproportionately (and quite possibly prohibitively) affected by the duplication of costs in multiple Member States. When attempting to differentiate the effects of the legislative proposal among subcategories of smaller companies, the statement 'the smaller the budget, the higher the benefit' can be indicative.

A more competitive single market for cloud services would have an impact on the competitiveness of European start-ups, scale-ups and SMEs. As explained in section 6.4.1.1. of the impact assessment, price reduction resulting from the removal of current market distortions by taking away data localisation restrictions could possibly yield around 276 million Euros per year in terms of savings for European SMEs.

Another specific benefit would be the lower costs of initiating a business in the EU, under the current level of 300 Euros and 3 days. This will be the result of the provision of cheaper and more competitive cloud services at a one-time cost for applicability in the whole EU.

SMEs and start-ups are expected to benefit most from the policy actions under the intervention area of **Switching and porting data between providers and IT systems**, because of the increased market dynamics introduced by easier switching.[11] Over all, as explained in the Impact Assessment, the demand for public cloud is forecast to grow by 20.5% CAGR. Particularly, smaller businesses would enjoy increased transparency regarding the data formats used by cloud service providers. This would be beneficial first and foremost for SMEs and start-ups operating on the cloud levels of PaaS and SaaS, which are more complicated in terms of IT architecture than IaaS. On top of this, clarity on the estimated time and cost of data transfer between IT systems would encourage small businesses to quicker switch to more favourable service providers without having to worry about costs related to disruption of the business process.

Data Storage and/or Processing Service Providers

Under the preferred option of the legislative proposal, data storage and processing (cloud) service providers would be impacted in terms of costs, more specifically in the intervention areas 'switching and porting data between providers and IT systems', 'data availability for

[10] The Lisbon Council, Nesta and Open Evidence (2016), "The scale-up Europe manifesto"

[11] SMART 2016/0032, IDC and Arthur's Legal (2017),"Switching between Cloud Service Providers", 2017 [IDC and Arthur's Legal Study (SMART 2016/0032)].

regulatory authorities' and 'data security' . However, the estimated benefits will outweigh the increased costs. Evidence suggests that data storage and processing service providers constitute the stakeholder category that benefits most, in relative terms, of this legislative initiative.

Costs

The proposed framework for **switching and porting data between providers and IT systems** will probably lead to direct compliance costs for data storage and processing service providers. The preferred option would rely to a large degree on market participants to comply with the principle that providers of data-based products and services should facilitate data porting for switching providers or porting data back to users' own IT systems. Also, data storage and processing service providers would have to give insights in the processes, technical requirements, timeframes and charges that apply in the situation of switching providers. Similar costs are predicted to arise under the intervention areas **data availability for regulatory control purposes** and **security of data processing.**

Therefore, direct compliance costs could arise from:

- Legal analysis of the current situation;
- The development of new model clauses for contracts between data storage and processing service providers and customers, regarding data availability for regulatory control purposes and regarding porting data to facilitate switching;
- The development codes of conduct regarding security of data processing;
- Standard setting in the area of security;
- Coordination with other data storage and processing service providers, e.g. through trade associations;
- Correspondence with the EU Free Flow of Data Cooperation Mechanism.

Additional costs could be:

- (Part of the) costs of migrating customer data to a new location;
- Loss of market share to other/new data storage and processing service providers as a result of increased data mobility.

The direct compliance costs are expected to be moderate, as data storage and processing service providers are already required to incur the compliance processes/costs enlisted above, under the new portability requirements in the framework of Article 20 of the General Data Protection Regulation (GDPR).[12] The obligations flowing from the principle of free switching of non-personal data under this legislative proposal could therefore be acted upon under the same process, leading to economies of scale. Another mitigating effect is that the cooperation provisioned in the area of data security would rely on voluntary schemes.

The additional costs, related to a new and more dynamic market situation, will largely by offset by the benefits of this same more competitive and open market. Importantly, it is unfeasible that data migration costs, which are incurred when a customer switches providers, will be borne by one single actor. The preferred outcome could be a division of costs between, on the one hand, the service provider and, on the other hand, the user or the 'new' service provider.

Benefits

[12] Regarding the portability of personal data.

Whereas costs for data storage and processing service providers will be higher than for business users, the benefits of the initiative will be higher for this group as well. Deloitte estimates an additional profit of 19.5 billion Euros for cloud providers. This would mean an impressive 21.53% change compared with the baseline scenario, where the Commission would not address the problem of unjustified data localisation restrictions.[13] This makes cloud service providers the stakeholder category that would benefit the most, in relative terms, of taking away data localisation restrictions. These expected benefits are expected to originate from a decrease in operating costs, combined with rising demand for cloud services.[14]

Also, the removal of unjustified data localisation restrictions would mean a decrease in administrative burden for cloud service providers. Currently, they are forced to undergo additional costs for complying with diverging requirements across jurisdictions, including in some cases heavy administrative requirements (e.g. for accreditation of providers offering hosting services for health-related data). Also, they are sometimes confronted with the up-front need to establish data processing centres dedicated to customers based in particular Member States. This obliges them to duplicate infrastructure, limiting their ability to make use of economies of scale by choosing business- and potentially environmentally-optimal locations for data centres. These costs, which will to a large extent be taken away by the legislative initiative, are more easily supported by large data storage and processing service providers, either established US companies developing into global players, or large EU based companies. Therefore, the legislative proposal will grant smaller, emerging players substantially improved access to European markets, and to domestic and/or sector-specific data service provision.

Theoretical example of costs for data storage and processing service providers avoided by this legislative proposal:

A small cloud service provider located in country A has in place an infrastructure spread across countries A, B and C in the EU. It has chosen the location for its data centres mainly based on the PUE index[15] and price of land and construction. It has successfully offered storage and processing services to businesses in the three countries, but it wants to expand and offer services cross-border. There is some demand especially from the health sector in Country D and the provider explores the opportunity of competing on the market in Country D.

building on Figure 4 and anonymised interviews from (LE Europe, 2016, p. 10)

Decision tree for entering the market (*see Figure 4*)	**Costs related to each step of the decision tree**
Is it illegal to store data outside Country D? Are there regulatory requirements which would be breached if data was transferred to another country?	Costs incurred for: detailed assessment of the regulatory framework in Country D compared to A, B and C.
Do customers have binding contracts to store their data in Country D? Does the provider need to match a competitor's commitments on data residency?	Costs incurred for: market (contractual) analysis
Are there public concerns around data travelling outside of Country D which could lead to loss of market share?	Costs incurred for: opinion mining

[13] Deloitte Study (SMART 2014/0031).

[14] The evidence cited here only considers the effects of removing data localisation restrictions. The study foresees even higher benefits if 'the promotion of existing relevant certifications and standards' by the Commission would be taken into account. However, the preferred option expects even more of the Commission, with regard to the intervention areas of data availability, data security and switching and porting data between providers and IT systems. Therefore, the benefits could be higher than predicted.

[15] Power Usage Effectiveness (PUE) ratio is a measure of the energy efficiency of data centres, calculated as the total energy (watts) supplied divided by the energy used to power the equipment in the data centre – i.e. ratio pointing to the energy used for cooling, lighting, etc., broadly depending on climate conditions.

If the answer is NO to any question of the decision tree and the decision is: Enter the market by offering cross-border services	Virtually no additional costs: exploits economies of scale and uses existing infrastructure in Countries A, B and C
If the answer is YES to any question of the decision tree and the decision is: Enter the market in Country D →	Costs of establishment Building and maintenance costs for new data centre in Country D Costs for technical solutions ensuring specific data is kept on servers in Country D and reported as such
If the answer is YES to any question of the decision tree and the decision is: Do not enter the market in Country D →	Mitigation of costs not affordable for the company

The cloud services sector would also benefit by the Commission's action in the area of **data availability for regulatory control**. It is expected that a significant portion of the market would be opened up to them by the increased cross-border demand which will be the result of increased legal certainty. The same mechanism underpinned by higher levels of legal certainty is applicable to the intervention areas **switching and porting data between providers and IT systems** and **security of data processing.** Both intervention areas would enhance the trust of business users and consumers in cloud services and therefore increase uptake.

Consumers

Costs

The initiative as provisioned under the preferred option will entail no costs for consumers. All costs will be borne by the public authorities of Member States and businesses.

The risk that data storage and processing service providers would pass on the costs that will be incurred as a result of this legislative proposal is negligible for two reasons. Firstly, because the benefits outweigh the costs, specifically for cloud service providers. Secondly, because research shows that that the price charged to users is currently still independent of the cost of provision of these services. Obviously, cloud service providers will need a return on investment in the longer term. But in the short-term other considerations, such as maximising market share, take precedence.[16]

Benefits

Consumers will be positively impacted by the initiative, through lower prices and more choice on the market of data storage and processing services.

The largest benefits of the intervention area of **switching and porting data between providers and IT systems** are expected for business. However, a principle of porting data for switching providers would also be important for consumers, who are increasingly using different types of cloud services. Whereas the data volume averagely stored by individual consumers tends to be modest, this is steadily growing over time as the accumulation of new data to be stored goes at a higher pace than deletion. Therefore, the time needed to transfer customer data over internet connections may become so long that it would render migration problematic if there would be no legal principle that facilitates switching providers.

[16] SMART 2015/0054, TimeLex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions" [TimeLex Study (SMART 2015/0054)].

Member States' public authorities

Costs

The preferred option of this legislative initiative would lead to moderate administrative burden for Member States' public authorities, caused by the allocation of Member States' human resources necessary for structured cooperation between Member States and the Commission by means of a 'single points of contact' coordination group. The average cost per Member State is estimated to be around 34.000 Euros.[17] These costs include both the provision of 0.5 FTE in the 'single points of contact' network created under the cooperation framework, and an average number of three notifications to be provided to the European Commission under the notification/review procedures. These procedures will be put in place to verify the compatibility of Member States' planned and existing measures with EU law.

For a more detailed explanation of the predicted impact of this initiative on the Member States' public authorities, the reader is referred to section 6.4.3. of the accompanying Impact Assessment.

Benefits

Member States' public authorities would benefit as well from the legislative initiative. In first instance, benefits would flow from the established safeguards regarding **data availability for regulatory control purposes**. This would entail improved supervision mechanisms, not only in sectors which are data-intensive today, but also in a broad array of sectors that are currently digitising.

Secondly, existing data location restrictions already cover a large spectrum of public sector data (related, for example, to public archives or public registers), hindering the implementation of cross-border or EU-wide digital public services. The technical implementation of such services generally requires distributed data storage and processing. The free flow of data legislative initiative would make this possible by removing ambiguous administrative requirements or straight-forward prohibition for using distributed technical solutions.

Thirdly, governments will also benefit from a more competitive cloud market, for example when procuring their own IT systems or shared cross-border digital public services. Removing unjustified data localisation restrictions would facilitate the selection of best-value-for-money offers and non-discriminatory selection of bidders in public procurement processes. For the smaller Member States, the ease with which cross-border data services can be contracted is even more business-critical than in the larger Member States,[18] given that the domestic market is smaller and allows to a lesser extent for economies of scale.

[17] The FTE cost estimation is based on the "Institutional Cost Estimation tool", used for the accompanying Impact Assessment and a support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005). The notification cost estimation is based on the data presented in the Impact Assessment accompanying the Proposal for a Directive on the enforcement of the Directive 2006/123/EC of the European Parliament and of Council of 12 December 2006 on services in the internal market, laying down a notification procedure for authorisation schemes and requirements related to services: the average time spent to comply with the notification procedure analysed in the IA is 12 working hours per notification. Taking the EU average of hourly earnings of civil servants with university education of €32.10, this results in an average administrative cost of €385.20 per notification.

[18] SMART 2015/0016, London Economics Europe, Carsa and CharlesRussellSpeechlys, "Facilitating cross border data flow in the Digital Single Market", 2016 [LE Europe Study (SMART 2015/0016)] at p. 9.

Finally, Member States' public authorities will benefit from the establishment of a future-proof network of single points of contact on data-related matters, which would minimise costs in the future, when other emerging data issues will possibly require ad-hoc cooperation on Member State level.

ANNEX 4: ANALYTICAL MODELS USED IN PREPARING THE IMPACT ASSESSMENT

1. Analytical model for calculating effects economic effects on the data market

The study "European Data Market" carried out by IDC and Open Evidence to support this Impact Assessment estimated the macro-economic impacts following the general adoption of data-driven innovation and data technologies in the EU19. This study concludes that a free flow of data legislative proposal taking away data localisation would be the most important factor in driving the European data economy towards the high growth scenario of 4% GDP by 2020.[20] The methodological approach[21] includes quantitative and qualitative indicators; a sensitivity assessment through scenario analysis is also performed.

The macroeconomic model forecasts were based on the estimates of key macroeconomic indicators (EU GDP, EU total ICT spending, and unemployment) and the assumptions for the three scenarios, as well as IDC's current forecasts to 2020.

The macroeconomic effects calculated by the model used for the analysis distinguishes between:

- The **direct impacts**: these are impacts generated by the data industry itself;
- The **indirect impacts**: indirect impacts are all the impacts which take place in other industries related to the considered industry, in our case the data industry. There are two different types of indirect impacts: the backward indirect impacts and the forward indirect impacts
- The **induced impacts**: these impacts include the economic activity created by additional payment of wages to staff in the data industry and its direct supply chain

The impacts are modelled for the Member States under three different scenarios, more or less ambitious in terms of macroeconomic forecasts and policy initiatives. The impact of Brexit is taken into account.

2. The policy scenario modelling for switching

The study "Switching Cloud Providers[22]" carried out by IDC and Arthur's legal to support this Impact Assessment modelled a number of potential economic impact on the cloud market of the alternative policy options to ensure data and application portability. The study considers three policy impact scenarios:

1. A "**No EU Policy Action**" impact scenario, which leaves relevant actions for portability to the Member States, if they are willing to do so.
2. A "**Soft Regulation**" scenario, which assumes that the European Commission promotes cloud portability through non-regulatory measures. These are advisory rather than mandatory and include: supporting and driving awareness of technology standards and tools that enable easier portability; supporting and driving awareness of best practices and codes of conduct developed by stakeholders including vendor and industry groups; encouraging the development and diffusion of standard legal contract terms that have the effect of enabling easy and reasonably priced portability between cloud services by customers.

[19] See SMART 2013/0063, IDC and Open Evidence, European Data Market, 2017 [IDC Study (SMART 2013/0063)].
[20] More information on this analysis will be presented in Annex 8 to this impact assessment.
[21] More information on the methodological approach and a complete list of indicators can be found in section 1.4 of the final report for IDC Study (SMART 2013/0063).
[22] IDC and Arthur's Legal Study (SMART 2016/0032).

3. A "**Mandatory Regulation**" scenario, which assumes the introduction of a mandatory data and application portability right, effectively extending the new data portability right created by the GDPR for personal data to non-personal data and to business users as well as private users.

The methodology includes[23]:

- Extraction of data from IDC's public cloud market forecasts 2016-2021 for the EU (excluding the UK) segmented by:

- Extraction and elaboration of data from IDC's annual surveys on European actual and potential cloud users' opinions[24], segmented by industry and company size, with a specific focus on:
  - Level of fear of customer lock-in;
  - Level of concern around non-conformance to SLAs and data governance;
  - Relevance of standardization and interoperability.

- Development of specific assumptions by scenario about the alternative policy options impacts on demand drivers, competitiveness and innovation influencing cloud spending, building on the quali-quantitative results of this study.

- Development of an ad-hoc model forecasting public cloud spending under the 3 policy scenarios to the year 2025, since new regulation will most likely be implemented and start having impacts no earlier than 2019 and the relative impacts by 2020 are likely to be very small.

- Comparative analysis of the results of the 3 policy impact scenarios.

3. Measuring administrative burden

All possible policy options have been subjected to an assessment of possible impacts in different categories. One of these categories is the administrative burdens for Member States' public authorities, caused by the policy option.

To calculate these burdens, the research for this Impact Assessment has utilised the 'Institutional Cost Estimation Tool'[25], developed by the Commission services that created the Impact Assessment for the European Electronic Communications Code.

This tool allows the calculation of the Full Time Equivalent (FTE) costs of 1 employee of different grade and placed in different types of organisations.

For calculating the administrative burden on Member States' public authorities in this Impact Assessment, the choice was made to work with the cost of an average desk officer in a national ministry. With the help of the tool, an average cost of 1 FTE for EU-28 was developed: EUR 33.384.

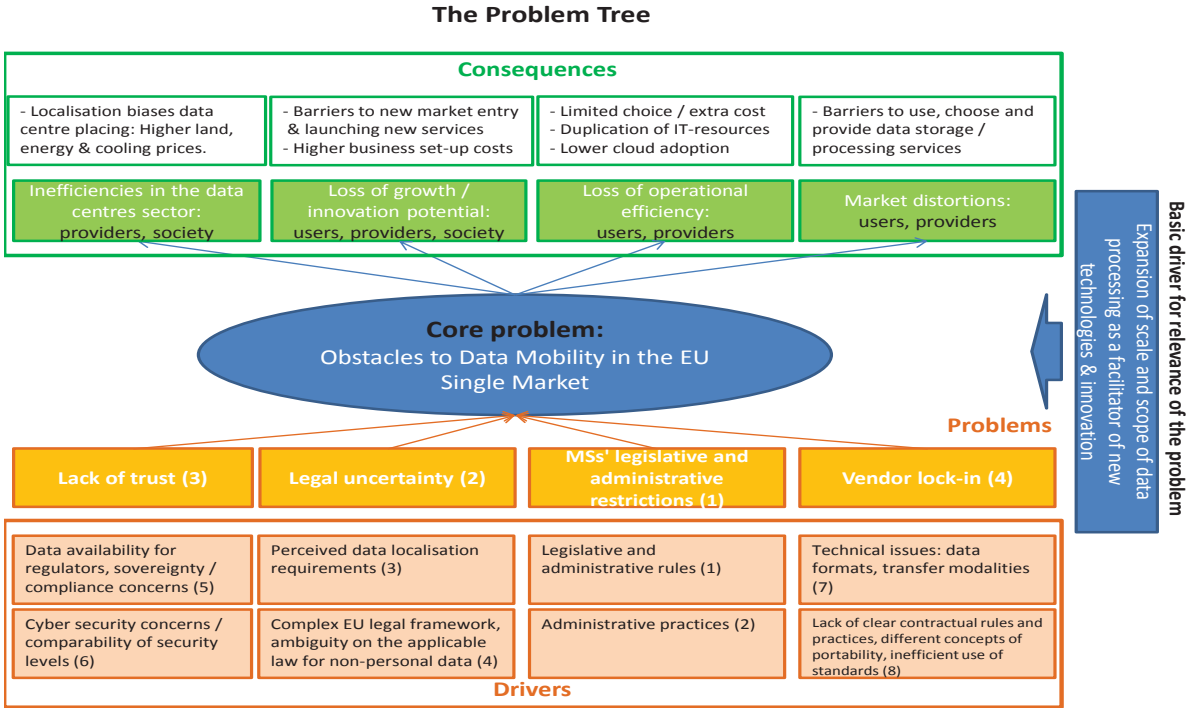
On the basis of this cost, total sums of burden could be calculated, combined with qualitative reasoning behind the number of FTE needed under the different policy options.

[23] More information on the methodology can be found in sections 5.1 and 7 of IDC and Arthur's Legal Study (SMART 2016/0032).

[24] The most recent is IDC's annual IDC 'CloudView' survey, based on over 1,000 interviews in Europe, November 2016.

[25] The "Institutional Cost Estimation tool", used to calculate Full Time Equivalent cost parameters, was developed in the context of the support study for the Impact assessment of the European Electronic Communications Code (SMART 2015/0005).

ANNEX 5: PROBLEMS, THEIR DRIVERS AND CONSEQUENCES



Problems

Having regard to the outcomes of the public consultation, the structured dialogues with the Member States and supporting studies carried out, the Commission has identified four interrelated problems that cause those obstacles to data mobility and, therefore, need to be addressed: lack of trust; legal uncertainty; legislative and administrative restrictions imposed by Member States; and vendor lock-in.

The four problems are driven by different types of factors (drivers): legal, administrative and contractual rules as well as the lack of legal certainty and the complexity of applicable rules; perception and approaches of market players, public sector organisations and public authorities; technical issues.

The movement of data within the EU is affected by different types of obstacles, which can be linked to the behaviours of Member States, public authorities, supervisory or regulatory authorities as well as of businesses.

In particular, **obstacles to the movement of data across borders in the EU** are caused by:

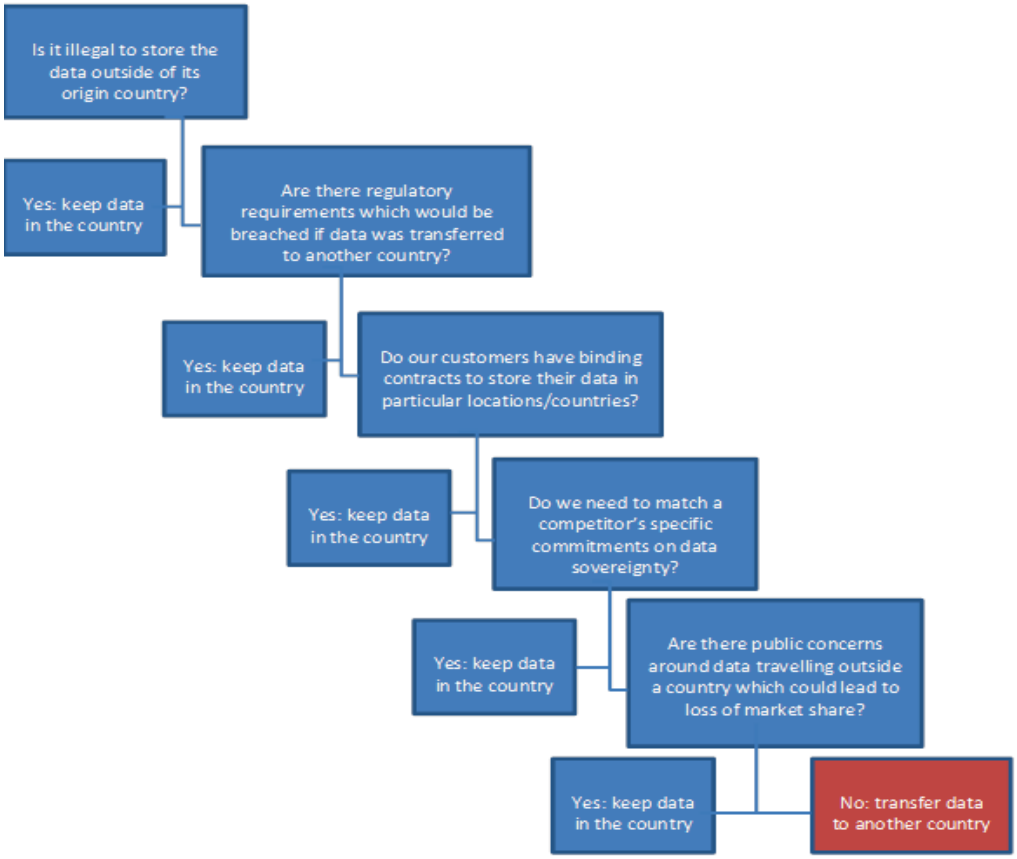
- legislative and administrative restrictions imposed by Member States (both rules and practices) (problem 1);

- legal uncertainty stemming from the perceived existence of data localisation requirements by businesses as well as public sector organisations and authorities and from complex EU legal framing (problem 2); and

- lack of trust displayed by public authorities (concerned about data availability for regulatory control / data sovereignty) and businesses or public sector organisations - users of data storage / processing services (concerned about the level of security of data storage and processing outside their own Member State) (problem 3).

The decision-making process of enterprises suggests furthermore[26] that different factors are interrelated before opting for a specific storage/processing solution: a sentiment of public concern or a strong security concern coupled with the wrong perception that it is safer to store data locally is likely to be reflected in contractual arrangements that limit data storage and processing activities across borders and turn 'data sovereignty' into an attribute on which companies compete for customers[27]:

Figure 1 - Steps in the decision to transfer data to another country



Obstacles to the movement of data across data (cloud) service providers / in-house IT systems are caused by:

- the vendor lock-in phenomenon (problem 4) driven in practice by the lack of clear contractual rules and practices concerning switching providers / porting data to a new provider or back to own IT systems; inefficient use of standards; as well as technical issues (e.g. data formats); and

- uncertainty about the existence or scope of legal rules for the portability of different types of data.

The figure below summarises the core problem, the four specific problems causing the core problem, the drivers of the specific problems (the specific problems and drivers are described in more detailed in the sub-sections below) and the consequences of those problems in a no change scenario or baseline (described in section 0 below).

[26] LE Europe Study (SMART 2015/0016).
[27] LE Europe Study (SMART 2015/0016).

Problem 1: Member States' legislative and administrative restrictions

Data mobility is undermined by restrictions to the localisation of data and to data services as well as measures having equivalent effect, both impacting business behaviour in the Single Market. There are still restrictions to fundamental freedoms guaranteed by the Treaty on the Functioning of the European Union that go beyond what is necessary and justified to protect important public interests, such as public security. The free movement of data services and the freedom of establishment are hindered in specific cases, notably through data localisation requirements under national law still in force in some Member States and/or obsolete administrative practices. This impairs the establishment and functioning of the Digital Single Market and raises further barriers to business and technical innovations emerging in the data economy.

In the public consultation of 2016, two thirds of respondents[28] – with an even distribution across all stakeholder groups, including SMEs – found that restrictions on the location of data have affected their business strategy.

In the public consultation of 2017, the majority of respondents[29] confirmed to know about the existence of data localisation restrictions. 80% of them stated that their organisations must comply with these restrictions. There is a broad consensus among stakeholders about the impacts of data localisation requirements, with only 2.6% of respondents indicating that they do not see any impact. To the question whether data localisation restrictions should be removed, more than half of respondents answer yes. When limiting the analysis to SMEs, roughly 60% say yes.

Member States' data localisation requirements stem from legislative and administrative rules (driver 1) as well as administrative practices (driver 2).

Driver 1: Legislative and administrative rules

Most Member States' data localisation restrictions take the form of legislative or administrative rules (i) **forcing data localisation** (mandatory requirements of storage in a specific geographical area or in a specific infrastructure which must itself be located in a specific area) or (ii) **having an equivalent effect** by imposing specific storage or processing requirements such as prior authorisation, accreditation or notification procedures before processing data or using a specific service provider (e.g. to ensure data security) or by requiring guarantee of timely and effective access to the relevant information for authorities (e.g. for control purposes). The equivalent effect is due to the administrative burden that the measures impose on businesses and public sector organisations to benefit from or provide cross-border services and/or common risk aversion by businesses and public sector organisations caused by the legal complexity and the lack of legal certainty.

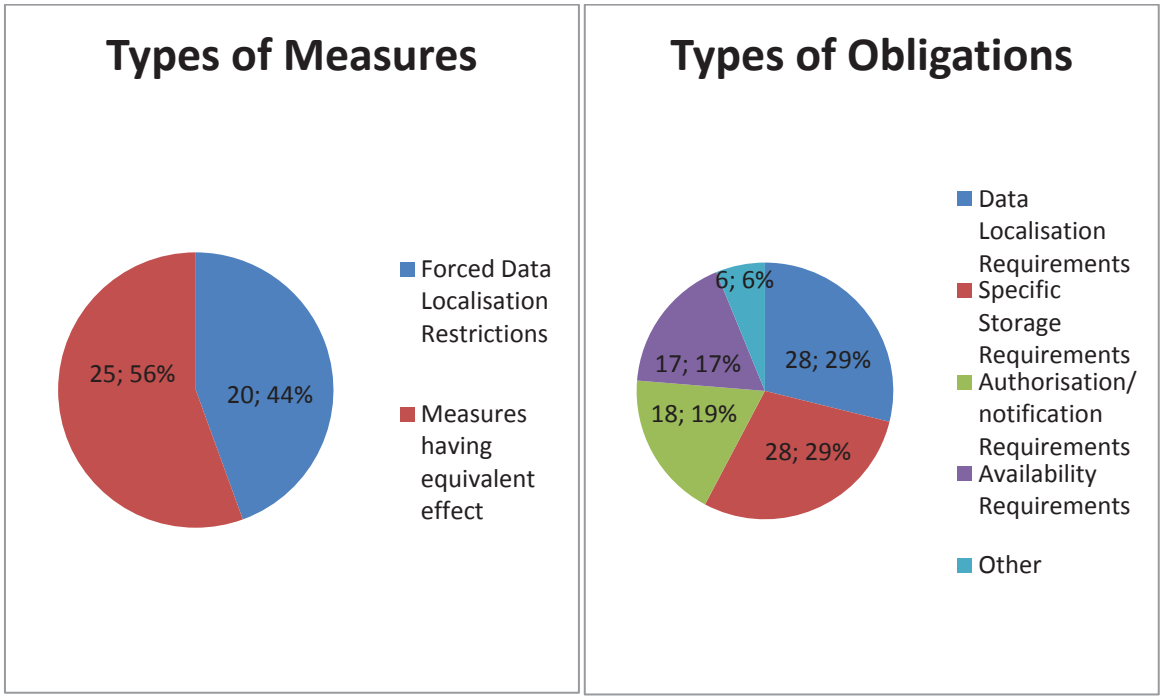
Two studies identified in total 60 restrictions (by means of a network of local legal and policy experts in 25 Member States).[30] Both studies were non-exhaustive in scope; hence the number of restrictions and requirements thereof are to be understood as an extract of the actual reality reflecting only the tip of the iceberg.

[28] A total of 328 respondents who answered to this particular question in the public consultation.
[29] A total of 380 respondents answered the public consultation.
[30] Czech Republic, France, Germany, Italy, Lithuania, Luxembourg, Spain and the United Kingdom in the LE Europe Study (SMART 2015/0016) & Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Ireland, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovenia, Sweden in the TimeLex Study (SMART 0054/2016).

The analysis of the public consultation as well as the structured dialogues with the Member States and other stakeholders delivered further evidence on both the existence of additional measures and their magnitude. Following the verification with the Member States in the context of the structured dialogue, a sample of 45 data localisation measures identified in 16 Member States has been retained as examples of measures either forcing data localisation or having an equivalent effect.[31] However, this still remains the **tip of the iceberg**. Besides confirming a number of measures already identified, the respondents to the public consultation of 2017 indicated examples of measures in two further Member States and 20 additional measures which they consider as hindering the free movement of data in the EU.

The types of measures (forced *v.* equivalent effect) and the 98 specific obligations/requirements entailed in these 45 data localisation measures are illustrated as follows:

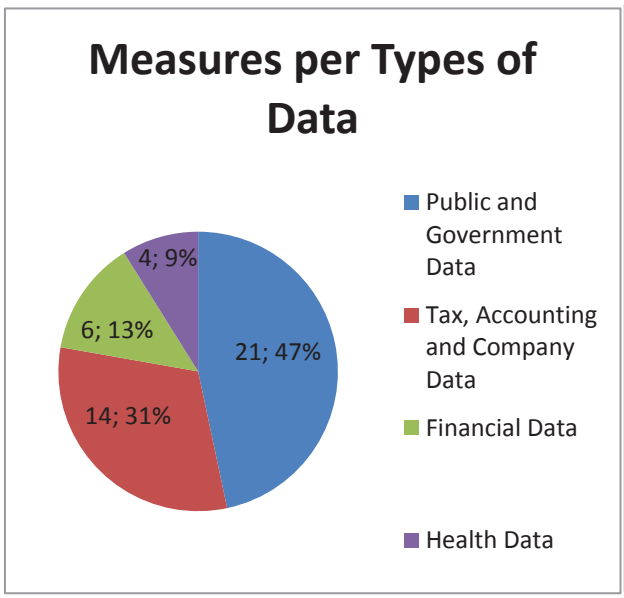
Figure 2 – Types of measures and obligations identified

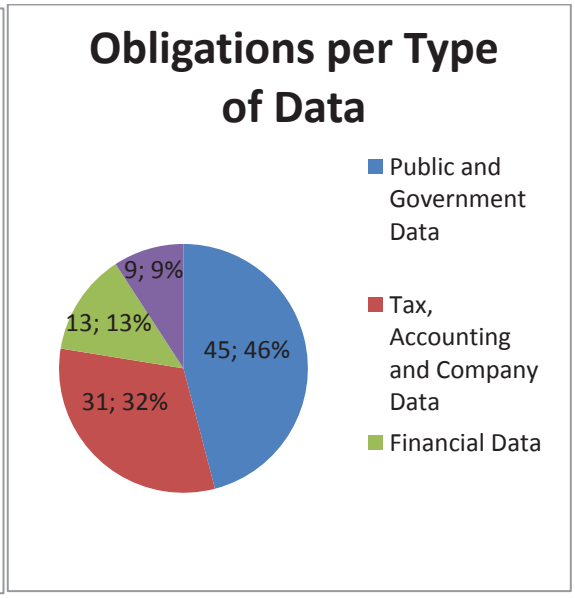


The measures / obligations included in the sample of 45 data localisation measures concern different types of data:

Figure 3 – Measure and obligations per type of data

[31] Annex 6.





Data localisation measures are adopted by Member States for **different reasons**, which are prominently data security (in a wide sense, which encompasses concerns like confidentiality, integrity, continuity and accessibility for the controller of the data), and the availability of data for supervisory and regulatory authorities of the Member States.[32] This has been confirmed by the bilateral and multilateral exchanges with Member States and private stakeholders, subsequently to the Communication of January 2017.

A number of the restrictions and requirements are based on considerations that originated in the 'paper era', where documents needed to be physically accessible for scrutiny or where only the original paper version had legal status. Other examples arise due to a misalignment between the objective to be achieved and the means to achieve it. Measures where the policy objective is maintaining *availability* of (access to) the data to the authorities for reporting purposes fail to acknowledge the technical reality of performant data storage and processing, where the physical location of the data is hardly, if at all, reassurance for the ability to access. This misalignment can be also observed in relation to the wrong perception that localisation increases security. On the contrary, the technological reality is that scale and "mirroring" of data in different locations substantially increases security of data storage and processing in the digital age.

For some legislative and administrative rules, Member States aim at ensuring that the data is immediately available to the national government, administrative authorities and/or law enforcement institutions. Paradoxically, some legislative and administrative rules are imposed in order to keep data out of reach of other jurisdictions and limit the access of other governments to specific types of data. Those restrictions reflect concerns to protect the confidentiality of certain types of data, to control access to such data and to oversee legal proceedings in case of unauthorised access, particularly to citizens' data, national sensitive data, privileged information and industrial secrets. A study raised that security is a common driver behind data location restrictions imposed by Member States and is often used as "convenient shorthand" for national security, national sovereignty and for security as a public policy task or as a protection of private interests.[33]

[32] LE Europe Study (SMART 2016/0016) and TimeLex Study (SMART 2015/0054).
[33] TimeLex (SMART 2015/0054).

Concretely, among the legislative and administrative rules identified, some may rely on legitimate public policy objectives but may constitute unjustified obstacles to free movement of data in the EU in the sense that they are disproportionate to achieve their objective.

Example: Mandatory use of a specific infrastructure located, which is located within the national territory and has a statutory mandate.

In one of the Member States, ICT tasks and duties with respect to the development, maintenance and operation (incl. hosting) are assigned by law to a dedicated Computing Centre. The statutory duties of that centre include giving IT support in the areas of unemployment, aviation, banking, disabled persons, insurance supervision, health, finance, and others. According to law, that centre has to be used as a subcontractor by governmental bodies before initiating a public procurement process, if their offer is in line with the market.

However, the structured dialogues have also revealed cases where some Member States decided to change voluntarily their legislation to meet the same objectives with less restrictive means:

Example: French Health Law

France revised Act number 2002-303 and the French Public Health Code which obliges hosting service providers to be approved by the Shared Healthcare Information Systems Agency within the Ministry of Health, following a strict accreditation procedure in accordance with the dispositions of Decree n°2006-6 in order to be allowed to undertake hosting activity for patient data. From 2019 the strict prior authorisation requirement will be replaced by a certification requirement.

Moreover, following the Communication of January 2017, the Commission services engaged in a preliminary **assessment to what extent the measures identified at the time and included in the sample could be considered unjustified or disproportionate**.

The main **criteria** used for the assessment were the following:

1 - Effective availability of alternative means to achieve the relevant public policy objective

For instance, requiring access to accounting and company data could replace outdated measures and obligations requiring accounting and company data to be stored locally (this approach was implemented in Denmark).

Similarly, as the French Health law example shows, strict and burdensome individual prior authorisation requirements can be replaced by a standardised certification scheme which guarantees sufficient security of sensitive health data.

2 – Excessive scope of a measure / non-critical nature of the data concerned

Restrictive measures and obligations requiring specific highly sensitive government data, critical for national security and defence, to be stored locally are most likely to be justified and proportionate.

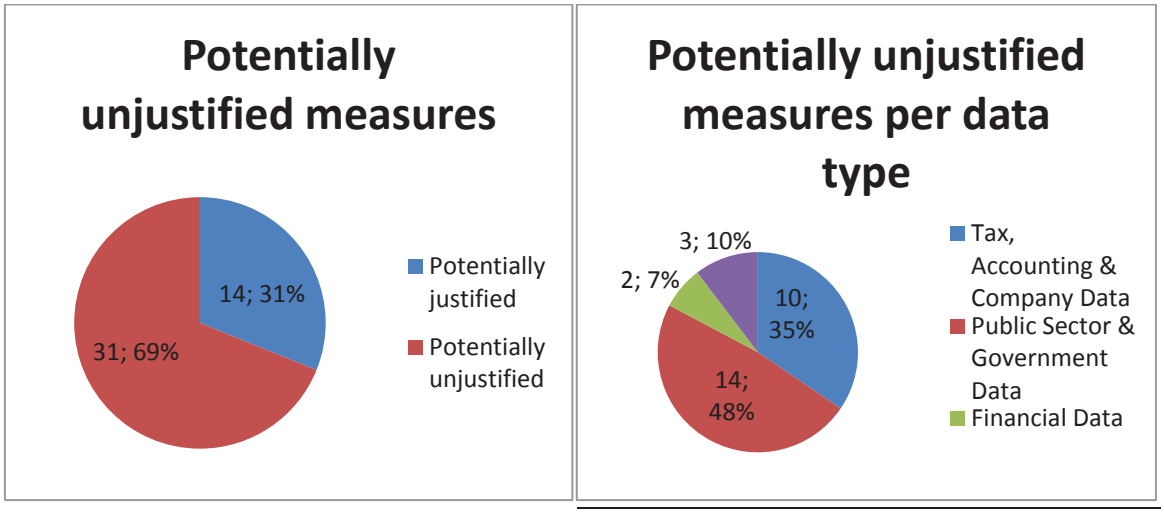
Example: The Slovenian Classified Information Act

The Slovenian Classified Information Act prescribes that **classified information** may only be transferred outside secure zone if encrypted, by methods confirmed by a committee for information security. All systems where classified information is held must be protected against electromagnetic radiation. […] Whenever classified information is processed outside the original location security measures must be comparable to those that must be implemented at the original location. If the information is stored electronically it must be separated from other possible information by way of physical or virtual separation. […] The information may only be transferred/ outsourced to those organizations that have acquired clearance, issued according to the regulation which defines checking procedures, issued by the competent ministry.

However, in cases where a measure is excessively wide in scope or is interpreted widely, thus captures public data and information of a non-critical nature (e.g. **all public archives**), it could be considered disproportionate.

Based on the criteria identified above, two thirds of the identified measures appear to be potentially unjustified or disproportionate.

Figure 4- Percentages and types of potentially unjustified measures (based on the sample of 45 restrictions)



35% of the potentially unjustified measures affect tax, accounting and company data and thus are cross-cutting in their impact on businesses. Over 48% of the measures concerned target public data and government data and could have an impact on costs of services for the public sector and could signal to businesses, especially SMEs, that outsourcing, in particular to other Member States, constitutes a risk. In any event, it must be underlined that such measures contribute significantly to the wrong conception that data localisation is a default requirement, in particular in relation to public data and tax data, and that proximity equals security and reliability when it comes to data storing and processing. In turn, this promotes more uncertainty and undermines trust in relation to use of data services available in other Member States.

Driver 2: Administrative practices

In addition to the sample of measures identified by the fact-finding exercise conducted by the Commission[34] a number of administrative practices (including specifically administrative decisions and procurement practices by public authorities) hindering cross-border data storage and processing services / in-house IT solutions were encountered.

Some impose the need to obtain specific permits through lengthy and cumbersome processes at national level to allow services for e.g. hosting patient data, without provisions for mutual recognition across Member States. Others require that data must remain accessible to a supervisor or that it must be exclusively accessible to the owner and yet other administrative practices are arbitrarily requiring data localisation without any reasonable justification. These administrative practices exist and develop due to restrictive interpretations of national provisions or due to individual or systematic decisions based on subjective considerations

[34] Primarily informed by two studies commissioned LE Europe Study (SMART 2015/0016) and TimeLex Study (SMART 2015/0054).

biased by risk aversion or even a degree of ignorance of technological realities and/or the applicable laws.

As part of the public online consultation of 2017, it was reported that: "*In the cloud computing business, the most common data localisation measures we see target financial, health telecom and public sector data. However, these measures are less often found in black and white legislation, but rather in sectorial guidelines by national regulators or government agencies*". As the respondent also stated, it is increasingly difficult for IT-service providers to be aware of all data localisation restrictions that are in place at a given time, because of the multitude of regulators and agencies and of their varying approaches to technology and data transfers. It is even more difficult to know it for IT-service providers located in another Member States and who try to enter a new market.

The wider dimension of the problem resembles in the fact that 179 out 353 respondents to the public consultation stated that they know of administrative rules and guidelines, including those adopted in the context of public procurement, that require to store or process data locally.[35]

The 2014 Trusted Cloud Europe survey[36] provided evidence that even if the rules do not have a legal status they can act as barriers to the cross-border transfer of data in the EU: over two thirds of respondents (180 responses out of 263) agreed to the statement that "even outside of formal laws, norms may exist (issued by supervisors, regulators, sector organisations etc.) which stop or discourage the use of cloud services outside national borders".

Example 1: X bank undertook an initiative to increase efficiency, lower costs and improve security through centralisation of IT infrastructures and avoidance of IT duplication in subsidiaries of the bank. The project was presented to all the local Regulators concerned for information / approval. All the Central Banks approved the project with the exception of Y National Bank, which insisted on local storage based on considerations of distance, the possibility of change of storage configuration in the future and the complexity. The X bank provided documentation demonstrating low levels of those risks. Still, the Y National Bank repeatedly rejected the project. As a result, the X bank had to maintain redundant IT operations in country Y.

Example 2: Testimony from an IT solutions provider who has worked on many projects with public health authorities in the UK. This provider reported that its proposal to store data generated by the UK's National Health Service (NHS) on servers located in another country was refused by its customer even though the proposal included using NHS encryption, using VPN, and then encrypting of hard drives.[37] The investigation by the provider unearthed two sets of guidelines by the Health & Social Care Information Centre (HSCIC) which are contradictory: one written in 2009 stating that "*Patient identifiable Data should not be recorded outside of the England boundary in any format for any reason without the prior explicit written permission of NHS CFH*"[38] and one written in 2013 stating that "*there is no Department for Health policy stating that patient information must be held in England*".[39] When asking for clarification on the rules, the provider said that he was directed to the 2009 guidance document.

Therefore it is obvious that restrictive administrative practices caused by either, factual ignorance, subjective preferences and bias, or by arbitrary decisions demonstrate to have a severe impact on the certainty and complexity for businesses and investors.

[35] The respondents to the public consultation could not distinguish between administrative rules and guidelines on the one hand, and administrative practices on the other hand. Therefore, administrative rules and guidelines must be understood as including practices.

[36] Report available: https://ec.europa.eu/digital-single-market/en/news/trusted-cloud-europe-survey-assessment-survey-responses

[37] LE Europe Study (SMART 2015/0016), p. 26.

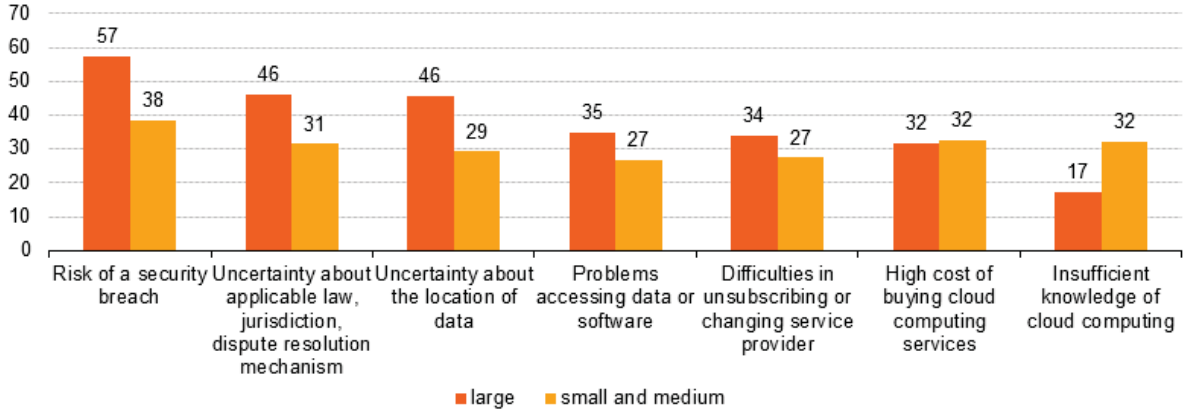
[38] http://systems.hscic.gov.uk/infogov/igsoc/links

[39] http://systems.hscic.gov.uk/infogov/igsoc/links

Problem 2: Legal uncertainty

Legal uncertainty is one of the main constraints to data mobility. The survey of factors preventing enterprises from using cloud computing services shows that uncertainty about the location of data and about applicable law/jurisdiction constitute, together with closely related security concerns, strong obstacles to cloud uptake and so, to free movement of data in the EU.

Figure 5 – factors limiting enterprise use of cloud services



Source: Eurostat (2014)[40]

Legal uncertainty arises from a perception that there is a legal obligation to store or process data in a specific territory (even if there is none) and a misinterpretation of rules (driver 3), and from a complex EU legal framing and ambiguity on the applicable law for non-personal data (driver 4).

Driver 3: Perceived data localisation requirements

Legal uncertainty leads users of data-based services to demand local data storage and/or processing from the service provider. 60% of European IT service providers who participated in the public consultation of 2017 indicated that their customers have demanded local storage of their data. The reasons indicated for this are either an assumption/perception that there is a local legal or administrative requirement to do so or a lack of familiarity with existing EU rules. The existence of the perception problem was also confirmed in the studies[41], the structured dialogues with the Member States and other stakeholders.

The perception might well differ from the actual legal situation, especially if the regulatory framework is unclear:

Example: a software as a service provider specialising in integrated solutions for universities has reported that some of their partner universities "believe" that laws applicable to them force them to keep data in their respective countries.

Also, regulation on providing access to data is sometimes interpreted as an obligation to give physical access to the server on which the data is stored. This is the case, for example, for

[40] Eurostat (2014), "Factors limiting enterprises from using cloud computing services, by size class, EU-28", 2014 (% enterprises using the cloud); http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

[41] LE Europe Study (SMART 2015/0016).

several national rules on tax data, invoices and company records where companies have a reporting and auditing obligation.

There is a strong sectorial dimension to the legal uncertainty problem. Market participants from heavily regulated and supervised sectors will assume that sector-specific localisation restrictions exist for them or at least that it is safer to store data locally in order to avoid complicated discussions with supervisors. In the health sector, some provisions require physical storage of hard copies of medical records in the hospital, with no clarification as to the applicability of this requirement for electronic records. Similarly, some sector regulators require notification of data transfers to other countries than the one where the company is established, which might be misinterpreted as localisation requirements by stakeholders.[42]

Testimonies of several actors in the health and banking sectors received through stakeholder engagement workshops show that businesses sometimes take a risk-averse decision to store and process data locally – to avoid the prospect of infringing the rules.[43] Many businesses seem to have internal corporate policies that are at least as restrictive as the legislation in place.[44] Such risk-averse behaviour discourages the adoption of innovative solutions and implies processing and/or storage of data in another Member State and, in some cases, leads to duplication of infrastructure.

Ultimately, "*such perceptions are as powerful as hard restrictions in deterring cross-border data transfers*"[45].

[42] LE Europe Study (SMART 2015/0016).

[43] European Union Agency for Network and Information Security (ENISA), Report "Secure Use of Cloud Computing in the Finance Sector", December 2015), available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/cloud-in-finance: "Despite the fact that some NFSAs around Europe (e.g. the Netherlands, Spain, Greece, Finland) have published opinions related to outsourcing/cloud based services, it appears that the financial industry is dealing with a lack of clear, formal guidance that is consistent across all NFSAs on the specificities of cloud based services. […]Our respondents have described various cases in which the need to notify NFSAs about the adoption of cloud based services has caused severe delays, or even blocked the prospective use of cloud services in their FIs. This on one hand is because information was not provided by the CSPs, but on the other hand also due to lack of guidance from the NFSAs on what specific information to be provided".

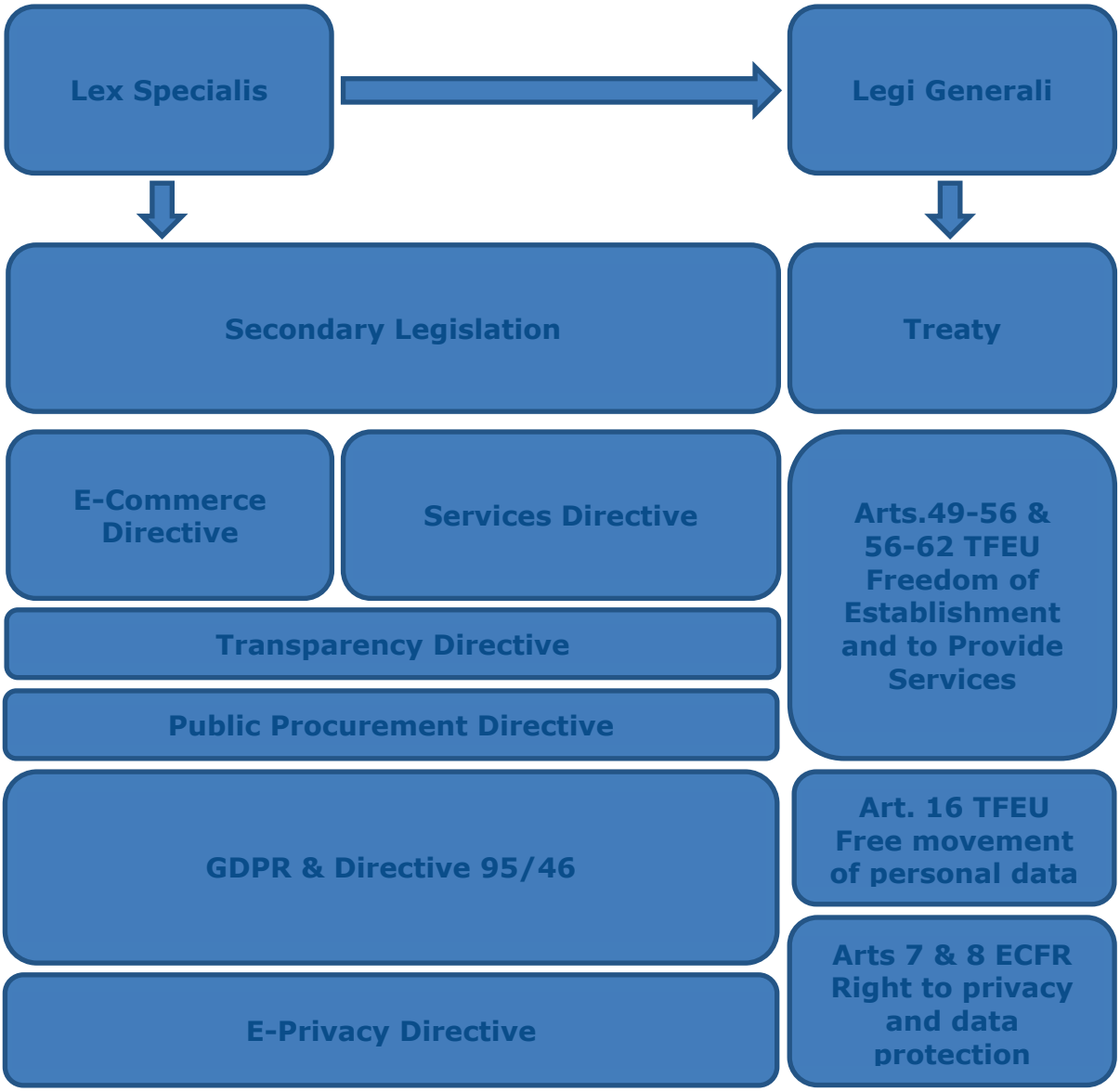
[44] LE Europe Study (SMART 2015/0016).

[45] LE Europe Study (SMART 2015/0016), p. 38.

Driver 4: Complex EU legal framing

1. Data localisation

The a*cquis communautaire* that could potentially be relied on to tackle obstacles to the EU single market for data and pursue a free movement of data consists of several TFEU provisions as well as a number of secondary legislative instruments varying in scope and having different Treaty bases. This section will assess the feasibility of relying on existing legislation to address in a cross-cutting manner the identified localisation restrictions and measures having equivalent effect, and to avoid the emergence of new restrictions. **Please also see section 6.3.1.1, infringements text box in the main report.**



The potentially applicable substantive provisions of the EU secondary legislation mentioned above have well-defined and targeted scopes and coordinated fields (e.g. the E-Commerce Directive covers information society services and the Services Directive covers services, both as defined by EU law) which overlap only partly with **Member States' legislative and administrative rules and practices** addressed by this initiative. Moreover, a number of relevant areas are expressly excluded from the scopes of such legislation.

This leads to legal uncertainty as to what extent obstacles to movement of data across borders in the EU are covered by existing EU law. Users of new technologies in regulated markets seem to be affected more seriously by this problem of uncertainty about rules.[46]

Existing secondary legislation and potential gaps

Existing regulatory instruments				Gaps	
Name of instrument	**Sectors covered**	**Data / activities covered**		**Sectors not covered**	**Data / activities not covered**
GDPR	Horizontal	personal data / processing	Regulation entered into force on 24 May 2016 and shall apply from 25 May 2018	Criminal prosecution	Non-personal data / derogations from free movement for reasons other than the protection of personal data Limited applicability in B2B relationships
E-commerce Directive	information society services (ISS)	taking-up and pursuit of the activity of an ISS notification by MS of planned derogations to the cross-border provision of ISS by a given ISS provider	No cases / examples detected	Several, incl. taxation, activities of notaries or lawyers, gambling activities	Not clear whether would apply to the restrictions on the entities storing or processing data or data as such (controller)
Services Directive	horizontal	establishment, provision of a service, reception of a service notification by MS of derogations from the freedom to provide services	No cases / examples detected	Long list, incl. taxation, financial services, transport, healthcare, gambling, social services	Lack of specific provisions targeting data localisation restrictions

[46] LE Europe Study (SMART 2015/0016) and IDC Study (SMART 2013/0063)

Transparency Directive	horizontal	notification by MS of draft planned technical regulations, incl. rules on information society services	Several cases on gambling and telecoms data retention	Several, incl. broadcasting, financial services	Notification obligation does not cover rules which are not specifically aimed at information society services
Public Procurement Directive	horizontal	public procurement by contracting authorities	No cases / examples detected	Long list, incl. broadcasting, certain legal services, certain financial services, partly defence and security	No specific provisions on data storage / processing, just a general non-discrimination principle

The public consultation confirmed that this legal patchwork leads to legal uncertainty. In its contribution, the government of the United Kingdom stated: "*There are at least four separate legislative instruments that may be relevant [GDPR, Services Directive, Transparency Directive, E-Commerce Directive], none of which explicitly sets out a regime for data storage and which have different objectives, different scopes, and different exemptions, with some exemptions listed in a separate annex to that legislation. Most organisations (including public authorities and SMEs) would find it hard to navigate and understand all that legislation. We believe a new regulation is needed to simplify the landscape […]".*[47]

Testing the applicability of the existing EU secondary legislation against the sample of 45 localisation measures confirms the difficulty to identify one key applicable instrument the enforcement of which would have the desired cross-cutting legal as well as economic impact, notably in terms of creating precedents and enhancing legal certainty. In particular:

GDPR: Only 7 out of the 45 measures identified potentially fall within the scope of the GDPR. However, the majority of these concern health data, hence could be justified under Article 9(4) of the GDPR which allows Member States to maintain or introduce further conditions, including limitations, with regard to the processing of data concerning health.

E-commerce Directive: Nearly one quarter of the 45 localisation measures identified, fall within the scope of either, the tax exemption (9 measures) or the gambling exemption (2 measures). Therefore, the E-commerce Directive is not applicable to tax and gambling related localisation measures which represent a substantial share of the overall measures in existence.

Services Directive: Between one quarter and two thirds of the localisation measures and entailed obligations identified are exempted from the scope of the Services Directive, depending on how widely or narrowly the exemptions are interpreted on a case-by-case review.

[47] UK Government response to the European Commission's consultation on Building the European Data Economy

Moreover, in the sample of 30 potentially unjustified restrictions, an even more significant share fall within the scope of the derogations and exemptions from the GDPR and the directives. Such scope might be interpreted differently, which adds yet another layer of legal uncertainty.

Example: Legislation on Health Data

One Member State has legislation that requires patient data to be stored according to state-of-the-art encryption and the provider of the electronic health record/data base must be authorised prior to using health records. Depending on whether the purpose of the measure and obligations foreseen are to protect personal data, the GDPR could potentially apply. However, in relation to sensitive data, such as health data, the GDPR could be understood as allowing for derogations by Member States from the free flow of personal data according to Art.9 (6). In case the specific purpose of the measure is not protection of personal data of natural persons, the requirement of state-of-the-art encryption could trigger both Art.3 of the E-commerce Directive and Art.14 of the Services Directive. However, it would most likely qualify as proportionate and justified, in view of the sensitive nature of the data. The prior authorisation requirement would fall under Art.16 of the Services Directive and could be unjustified due to its burdensome nature for providers from other Member States. However, Art.2 (f) excludes healthcare services from the scope of the Services Directive.

Below is a detailed explanation of the reasons why few of the identified data localisation restrictions could be addressed under the existing EU secondary legislation.

1 – No comprehensive "free movement of data" principle covering the different types of data within the scope of the initiative

Article 16 TFEU established solely the principle of free movement of personal data. Accordingly, Regulation 2016/679 (the GDPR, applicable from 25 May 2018) and Directive 95/46/EC provide for the free movement of *personal* data. Articles 1(1) and 1(3) of the GDPR ban Member States' restrictions to the free movement of personal data to the extent they are motivated by the protection of personal data of natural persons. Restrictions related to other objectives and justified by other reasons than the protection of personal data, e.g. under accounting or company laws, are not covered by the GDPR. Furthermore, non-personal data remains outside the scope of the GDPR.

Only 7 out of the 45 measures identified could fall within the scope of the GDPR. However, the majority of these concern health data, hence could be justified under Article 9(4) of the GDPR which allows Member States to maintain or introduce further conditions, including limitations, with regard to the processing of data concerning health.

Other TFEU provisions, notably those on the free movement of services or freedom of establishment, and secondary legislation, in particular the E-commerce and the Services Directives, apply to data storage and processing services. However, the apparent lack of case-law clarifying the application of those provisions / legislation to data localisation measures and the lack of general applicability of the potentially relevant provisions with respect to data localisation point to the absence of an implied cross-cutting free movement of data principle. This is mainly due to the various derogations and exemptions to secondary legislation as well as the difficulty of demonstrating the unjustified nature of data localisation measures under relevant provisions in view of the given margin of interpretation.

2 – Exclusions from the scope of the existing EU secondary legislation

A significant number of sectors and/or activities are excluded either, from the scope of the existing EU secondary legislation in the fields of the free movement of services and freedom of establishment, or from the scope of the particular provisions of those legislative instruments.

The E-commerce Directive

The underlying objective of Directive 2000/31/EC on certain aspects of information society services, in particular electronic commerce (E-commerce Directive, ECD), in the Internal Market is to ensure a free movement of information society services between Member States. This shall be achieved through approximation of certain national provision on information society services relating to the internal market and the establishment of service providers in particular. Therefore, the E-commerce Directive has established the country-of-origin principle, banning restrictions to the freedom to provide information society services from another Member State to the extent that these requirements fall within the coordinated field.

The E-commerce Directive is applicable where a provider of an information society services is at issue as defined in Art. 2(a) of the E-Commerce Directive. This legal provision sends the reader to the pre-existing definition in Art. 1(2) of the Technical Standards Directive as amended by Art. 1(2) of the Technical Standards (Amendment) Directive, which defines an information society service as "(1) any service normally provided for remuneration, (2) at a distance, by electronic means and (3) at the individual request of a recipient of services."

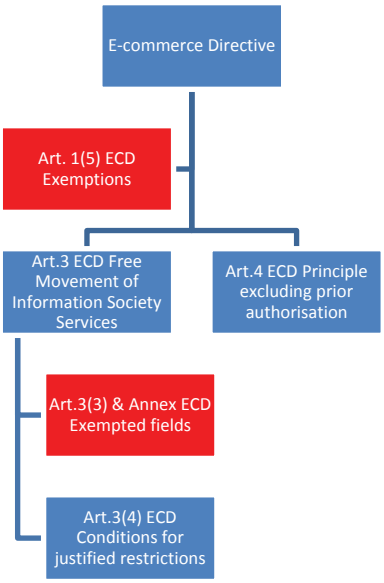
Not only an important distinction to be made is between a pure information society service and a service that makes use of information society technology[48], but it must be pointed out that it is not entirely clear whether or not the provisions in the E-commerce Directive only apply to national requirements hindering a free movement of information society services between Member States imposed on service providers. It is to be doubted that the freedom to receive services is implied in the E-commerce Directive and therefore can be invoked in relation to data localisation measures imposed on the potential recipients of information society services ("data controllers"), as this has not yet been tested in front of the European Court of Justice (ECJ).

This must be viewed in light of the fact that only the minor part of the data localisation measures identified in this IA (approximately 10) imposes obligations explicitly on service providers, and these obligations exist predominantly in the areas of gambling, financial services and only few regard data storage / processing service (cloud) providers.

Potentially less than one quarter of the 45 localisation measures identified fall within the scope of the E-commerce Directive.

Moreover, a number of activities are excluded from the scope of the ECD or from the scope of specific provisions, because they cannot be guaranteed under the Treaty or in accordance with secondary legislation.

[48] A service that makes use of information society technology may be seen to be a composite service and potentially not qualify as information society service. See further Case C-434/15 *Asociación Profesional Elite Taxi v. Uber Systems Spain SL*, Opinion of the Advocate General, 11 May 2017.



Article 1(5) of the ECD states the fields and activities which shall be excluded from the applicability of the ECD. These include the field of taxation, questions covered by EU personal data protection law, questions governed by cartel law, activities of notaries or lawyers, activities related to legal representation before courts and gambling activities.

In particular, the exclusion of the field of taxation, which is justified by the fact that the Treaty provides specific legal bases for taxation matters and by the existence of Community instruments already adopted in that field, curtails the ECD's applicability to the identified localisation measures substantially.[49] Furthermore, activities related to gambling are also excluded from the scope of the ECD because of the specific nature of these activities, which acknowledges the need for implementation of policies relating to public policy and consumer protection by Member States.[50]

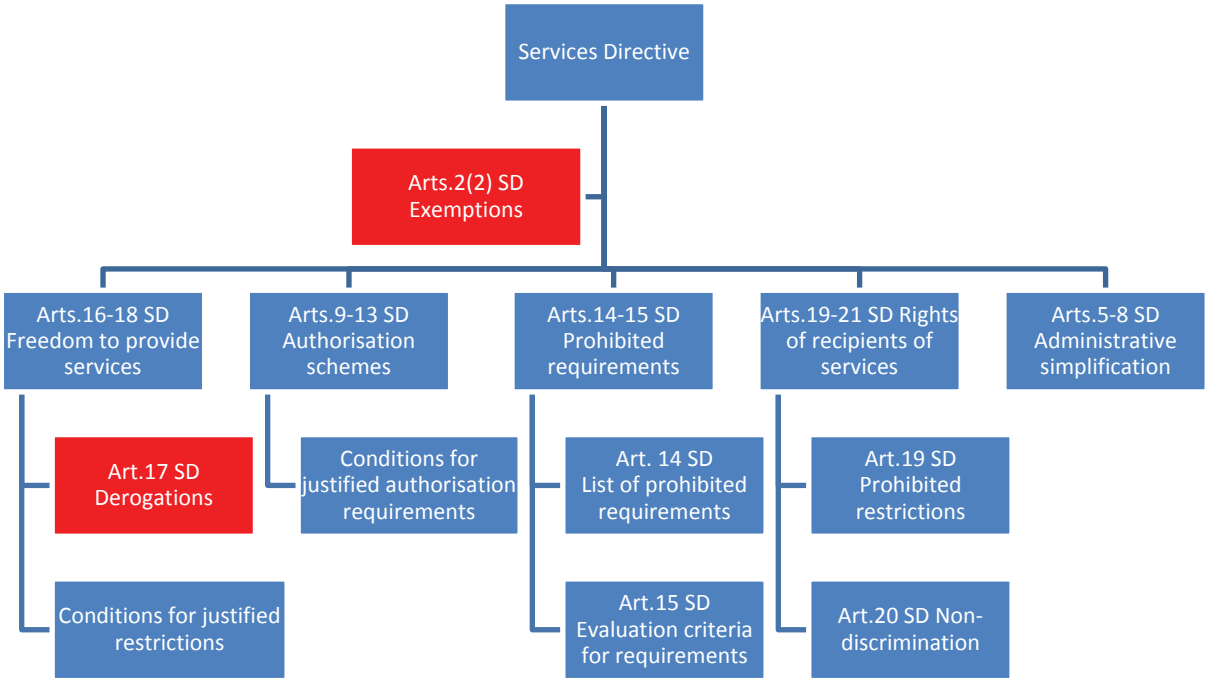
Nearly one quarter of the 45 localisation measures identified fall within the scope of either the tax exemption (9 measures) or the gambling exemption (2 measures).

Moreover, Article 3(3) of the ECD in conjunction with the Annex established derogations from the Free Movement of Information Society Services enshrined in Article 3. These include but are not limited to intellectual property rights, the freedom of the parties to choose the law applicable to their contract and the permissibility of spam.

The Services Directive

Similarly to the E-commerce Directive, Directive 2006/123/EC on services in the internal market (the Services Directive, SD) has a strong focus on service providers. The underlying objective of SD is to facilitate the exercise of the freedom of establishment for service providers and the free movement of services without undermining the quality of services. In order to fulfil this objective the SD goes beyond the Treaty and specifies concrete obligations on Member States which shall facilitate the cross-border provision of services as illustrated below:

[49] Recital 29 of ECD.
[50] Recital 25 of ECD.



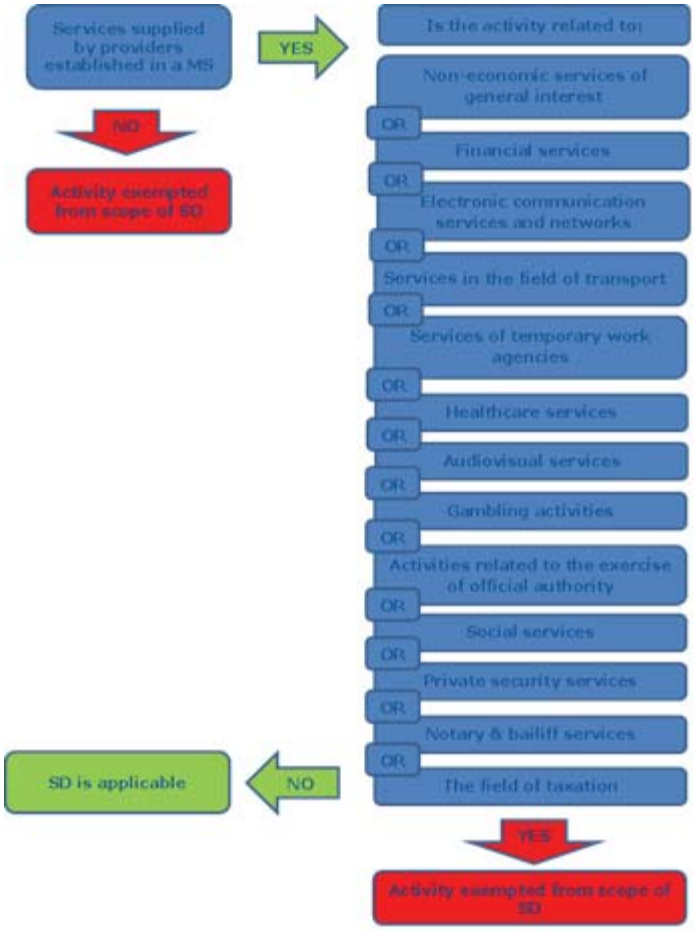
As illustrated the Service Directive provides for exemptions in Article 2(2) which features a long list of activities to be excluded.

Just as in the case if the E-commerce Directive the field of taxation is excluded from the scope of the SD according to Article 2(3). The exclusion covers both substantive tax law and administrative requirements necessary for the enforcement of tax laws.[51] Localisation restrictions stemming from strict local storage and data availability requirements of Member States' tax laws would qualify as administrative requirements imposed in order to safeguard the enforcement of such tax laws. Also, gambling is excluded from the scope of the Services Directive for reasons of public policy and consumer protection.

Healthcare related activities are excluded too (Article 2(2)(f) of the SD). This concerns services provided to a patient and covers activities which are reserved to a regulated health profession in the Member State where the service is provided. However, services to the health professional himself or to a hospital as well as services which are not intended to maintain, assess or restore patient's state of health are not covered by the exclusion. In addition, services and activities designed to enhance wellness, to provide relaxation or services which can be provided without specific professional qualification fall within the scope of the SD.[52] In view of this a substantial margin for interpretation is given.

[51] Directorate-General for the Internal Market and Services (European Commission), "Handbook on implementation of the Services Directive", 2008, available at : http://publications.europa.eu/en/publication-detail/-/publication/a4987fe6-d74b-4f4f-8539-b80297d29715 at p. 13.

[52] Directorate-General for the Internal Market and Services (European Commission), "Handbook on implementation of the Services Directive", 2008, available at : http://publications.europa.eu/en/publication-detail/-/publication/a4987fe6-d74b-4f4f-8539-b80297d29715at p. 12.



Financial services excluded by Article 2(2)(b) of the SD concern banking services, credit services, securities and investment funds and insurance and pension services. The financial services exemption also extends to services related to the take-up and pursuit of the business of credit institutions[53]. However, neither the SD nor the Handbook on its implementation explain whether services ancillary to financial services, such as related data storage / processing services, are also excluded from the Directive.

Moreover, it shall be noted that transport services, such as urban transport, taxis and ambulances as well as port services, should be excluded from the scope of the Services Directive as well. This would potentially prevent the applicability of the Services Directive to services related to smart transport and mobility.

Between one quarter and a two thirds of the localisation measures and entailed obligations identified are exempted from the scope of the Services Directive, depending on how widely or narrowly the exemptions would be interpreted by the European Court of Justice.

Additional derogations from the freedom to provide services are stated in Articles 17 and 18 of the Services Directive. These include but are not limited to services of general economic interest, questions relating to EU data protection law and intellectual property rights.

3 – Lack of substantive provisions in the existing EU secondary legislation (beyond the GDPR) that are sufficiently focused on the data localisation issues addressed by the initiative

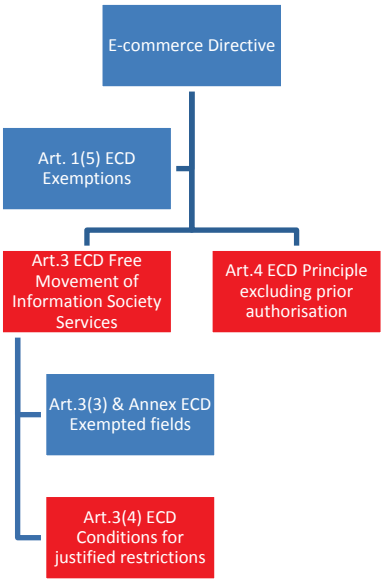
Only once the data localisation restriction or the measure having equivalent effect at issue does qualify as falling within the scope of either, the E-commerce Directive or the Services Directive, compliance with the criteria in the respective provisions must be established. This constitutes a burdensome task as will be outlined below.

The E-commerce Directive

As shown, the E-commerce Directive ought to ban restrictions to the freedom to provide information society services from another Member State to the extent that these requirements fall within the coordinated field. This includes requirements *with which the service provider has to comply* in respect of: (i) the taking up of the activity of an information society service,

[53] As set out in Annex I to Directive 2006/48/EC.

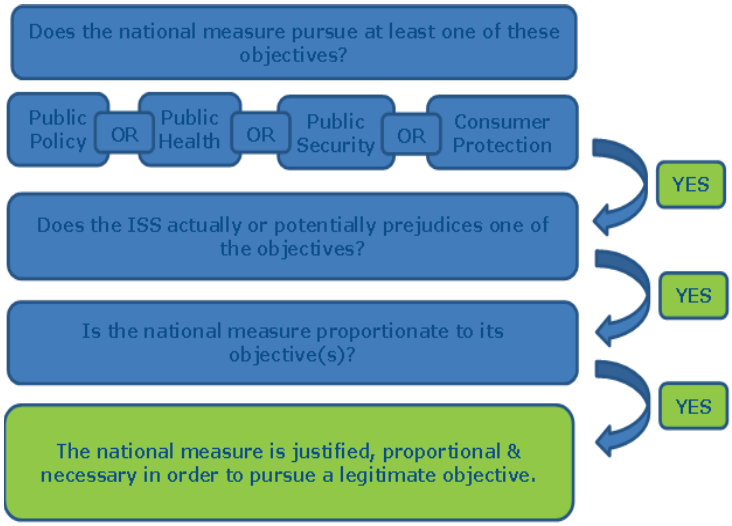
such as requirements concerning qualifications, authorisation or notification or (ii) the pursuit of the activity of an information society service.



Regarding prior authorisation schemes, Article 4(1) of the E-commerce Directive prohibits Member States to make the taking up and pursuit of the activity of an information society service provider subject to prior authorisation or any other requirement having equivalent effect. However, this only applies if the prior authorisation schemes target information society services specifically and exclusively, but not to authorisation schemes directed at the (potential) recipients of the services.

Two measures potentially fall within Art.4(1) and with regards to six measures the applicability is rather uncertain.

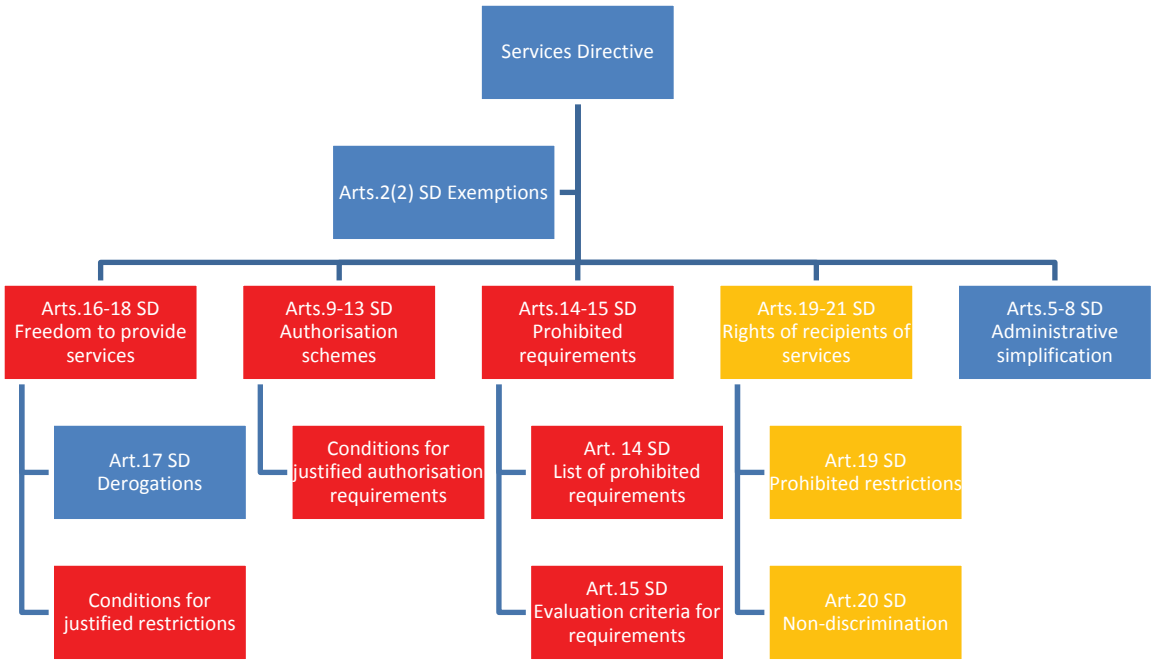
Similarly, the provisions of the E-commerce Directive allowing for restrictions to the freedom to provide information society services are very much focused on providers of such services. One of the steps in the three-fold test established by Article 3(4) of the Directive (see the graph below) is that the Member State intending to impose such a restriction has to comply with a notification requirement: it has to first address its concerns to the Member State of origin of the service provider; if that Member State does not adequately resolve the issue, the measure restricting the freedom to provide information society services can be taken; the measure shall be notified to the Commission and the Member State of origin of the provider.



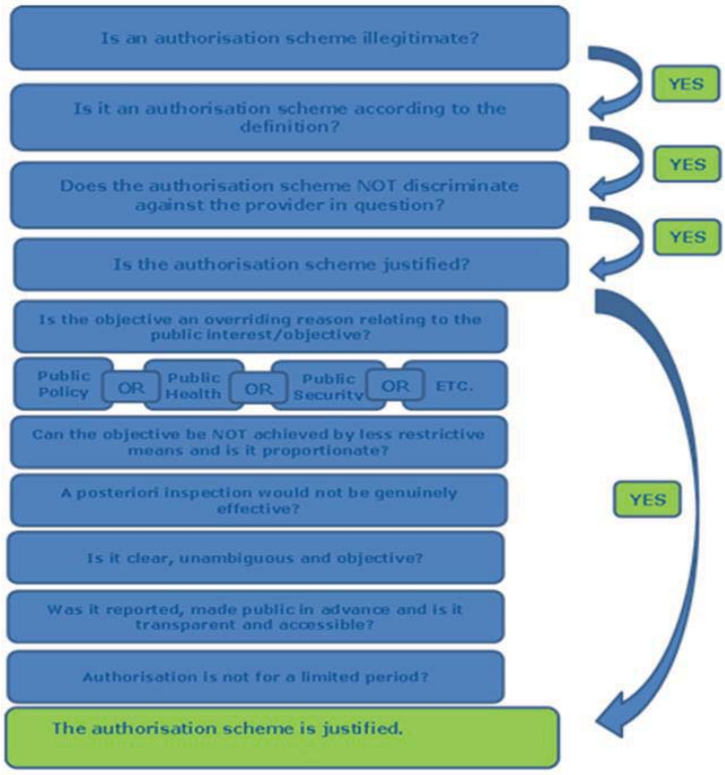
Eight measures would need to be scrutinized in compliance with Article 3(4) on whether they are unjustified and disproportionate. The final outcome of such an assessment by the European Court of Justice can be hardly foreseen.

The Services Directive

Similarly to the E-commerce Directive, the Services Directive, SD has a strong focus on restrictions imposed on service providers as reflected by the number of dedicated provisions (See in the graph below in red). Only Articles 19 to 21 define and address specifically the rights of recipients of services (See in the graph below in orange). The inclusion of additional provision for recipients of services might be viewed as reassuring that provisions focused on providers cannot be invoked where recipients are subject to potential unjustified restrictions.



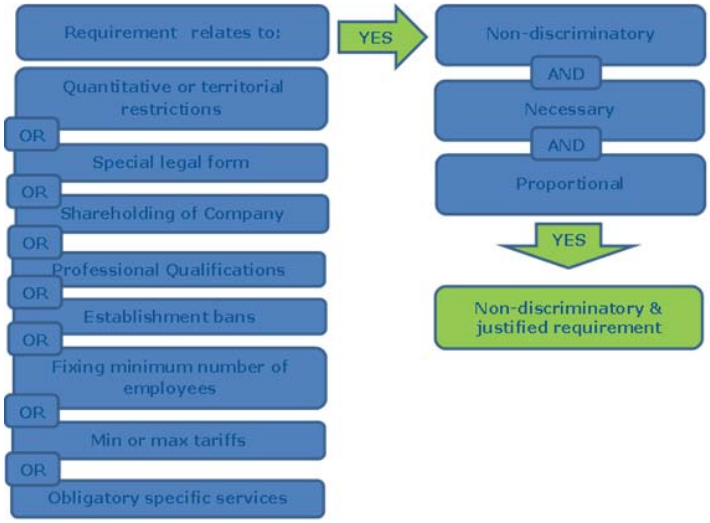
As regards the freedom of establishment, the Services Directive deals in Articles 9 to 13 with authorisation schemes and other requirements regulating access to, or the exercise of, a service activity (e.g. an obligation on a provider to take a specific legal form). Article 9 of the Services Directive prohibits discriminatory authorisation schemes or schemes which are not justified and proportionate in view of an overriding reason relating to public interest. In comparison with Article 4(1) of the E-commerce Directive, SD (Articles 10 – 13) explicitly adds the condition of non-discrimination and outlines precisely conditions and procedure for authorisation schemes (see the graph next to the text). In light of the given margin of interpretation and an easily established legitimate objective the difficulty in arguing



the unjustified and discriminatory nature of an authorisation scheme cannot be denied.

Only in relation to 2 measures the applicability of Articles 9 -13 would be highly probable, whereas with regards to further 3 measures applicability is uncertain. Whether the authorisation scheme is justified and may be granted would be subject to a margin of interpretation, hence the final outcome of such an assessment by the European Court of Justice can be hardly foreseen.

In Article 14 of the Services Directive a categorical prohibition of certain types of discriminatory requirements is set out. These are direct or indirect requirements discriminating natural persons depending on nationality or discriminating companies depending on the location of the registered office. Whereas, Article 15 states that Member States may impose requirements where they are justified for reasons of public policy, public security, public health or the protection of the environment as well as with regards to employing conditions as illustrated. Again, in light of the given margin of interpretation and the list of legitimate requirements the difficulty of proving the unjustified and discriminatory nature of an imposed requirement cannot be denied.



Only 6 measures would potentially trigger Articles 14 & 15, but the final assessment by the European Court of Justice can be hardly foreseen.

As regards the free movement of services, the Directive contains provisions both to ensure the right of providers to provide services in a Member State other than that in which they are established (e.g. the provider cannot be required to have an establishment in the Member State of recipient) and to prevent Member States from imposing on a recipient requirements which restrict the use of a service supplied by a provider established in another Member State (e.g. an obligation to obtain authorisation from or to make a declaration to their competent authorities).

The freedom to provide services as enshrined in Article 16 of the Services Directive requires Member States to respect the right of providers to provide services in a Member State other than that in which they are established. Possible requirements with which providers must comply shall be non-discriminatory, necessary and proportionate. It must be repeatedly noted that this three-fold test amounts to the previously mentioned difficulties. The Article also explicitly precludes Member States from imposing certain specific requirements:

- an obligation on the provider to have an establishment in their territory;
- an obligation on the provider to obtain an authorisation from their competent authorities including entry in a register or registration with a professional body or association in their territory, except where provided for in this Directive or other instruments of Community law;
- a ban on the provider setting up a certain form or type of infrastructure in their territory, including an office or chambers, which the provider needs in order to supply the services in question;

- the application of specific contractual arrangements between the provider and the recipient which prevent or restrict service provision by the self-employed;
- an obligation on the provider to possess an identity document issued by its competent authorities specific to the exercise of a service activity;
- requirements, except for those necessary for health and safety at work, which affect the use of equipment and material which are an integral part of the service provided.

In total 14 measures could potentially be in breach of the free movement of services under Article 10. However, it must be noted that a clear case is given only with regards to 3 measures, whereas applicability on the remaining 7 is uncertain.

However, the freedom to provide services is subject to an extensive list of derogations entailed in Article 17 of the Services Directive. Furthermore, Article 18 permits measures relating to the safety of services which restrict the freedom to provide services if:

- the mutual assistance procedure in Article 35 was complied with;
- no applicable EU law in the field of safety services is available;
- the measures guarantee a higher level of protection of the recipient;
- measures in the Member State of origin are not in place or inefficient;
- the measure at hand is proportionate.

As opposed to the E-commerce Directive, the Services Directive addresses in Article 19 specifically the fact that Member States may not impose on a recipient requirements which restrict the use of a service supplied by a provider established in another Member State, in particular the following requirements: (a) an obligation to obtain authorisation from or to make a declaration to their competent authorities; and (b) discriminatory limits on the grant of financial assistance by reason of the fact that the provider is established in another Member State or by reason of the location of the place at which the service is provided.

Furthermore, Article 20 of the Services Directive defines that neither discriminatory requirements based on the recipients nationality or place of residence, nor discriminatory general conditions of access to a service shall be allowed. However, it must be noted that *"[…] the possibility of providing for differences in the conditions of access where those differences are directly justified by objective criteria […]"* is given. This caveat combined with the well-known difficulty of proving in particular indirect discrimination makes it a challenging task to establish applicability in cases where it is not immediately obvious and in view of interpretation margins.

17 measures possibly trigger Articles 19 & 20 of the Services Directive, but only five of them constitute an obvious potential violation of the respective articles.

The Public Procurement Directive

Directive 2014/24 (the Public Procurement Directive) has established a general non-discrimination principle, according to which "contracting authorities shall treat economic operators equally and without discrimination and shall act in a transparent and proportionate manner". However, it does not contain more specific provisions dealing with data services or data storage / processing activities. While there is no reason why the general principle should not apply to discriminatory data storage or processing conditions imposed in the context of public procurement tenders, the evidence-gathering for this IA has not brought up any cases of such application of the principle in practice.

14 measures could potentially or actually violate the non-discrimination principle enshrined in the Public Procurement Directive.

Conclusion: it is very likely that most of the data localisation restrictions identified in this IA would not "match" the substantive scope of application of the provisions assessed and/or would be explicitly excluded from the scope of the relevant directive. Also, both the provisions and the exclusions are open to different legal interpretations which have not been tested in front of the ECJ yet, which leads to significant legal uncertainty.

2. Switching providers, porting data

As regards **movement of data across data (cloud) service providers / in-house IT systems**, while there are several legal provisions, e.g. in EU data protection law[54] and proposed EU consumer law[55], as well as certain national laws[56], to ensure data portability rights for individuals and consumers, there are no such rights granted to businesses. For business users of cloud services, portability is regulated by the contract with their cloud service provider(s). This may not be of great concern to larger business organisations, but for smaller players (SMEs and start-ups) it is reportedly very difficult to negotiate satisfactory terms for a possible exit/data migration from the cloud service. Businesses are often met with "take it or leave it" terms from Cloud Service Providers, leaving them little room to protect their interests.

Problem 3: Lack of trust

Security is a common driver behind data localisation requirements and can sometimes lead to an extensive use of what may be legitimately considered as falling under national security[57]. The general perception tends to believe that 'data is safer if stored / processed locally' and "once data skips one boundary, it may skip 2 or 3".[58] In other words, "location is seen by many market participants as a proxy for substantial assurances in terms of data access, privacy, audit, data integrity and law enforcement, despite the fact that technical security is not enhanced by local data storage".[59]

Driver 5: Data availability for regulators / compliance concerns

Some restrictions originate from a lack of trust of regulatory or supervisory authorities vis-à-vis cross-border storage of data, in particular vis-à-vis foreign market participants that could deny to the authority the access it needs to audit or control.

This is confirmed by the evidence gathered[60]. For example, in the area of **taxation**, German legislation applicable to all natural and legal persons requires them to keep "the records required for tax declaration within Germany"[61], and companies operating in foreign markets

[54] Article 20 of the General Data Protection Regulation gives data subjects a right to port their personal data. It allows for them to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller.
[55] The proposal for a Directive on the supply of digital content envisages a right for consumers to retrieve non-personal data from professional suppliers in certain circumstances.
[56] Article 48 of the French Loi Lemaire (entitled "Récupération et portabilité des données") states that consumers shall have a right to portability of their data.
[57] TimeLex Study (SMART 2015/0054).
[58] LE Europe Study (SMART 2015/0016).
[59] LE Europe Study (SMART 2015/0016).
[60] TimeLex Study (SMART 2015/0054).
[61] TimeLex Study (SMART 2015/0054) at p. 43 referring to Procedural rules for accounting and records, § 146 AO and § 147 (federal legislation)..

need approval for electronic storage outside the country. Some other accounting laws were identified as requiring that a copy of accounting records is kept locally even if stored electronically.[62]

Similarly, in regulation of **gambling**, Bulgarian and Romanian legislation impose restrictions, such as a requirement that all data relating to gambling offering be stored within national borders.[63]

In the **financial sector**, a number of provisions (e.g. on onsite audit/inspection mechanisms for national supervisors) have also been identified as data localisation restrictions.[64] For instance, in Spain, "the banks are obliged to provide a detailed plan of any outsourcing (if core activities are affected) to the Bank of Spain and ensure that in such a case the service provider/s will allow to the Bank of Spain the access to their facilities and systems, just as before the outsourcing."[65] This arguably makes more difficult the use of data storage and processing service providers located abroad.

The challenge of trust as well as jurisdictional and law enforcement issues were also raised during the Structured Dialogues with the Member States.[66]

It is to note, however, that if the data is stored in another Member State's territory, it can still be readily available for inspection electronically,[67] as exemplified by the amendment to the Danish Bookkeeping Act 2015.

Example: Denmark now allows accounting records in electronic format to be stored anywhere without prior application or notification to the public authorities, subject to the requirement on the business to provide online access to the records held abroad at any time.[68] Denmark explained at the High level conference on Building a Data Economy on 17 October 2016 that this legislative change solved the issue of having more than 1000 requests for exemptions per year and that they did not notice an increase in fraud.

In that regard a submission to **the REFIT Platform** from the Royal Norwegian Ministry of Trade, Industries and Fisheries (April 2017) states that as long as enforcement bodies have sufficient access to documentation, it should make no difference if a business keeps paper documents stored in a cabinet in their headquarter office in one European Member State, or

[62] Annex 6.

[63] TimeLex Study (SMART 2015/0054) at p. 56 citing Gambling Act, promulgated, State Gazette, No. 26/30.03.2012, lastly amended and supplemented, SG No. 1/3.01.2014, effective 1.01.2014, article 6(4); the study also refers to the Romanian Government Decision no.111/2016 approving the Norms of application of 24 February 2016 on gambling, articles 127 and 136.

[64] TimeLex Study (SMART 2015/0054) at p..20-25 and p.57 and footnote 10, citing for: Austria, Federal Act on the Supervision of Securities, art. 25-26, specified by Regulation Auslagerungsverordnung, BGBI. II Nr. 215/2007, latest amendment BGBI. II Nr. 272/2011; Belgium: Circular PPB 2004/5 on healthy management practices in outsourcing by credit institutions and investment companies issued by the Belgian Banking, Finance and Insurance Commission on 22 June 2004; Ireland: Central Bank UCITS Notice, October 2013, Annex II and NL: Circular Cloud Computing 2011/643815 issued by the Dutch Central Bank on 6 December 2011; Portugal: Regulation of the Bank of Portugal implementing Article 39(1) of Law No 25/2008 of 5 June and Article 5 Law No 25/2008 of 5 June, lastly amended by Law No 118/2015 of 31 August.

[65] LE Europe Study (SMART 2015/0016) at p. 16, referring to Spanish law 10/2014, of 26 of June, about ordination, supervision and solvency of credit entities. (BDE of 28 of June).

[66] Specifically, Workshop held on 23 February 2017.

[67] See to that effect, TimLex Study (SMART 2015/0054) at p. 99: if data should be stored on a server in a specific Member State in order to ensure its accessibility to a national supervisor, then the formal data location requirements can be "recast into a functional accessibility requirement".

[68] Annex 2, point 2.5.

chooses to store the same documents electronically with a service provider with servers located in another EU Member State.

Also business stakeholders are of the view that "the supervision (right to audit) must not block the development, adoption of new technologies."[69]

A potential challenge for national authorities would arise **if the private actor subject to regulation does not comply with its commitment to provide access for regulatory control purposes**, and the data might be outside the jurisdiction of the Member State engaged in a regulatory activity (as territorial jurisdiction is largely based on the place where the data is stored[70]). In such cases, the Member State will have to resort to judicial cooperation mechanisms in civil and commercial matters or in criminal matters, or to administrative cooperation mechanism such as in the area of VAT or financial regulation, or seek the voluntary assistance of the data storage and processing service providers. Several prominent avenues for Member States to obtain assistance from public authorities in another Member State for the purpose of accessing data can be found in Annex 8.

For example, in criminal matters, the European Investigation Order Directive (EIO)[71] allows for the issuance of an EIO, *i.e.* "a judicial decision which has been issued or validated by a judicial authority of a Member State to have one or several specific investigative measure(s) carried out in another Member State to obtain evidence."[72] Member States have the obligation to "execute an EIO on the basis of the principle of mutual recognition". Following the 9 June 2016 Council Conclusions on improving criminal justice in cyber-space[73] and the subsequent mandate given to the Commission by the Justice and Home Affairs Council on 8 June 2017[74], a legislative initiative on cross-border access to electronic evidence for criminal investigations by law enforcement authorities is now being considered and developed[75] in

---

[69] Consultation workshop, "Facilitating cross border data flow in Europe - data location restrictions", 26 February 2015.

[70] "Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace": https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf at p. 30. Other connecting factors can also be determinative of jurisdiction, depending on the area of law: see T-CY Cloud Evidence Group, "Criminal Justice access to data in the cloud: challenges", T-CY(2015)10 at p.10-11. For example, for tax purposes, the location of the subsidiary doing business might determinative; in consumer protection, "the location of the consumer seems decisive". See also *Microsoft v United States*, in the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 2nd Circuit Court of Appeals, 14 July 2016. See also Anna-Maria Osula, "Transborder Access and Territorial Sovereignty", Computer Law and Security Review 31 (2015) 719 – 735 at 721; Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet" (Part 2), International Journal of Law and Information Technology (2010) 18 (3): 227-247 at p. 232.

[71] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1 ("EIO Directive").

[72] EIO Directive, Article 1(1). Further, "EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State."

[73] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf

[74] http://www.consilium.europa.eu/en/meetings/jha/2017/06/08-09/

[75] "Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace" : https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf; "Non-paper from the Commission Services" : https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

two key respects: direct cooperation with Service Providers and direct access to electronic evidence stored remotely. Further, practical measures are considered, such as streamlining of procedures of Service Providers when responding to access requests.

Similarly, in the area of VAT monitoring, Council Regulation (EU) 904/2010 of 7 October 2010,[76] allows cooperation and exchange of "any information that may help to effect a correct assessment of VAT, monitor the correct application of VAT, particularly on intra-Community transactions, and combat VAT fraud."[77] Such exchanges can take place on request,[78] where requests can be refused on specific grounds defined in the Regulation.[79]

The number of potential actors in a given business – public authorities' interaction, the specific scopes in relation to type of information, and the delays associated with judicial cooperation procedures[80],are likely causes of Member States' distrust and reluctance to let data flow out of their borders.

In addition, it appears[81] that Member State national laws do not contain rules specific to situations where the physical data storage location is unknown.[82] In the context of the Expert Consultation of the e-Evidence Task Force, national and EU experts observed that the situation of undeterminable data location makes it unclear "which country might be affected [or] who is the addressee of a cooperation request".[83]

Another motivation behind some data localisation measures is to keep data out of other jurisdictions and limit the access of other governments to specific types of data. Those restrictions reflect intertwined concerns to protect the confidentiality of certain types of data, to control access to such data and to oversee legal proceedings in case of unauthorised access (in particular, to citizens' data, national sensitive data, privileged information and industrial secrets).

[76] OJ L268 of 12/10/2010, p.1

[77] Council Regulation (EU) 904/2010 of 7 October 2010, OJ L268 of 12/10/2010, p.1 (the "VAT Cooperation Regulation") at Article 1.

[78] VAT Cooperation Regulation at Article 7, where under Art. 7(2) " For the purpose of forwarding the information referred to in paragraph 1, the requested authority shall arrange for the conduct of any administrative enquiries necessary to obtain such information."

[79] VAT Cooperation Regulation at Article 7(4) and Article 54. The requests are submitted in standard forms and information must be provided to the requesting Member State "as quickly as possible and no later than three months following data of receipt of the request." (VAT Cooperation Regulation at Article 10).

[80] Regarding time delays in mutual assistance in criminal matters, see among others, Cybercrime Convention Committee (T-CY), "T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime", T-CY(2013)17rev, December 2014, available at : https://rm.coe.int/16802e726c; and the Evidence Project, Deliverable D3.1 Overview of existing legal framework in the EU Member States, Collaborative Project EVIDENCE "European Informatics Data Exchange Framework for Courts and Evidence", FP7-SEC-2013.1.4-2. ; See also CCNum, "La levée des obligations de localisation de données" at p 1: "S'il existe bien des mécanismes de coopération pour faciliter l'accès aux données à travers les frontières, il n'en demeure pas moins que la localisation des données en dehors des frontières nationales pourrait compliquer et ralentir l'exercice de tels contrôles voire favoriser la disparition de pièces et de preuves".

[81] The "Evidence Project", http://www.evidenceproject.eu/ .

[82] The "Evidence Project", D3.1 Overview of existing legal framework in the EU Member States, Collaborative Project EVIDENCE "European Informatics Data Exchange Framework for Courts and Evidence", FP7-SEC-2013.1.4-2 at 84.

[83] DG HOME, Report – Expert meeting on Access to Electronic Evidence, 17/18 January 2017, Brussels, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/e-evidence_report_17-18_january_2017_en.pdf.

Market players (users of data services) also display a degree of lack of trust in cross-border storage of data: 15.3% of (104) respondents indicated "law enforcement concerns" as the reason they do not choose services involving data storage abroad.

One reason for this is lack of clear guidance on the part of regulators. ENISA observes that guidance from regulators is not always available in its Report on "Secure Use of Cloud Computing in the Finance Sector" (December 2015): "respondents have described various cases in which the need to notify NFSAs about the adoption of cloud based services has caused severe delays, or even blocked the prospective use of cloud services in their FIs. This on one hand is because information was not provided by the CSPs, but on the other hand also due to lack of guidance from the NFSAs on what specific information to be provided."

Driver 6: Cyber security concerns, comparability of security levels

Many respondents to the public consultation and position papers received by the Commission[84] highlighted the discrepancy between the frequently held view that data is more secure when kept on-site and the fact that (cloud) data storage and processing service providers are often much better equipped in terms of security systems. Therefore, these respondents state that data is actually more secure when stored in the cloud.

The technical benefits of cloud computing are numerous. There is no need for the user to put in place complex maintenance processes to upgrade its hardware and software whereas it can be handled more systematically, more quickly and with less disruption to the users. The European Union Agency for Network and Information Security (ENISA) analysed the security benefits and risks of cloud computing (compared to on-premises solutions)[85] and concluded that the concentration of resources and data may be 'a more attractive target to attackers' but the benefits of scale in cloud computing allow for higher security provisions. Protection of IT infrastructure against cybersecurity risk now requires very specific professional skills that most companies cannot afford. On the contrary, recruiting this expertise is at the heart of cloud service providers businesses, whose reputation is highly dependent on their capacity to maintain the security of their customers' data.

When the data and its processing are performed externally to a given company, it may indeed create a feeling of loss of control over what is being transferred. This feeling is shared by national authorities, consumers and businesses. The public consultation pointed out that these groups often demand that their IT-providers store or process their data locally. When asked about the reasons behind this, 65.6% of respondents attributed high importance to critical/confidential nature of data as a reason for not storing or processing their data in multiple locations within the EU.

In a survey[86], 30% of business respondents recognised they preferred that the data generated and used by their business is stored and processed inside the country they operate. Over 35% of the respondents see location as a proxy for security of data. A 2014 Eurostat survey

[84] These position papers were received in the framework of the Public online consultation and accessible online via https://ec.europa.eu/digital-single-market/en/news/position-papers-received-framework-public-consultation-building-european-data-economy

[85] ENISA, Report "Cloud Computing Risk Assessment", November 2009, available at https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[86] LE Europe Study (SMART 2015/0016).

confirms that "risk of a security breach" is an important factor limiting the use of cloud services[87].

It may therefore be concluded that concerns about the security of data when stored in a datacentre abroad remain. At the same time, storage or processing of data within a specific geographical area or on-premises would not prevent data from being the target of cyberattacks and from the need to implement technical and organisational security measures (e.g. encryption, physical access control, data access management, disaster recovery plan, audit) to bring down the risk to an acceptable level and to implement incident management procedures. In addition, when data storage and processing services are contracted by users, security levels are important competitive criteria proposed by the providers. A restricted market, induced by data localisation measures, may lead to offers with suboptimal level of security.

In most cases, the level of security of data in electronic format does not depend on its storage location, but rather on **the security of the IT infrastructure,** the cybersecurity measures deployed in the IT systems and **the strength of the encryption techniques used**. The **WannaCry ransomware attack** of May 2017 is a recent example confirming this. This attack targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin electronic currency. The attack spread within a day to more than 230.000 computers in over 150 countries. However not every computer in those countries was affected, depending on whether users had upgraded their machine with the latest security patch. Therefore, the lack of trust still present in society is also an **awareness** problem.

The NIS Directive 2016/1148 provides legal measures to boost the overall level of cybersecurity in the EU. Member States are required to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority. A cooperation group has been set up in order to support and facilitate strategic cooperation and the exchange of information among Member States. A CSIRT Network has also to be set up in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks. Digital service providers, **including cloud computing services** and online marketplaces have also to comply with the security and notification requirements under the NIS Directive.

Also, accompanying the revision of the mandate of ENISA foreseen in September 2017, the European Commission may propose the establishment of a European Framework for ICT Security Certification and Labelling. Such a Framework would put in place the necessary conditions that allow the EU to further develop its capacities to conduct ICT security assessments across a wide area of ICT products, services and systems, including cloud services.

Trustworthiness of contracted or procured ICT systems is one of important features the buyers are considering. However, a simple claim that a data service is secure is often not enough to ensure user's trust in it. In a recent public consultation of the European Commission[88] almost 38% of respondents stated that the current ICT security certification

[87] Eurostat, "Factors limiting enterprises from using cloud computing services, by size class, EU-28", 2014 (% enterprises using the cloud); http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

[88] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-contractual-ppp-cybersecurity-and-staff-working-document (2016)

schemes did not adequately support the needs of European industry (either suppliers or users of secured ICT solutions).

A number of **security certification schemes** for ICT products exist in the EU[89] but they are effective only in a few Member States and the use of existing schemes is not actively promoted. An ICT service provider might need to undergo several certification processes in order to provide reassurance on its service in different Member States. There is also a fundamental problem of comparability between the different existing cloud security labels in the market.[90] In addition, the number of cloud service providers adhering to one of these schemes remains very limited.[91]

While security evaluations are a very technical area, the ability to determine adequately and to attest independently whether a product, system or service meets specific security requirements lies at the heart of being able to trust the digital systems we rely on. Carrying out these evaluations in a harmonized way across the European single market would prevent innovation from being stifled or industry from being over-burdened, while providing recognizable trustworthy security marks for potential buyers and users.

Problem 4: Vendor lock-in

There is a clear tendency in the data storage / processing (cloud) market that once a business has chosen to contract with a cloud service provider, they stay with that provider. There are both technical and legal barriers to switch cloud services providers.

When asked in the public consultation[92] whether they had ever intended to switch cloud providers, nearly 72% of all respondents answered yes, and nearly half (45%) of these indicated to have experienced difficulties with doing so. This problem is larger for SMEs and start-ups: 56,8% of which have experienced such difficulties.

Driver 7: Technical issues: data formats, transfer modalities

The main concern for cloud services customers is how to move data to another cloud service provider or to their own premises at low cost, without risking lower service levels and with minimal disruption. Portability of data is of most concern for Software as a Service (SaaS)[93], Platforms as a Service (PaaS)[94] and certain Infrastructure as a Service (IaaS)[95] providers and customers. For these services the content, data schemas and storage format are under the control of the cloud service provider. For the other IaaS, the cloud service customer has greater control of the technical modalities, potentially reducing their problems with portability.

---

[89] COM(2016)410, "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" and accompanying Staff Working Document, SWD(2016) 216.
[90] SMART 2015/0018, TimeLex, Spark, "Clarification of Applicable Legal Framework for Full, Co- or Self-Regulatory Actions in the Cloud Computing Sector" (Ongoing).
[91] Ibid.
[92] [Reference to POC synopsis report here once published]
[93] Cloud service category in which the cloud service customer can use the **cloud service provider's** applications (ISO/IEC 17788). See also Annex 9 for common definitions and examples.
[94] Cloud service category in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider (ISO/IEC 17788). Also Annex 9.
[95] Cloud service category in which in which the cloud service customer can provision and use processing, storage or networking resources (ISO/IEC 17788). Also Annex 9.

The lack of interoperability of **data formats** is an important barrier to data portability in the cloud context. This forces cloud users to re-process and reformat their data before moving it from one cloud service to another. In order to be able to successfully port data, cloud users need better knowledge of the formatting being applied to the data, as well as an understanding of how data are organized in the cloud service (i.e. data schema/model, semantics/meaning of the data, access of datasets to the underlying infrastructure, business logic between data, etc.). Without such knowledge it is very difficult to prepare for the migration of data sets. Many cloud services providers are not transparent about their set-up.

There is also an issue with the **transfer modalities** for data sets in the cloud. Many cloud users experience difficulties in terms of time allotted for the acquisition and transfer of data. The internet bandwidth needed to transfer large amounts of data is considerable, and networks have physical limitations in terms of the volume and speed of the traffic they can handle. Also, bandwidth costs money. There may also be differences between the cloud vendors in the data transfer connectivity speeds they use, and the network reliability itself could cause issues.

Driver 8: Different concepts of portability, lack of clear contractual rules and practices, inefficient use of standards

Portability generally refers to the ability to move, copy or transfer electronic data. The legal and practical implementation of portability varies according to the objective for porting and what exactly is to be ported. Consumer and data protection laws are two relevant examples.

Article 20 of the **General Data Protection Regulation (GDPR)** gives data subjects a right to port their personal data. It allows them to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller. 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. Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the **free flow of personal data** in the EU and foster competition between controllers.

Consumers also benefit from a certain level of protection through existing general consumer legislation, and the proposal for a Directive on the supply of digital content envisages a right for consumers to retrieve non-personal data from professional suppliers in certain circumstances.

With the possible exception of the additional rights to portability included in article 48 of the recently adopted French Digital Republic Bill ("Loi Lemaire")[96], **existing laws generally do not provide portability rights for legal persons**. For business users of cloud services, portability is regulated by the contract with their cloud service provider(s). This means that business users of cloud services are themselves responsible for ensuring their interest in data portability is sufficiently protected in the contract they agree with the cloud service provider (e.g. including what data can be ported, price, data formats and time limits).

[96] Article 48 of the French Loi Lemaire (entitled "Récupération et portabilité des données") states that consumers shall have a right to portability of their data. For what concerns personal data, the right shall be equal to that in the GDPR Article 20. The question is how, and to what extent the right will apply to non-personal data. French law also does not differentiate between professional and private 'consumers', as opposed to EU law, and may therefore in theory also be invoked by legal entities (including business users of platforms).

Switching of cloud service providers for business users entails the ability of users to move from one provider to another or benefit from different cloud services without data or applications being locked-in during the contract term or when their contract expires or is terminated. The ability to move data and applications between different systems and/or service providers is a key enabling factor for the freedom to choose and engage with suppliers, and to leverage their respective cloud services. To avoid confusion with the principle of data portability as introduced in the GDPR (which is a right relating only to data subjects), **this IA also uses term "switching"**, although this should be understood to include porting of data back to a user's own in-house IT resources**.**

In their response to the public consultation[97] hardly any of the business respondents claiming to offer data portability to their customers gave examples of the conditions posed. One possible reason could be that **conditions are rarely stated in contracts** with the customers. Judging from the results of a study on Switching between Cloud Services Providers[98], as well as from workshops[99] and meetings the Commission has had with stakeholders, there is a widespread **lack of exit strategies in the contracts** between businesses and their cloud service providers.

This seems to be the case in the assessment, negotiation and update/termination phases of the contracting. Exit strategies are also often missing from the Service Level Agreements or Service Level Objectives that accompany cloud service contracts. In order to enable switching, these documents should specify e.g. the electronic format(s) for data transfer, the interface to be used, APIs, transport protocols, minimum speed/bandwidth rates of transfer.

Including exit strategies in cloud contracts is not mandatory, and cloud service providers mostly offer 'take it or leave it' terms to customers. Many of the larger business customers do not have problems with adapting to this, e.g. by bearing the cost of managing a migration process themselves. However, SMEs and small start-ups often do not have the resources, nor do they have sufficient negotiating power to protect their interest.

Cloud services are developed using building blocks with standard interfaces. **Standards** are the cornerstone of interoperability and portability of these building blocks, defining how cloud components work and guaranteeing security and speed. Standards should define the functionality and in many cases also the Quality of Service (QoS). However, different cloud service providers' specifications are often incompatible, as **providers have little incentive to facilitate easy transfer of data of their customers to competitors**.

It should be borne in mind that the complexity of cloud standards depends on the type of service. IaaS and PaaS standards can be defined using simple interfaces. SaaS standards are often not possible or at least require more complex interfaces. Each application is different and although clusters of applications may be interoperable, usually industry sectors do not collaborate. This is not necessarily due to a deliberate intention to lock-in. Application variations might well be necessary to respond to different customer requirements.

Consequences

This section assesses the consequences of the problems identified and described in the preceding sections. The consequences shown already occur at present and will persist if no policy action would be undertaken.

[97] [Reference to POC synopsis report here once published]
[98] IDC and Athur's Legal Study (SMART 2016/0032) Switching Between Cloud Services Providers.
[99] EC Workshop on Switching between Cloud Services Providers, Brussels, 18 May 2017.

Consequence 1: Loss of growth and innovation potential

There is an inextricable causality between the take-up of new digital technologies and growth of business. The European Commission's Digital Economy and Society Index of 2017 identifies digital transformation as a core strategy for European businesses to enhance their efficiency, reduce costs and better engage customers and business partners[100]. To enable growth, therefore, the development and uptake of new technologies needs to be stimulated.

Those new digital technologies are increasingly dependent on data flows, which form the fundament of the most prominent disrupting technological paradigms of today: the Internet of Things, data analytics and artificial intelligence. That is why obstacles to data mobility within the EU would mean barriers to economic growth and innovation.

The public consultation highlighted that most respondents identified the impact of data localisation restrictions as 'high' in general, but predominantly on the categories 'launching a new product or service', 'entering a new market' and 'providing a service to private entities'. These categories are all synonymous to growth and characterise an innovative economy.

An especially harmful element of data localisation in this respect is that small companies, such as start-ups are disproportionately affected by them. Outcomes of the public consultation emphasized the detrimental effects of duplication costs that these companies are confronted with because they need to process data in different Member States when they want to operate in the single market but across borders. Costs for running servers in multiple locations, for example, are recurrent instead of one-off, state 95,6% of respondents to the relevant section of the public consultation. These costs are easier to bear for larger companies, but make it impossible for immature start-ups and small SMEs to compete with their larger competitors. As crucial innovations are often introduced in the economy by start-ups, the distortions stemming from data localisation restrictions mean a loss of innovation and growth potential.

Data localisation does not only impose innovation problems for the ICT-industry but for all sectors, as they cannot benefit from product and service innovation[101] and are unable to pass on savings to their users.

The problem is also measurable, already today, in terms of cost of non-Europe, or foregone growth potential. Indeed, according to one study, "If existing data localising measures are removed, GDP gains are estimated to up to 8 billion euros per year (up to 0.06% of GDP), which is on par with the gains of recent free trade agreements (FTAs) concluded by the EU. These gains approximate the impact of a fully price-transparent "industrial" DSM".[102]

Innovative technologies affected

The majority of **big data analytics** platforms function through distributed architectures supporting applications for **machine learning and artificial intelligence** in all sectors. These technologies are migrating towards distributed models, with state-of-the-art database

[100] DESI, 2017.

[101] J. Force Hill finds data free flow policies as limiting data flows and competition between firms. Over time, these policies will raise costs, retard technological innovation and the internet's 'generativity'. The author examined data localization policies and found that these policies are distorting trade and undermining human rights. See Jonah Force Hill, "The Growth of Data localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders", Lawfare Research Paper Series, 2014, available at: https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf

[102] European Commission, DESI, 2017

algorithms optimising[103] the distribution and use of data across servers in remote locations. In such applications, an imposed data location (not excluded in the current status quo by restrictions on tax data, for example), *de facto* **limits the participation** in the 'chain' for participants in specific locations.

Applications relying on the **Internet of Things** could suffer from legal uncertainties or blockages brought by data localisation. With an explosion in the number of connected objects in a variety of application areas – connected cars, manufacturing, energy, oil extraction, etc. – data generated by the Internet of Things is geographically distributed by design.

Cloud computing services are also affected. As this particular problem poses particular spin-off problems to the rest of the economy, this will be discussed at more length in the next section.

Consequence 2: Loss of operational efficiency

Legal uncertainty and lack of trust caused by (perceived) data localisation restrictions, combined with vendor lock-in concerns, restrain cloud adoption. This leads to a loss of operational efficiency for the wider economy. A study estimated that all companies can cut their overall IT-expenditure with 20% to 50% by migrating services to the cloud.[104] However, only 29% of larger EU companies see themselves as ready for these technologies while more than 50% say they are not. For the SMEs the picture is worse, only 6% of SMEs have adopted big data technologies and only one out of every five enterprises in the EU use cloud services.

This means that there is still a large potential for gaining efficiency, as data storage and processing services such as cloud computing can support especially small businesses across sectors in reducing their infrastructure investment to virtually no initial cost and transform substantial fixed costs into affordable variable costs (i.e. subscriptions to data services). Moreover, such services allow them to be active on the global market through the internet. However, data localisation measures limit the access of businesses to global cloud services, driving up prices and curbing the quality of services offered on the single market.

As respondents mention in the public online consultation, data localisation restrictions inhibit international competition in cloud services, which in turn diminishes the impetus to lower prices and improve services. This raises costs and reduces opportunities for both small and large companies that rely on these services. A less competitive cloud market drives up costs for businesses even further when they have to invest in data storage in multiple countries. That inflates their own prices, stifles product innovation and makes it costlier to enter new markets. The overall effect is a less competitive and less innovative economy with inflated prices and diminished choices for consumers.

Cost

The cost of storing data varies between EU Member States. There is an average difference of 120% from the cheapest to the most expensive[105], which is more than doubling the cost.

[103] E.g. The Spanner database architecture used by Google for its advertising applications brings a globally-distributed and fully synchronously replicated database, where data is automatically redistributed across servers and across data centres to balance load, to mitigate latency and availability of data and to prevent damage through a span of incidents, including natural disasters. Such technological solutions bring resilience in data storage and processing, by amortising risks over distributed machines and locations.
[104] Deloitte Study (SMART 2014/0031)
[105] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016

However, two thirds of the ICT-related demands are still sourced locally, also where prices are highest. These extra costs result comparatively bigger for SMEs, accounting for nearly 60% of European GDP and 65% of European employment. Therefore, increasing their efficiency would have a wide impact on the economy.

Consequence 3: Inefficiencies in the data centres sector

Data localisation restrictions can lead to inefficiencies in the allocation of data centres, as cloud service providers would be inclined to deploy data centres in Member States with large markets where localisation restrictions are in place. Topographically, however, such larger markets are often suboptimal places to deploy data centres in terms of costs or environmental footprint.

As an example, private estimations[106] show that it can cost up to 120% more to build a data centre in some European locations compared to others because of higher land, labour and operating costs. Examples of the latter are higher energy prices, or increased energy consumption to maintain efficient operating temperatures when located in warmer European regions. In the most 'expensive' EU Member State the cost of operating a data centre is twice as high as in the 'cheapest' Member State.

In addition, the choice of location for a data centre depends on a variety of conditions, and risk-indexes used by industry include risk of natural disasters, cost of compliance with administrative requirements, energy costs, average temperature, proximity of skilled workforce, ease of doing business, political stability etc.[107] These criteria converge to a business decision on the placement of a data centre, and the current overemphasis on one of them – e.g. legal and administrative requirements for data localisation – can overthrow other criteria – e.g. energy costs or environmental considerations.

Consequence 4: Market distortions

An analysis of the data processing service market in Europe points to difficulties for European players to scale up and be competitive on the European market. More than 50% of revenues from public cloud services in Europe are collected by the largest seven cloud service providers, whilst smaller players offer customised services at national level[108]. A study shows that historically, public cloud services were introduced in Europe by the large international players, mostly with headquarters based in the US, occupying 17 of the top 25 positions on the EU market.[109]

This problem of market distortion is caused partly by the existing restrictions on data mobility over geographical borders (data localisation restrictions) and over IT-systems (vendor lock-in), generating market distortions that are reflected in a number of barriers to use, choose and provide data storage as well as processing services within the EU.

First, the lack of trust and legal uncertainty affect the perception of reliable available suppliers and distort the rational purchase decisions. These market distortions cause misallocation of resources in the economy and affect supply and demand in the concerned market. The distortion leads to a cost increase due to the higher level of inefficiency in the upstream market.

---

[106] ECIPE, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", December 2016.
[107] Time.lex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (SMART 2015/0054).
[108] Deloitte Study (SMART 2014/0031).
[109] (IDC, 2014)

Second, the ability to port data for switching providers has been identified as an issue that leads to market distortion by the public consultation. 43% of respondents to the public consultation in Austria and 38% of those in Spain indicated that they would be more likely to adopt public cloud if they were guaranteed data portability for switching providers.

The size of the consequences in terms of market distortions is likely to be large. The data market in the EU27 is estimated in 46 billion[110] Euros[111]. 37% of the data storage and processing service providers responding to the public consultation had experienced demands by their customers for local data storage or processing, mostly due to an assumption or perception that they are required to do so.

The rough estimation would be that the size of the supply that is affected by market distortions resulting from legal uncertainty responds to a demand of 17 billion Euros (37% of 46 billion). This figure is large enough to condition the competing options of the whole market and to have wider implications in terms of a less efficient single market for data based services.

[110] The word billion is used referring to the short scale, i.e., 1 Billion = 1 000 000 000
[111] IDC Study (SMART 2013/0063), Table 29.

ANNEX 6: DATA LOCALISATION MEASURES AND OBLIGATIONS PER MEMBER STATE

Member State	Source	Source type	Data type	Localisation Restriction	Specific Storage Requirement	Prior Authorisation/ Notification Requirement	Availability Requirement	Other Requirements	Source
AT	Gesundheitstelematikgesetz (GTelG 2012), BGBl. I Nr. 111/2012 (Federal Act on Data Security Measures when using personal electronic Health Data or Health Telematics Act 2012), § 6, 14 and 20	Legislation	Health data	Yes	Yes	Yes	No	Yes	SMART 2015/0054;
AT	Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen, BGBl. I Nr. 60/2007; Latest amendment: BGBl. I Nr. 117/2015; (Federal Act on the Supervision of Securities), Art. 25, 26; Specified by the Austrian national regulation Auslagerungsverordnung, BGBl. II Nr. 215/2007, latest amendment: BGBl. II Nr. 272/2011	Legislation	Financial data	Yes	Yes	No	Yes	No	SMART 2015/0054;

AT	Bundesgesetz über allgemeine Bestimmungen und das Verfahren für die von den Abgabenbehörden des Bundes, der Länder und Gemeinden verwalteten Abgaben (Bundesabgabenordnung - BAO), original version: BGBl. Nr. 194/1961, latest amendment: BGBl. I Nr. 163/2015 (Federal Act on the General Principles and Procedures for the Regulation of Taxation as administrated by the Federal Government, the State Governments and the Municipalities (Regulation of Taxation Code, BAO). Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen (Unternehmensgesetzbuch - UGB), Austrian Commercial Code, original version: dRGBl. S 219/1897, latest amendment: BGBl. I Nr. 163/2015.	Legislation	Tax, accounting, company data	No	No	No	Yes	No	SMART 2015/0054;
AT	Bundesgesetz über die Bundesrechenzentrum GmbH (BRZ GmbH), Federal Act on the Federal Computing Centre (BRZ); Original version: BGBl. Nr. 757/1996, Latest amendment: BGBl. I Nr. 71/2003. Bundesgesetz, mit dem IKT-Lösungen und IT-Verfahren bundesweit konsolidiert werden (IKT-Konsolidierungsgesetz – IKTKonG), Federal Act on the Consolidation of ICT Solutions and IT Processes (ICT Consolidation Act), Original version: BGBl. I Nr. 35/2012.	Legislation	Public and government data	Yes	No	Yes	No	No	SMART 2015/0054;

BE	Article 315 of the Income Tax Code	Legislation	Tax, accounting, company data	Yes	No	No	Yes	No	SMART 2015/0054; Public Consultation;
BE	Article 60, § 3 of the VAT Code and ; Circulaire AGFisc N° 14/2014 (n° E.T. 120.000) dd. 04.04.2014	Legislation in conjunction with administrative guideline	Tax, accounting, company data	Yes	Yes	No	Yes	No	Public Consultation;
BE	Circular PPB 2004/5 on healthy management practices in outsourcing by credit institutions and investment companies) ; Issued by the Belgian Banking, Finance and Insurance Commission on 22 June 2004	Administrative guideline	Financial data	No	Yes	Yes	Yes	No	SMART 2015/0054;
BE	(Law of 8 August 1983 regulating a National Register of natural persons), Articles 4 ter, 5, 8 § 1 and § 2 and Article 14.	Legislation	Public and government data	No	No	No	No	Yes	SMART 2015/0054;
BG	Gambling Act, Promulgated, State Gazette, No. 26/30.03.2012, lastly amended and supplemented, SG; No. 1/3.01.2014, effective 1.01.2014, article 6(4).;	Legislation	Tax, accounting, company data	Yes	No	No	No	No	SMART 2015/0054;
BG	Accounting Act (promulgated on 08 December 2015, in force as of 01 January 2016) (article 12), Value Added Tax Act (promulgated on 04 August 2006, last amendments in force as of 01 January 2016) (Articles 121 and 122), Tax and Social Insurance Procedure Code (promulgated on 29 December 2005, last amendments in force as of 15 April 2016) (Article 73);	Legislation	Tax, accounting, company data	No	Yes	No	Yes	No	SMART 2015/0054;

DE	(Muster-) Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (“MBO-Ä“); ((Model) Professional Code for doctors working in Germany.; Federal regulation in conjunction with recommendation of Kassenärztliche Bundesvereinigung (Federal Association of Physicians participating in the public health insurance system	Administrative guideline	Health data	No	Yes	No	Yes	Yes	SMART 2015/0054;
DE	Decision of the Federal CIO Council (No. 2015/5) (3a)	Administrative decision	Public and government data	Yes	Yes	Yes	No	No	Stakeholder Engagement;
DE	§ 146 and 147 II Tax Code (Abgabenordnung, AO).	Legislation	Tax, accounting, company data	Yes	No	Yes	Yes	No	SMART 2015/0054; SMART 2015/0016; Public Consultation;
DE	§ 14 b II Act on Value Added Tax (Umsatzsteuergesetz, UStG).	Legislation	Tax, accounting, company data	Yes	Yes	Yes	Yes	No	SMART 2015/0016; Public Consultation;
DE	§ 41 I Income Tax Act (Einkommensteuergesetz, EStG)	Legislation	Tax, accounting, company data	Yes	No	No	No	No	SMART 2015/0016; Public Consultation;
DE	§ 257 HGB (German commercial code)	Legislation	Tax, accounting, company data	Yes	Yes	No	Yes	No	SMART 2015/0054; SMART 2015/0016; Public Consultation;
DE	Article 7 AGPStG (Law on the implementation of the civil registry in Bavaria)	Legislation	Public and government data	Yes	No	No	No	No	SMART 2015/0016;

DE	§ 87 Subs 1 No. 6 BetrVG (Works Council Constitution Act)	Legislation	Tax, accounting, company data	No	No	No	No	Yes	SMART 2015/0016;
DE	sec. 80 SGB X (German Social Law Code Book 10)	Legislation	Public and government data	Yes	Yes	No	No	No	Stakeholder Engagement;
DE	sec. 35 German Banking Act	Legislation	Financial data	No	Yes	No	No	No	Stakeholder Engagement;
DE	§ 126 III Grundbuchordnung (real estate register)	Legislation	Public and government data	Yes	Yes	No	No	No	SMART 2015/0054;
DK	Audit Act (section 45)	Legislation	Public and government data	Yes	Yes	Yes	Yes	No	Stakeholder Engagement;
DK	Sammenskrevet udgave af persondataloven, Lov nr. 429 af 31. maj 2000 som ændret ved § 7 i lov nr. 280 af 25. april 2001, § 6 i lov nr. 552 af 24. juni 2005, § 2 i lov nr. 519 af 6. juni 2007, § 1 i lov nr. 188 af 18. marts 2009, § 2 i lov nr. 503 af 12. juni 2009, § 2 i lov nr. 422 af 10. maj 2011, § 1 i lov nr. 1245 af 18. december 2012 og § 1 i lov nr. 639 af 12. juni 2013; Act on Processing of Personal Data (law implementing the Data Protection Directive, section 41, nr 4).	Legislation	Public and government data	Yes	No	No	No	No	Danish Data Flow Report;
ES	Resolución 320/14546/13, de 23 de septiembre and implementing acts (Data held by contractors to the Ministry of Defence)	Legislation	Public and government data	No	Yes	No	No	Yes	SMART 2015/0016;

FR	Law n°80-538 dated 16 July 1980 ('French Blocking Statute') - Information which could adversely affect the sovereignty, security, public order or essential economic interests of France when used as evidence in foreign judicial or administrative proceedings or in relation thereto.	Legislation	Public and government data	Yes	No	No	No	No	SMART 2015/0016;
FR	Ministerial decree dated 30 November 2011 on the protection of the secrecy of national defense ('Defense Decree')	Legislation	Public and government data	No	No	No	No	Yes	SMART 2015/0016;
FR	Code du Patrimoine and Note d'information du 5 avril 2016 relative à l'informatique en nuage (cloud computing)	Legislation	Public and government data	Yes	Yes	No	No	No	SMART 2015/0016;
FR	Act number 2002-303 of 4th March 2002 ; and ; 1111-8 of the French Public Health Code	Legislation	Health data	No	No	Yes	No	No	SMART 2015/0016; Public Consultation;
FR	Secure Cloud certification/label ((Secure Cloud), defence data (Secure Cloud Plus))	Legislation	Public and government data	Yes	Yes	No	No	No	SMART 2015/0016;
HR	Law on the State Information Infrastructure, Official Gazette of Republic of Croatia no. 92/2014 passed on July 15, 2014 and Regulation on Organizational and Technical Standards for Connecting to the State Information Infrastructure, Official Gazette of Republic of Croatia no. 103/2015.;	Legislation	Public and government data	Yes	No	Yes	Yes	No	SMART 2015/0054;
HR	Croatian National Bank	Administrative decision	Financial data	Yes	No	No	No	No	Stakeholder Engagement;

HU	Act L of 2013 on Electronic Information Security of State and Municipal Bodies ("Information Security Act") adopted by the Hungarian Parliament with the effect of 25 April 2013. ; Act CLVII of 2010 on National Data Assets ("Data Assets Act"), adopted by the Hungarian Parliament with the effect of 22 December 2010;	Legislation	Public and government data	Yes	Yes	Yes	No	No	SMART 2015/0054;
IE	Notice from the Revenue Commissioners published in Iris Oifigiuil (Official Journal), 27 January 2012, drawn up in exercise of powers conferred on them by s.887 of the Taxes Consolidation Act 1997 (substituted by s.232 of the Finance Act 2001). (Regulatory Regulated Act);	Administrative guideline	Tax, accounting, company data	No	Yes	No	Yes	No	SMART 2015/0054;
LU	19 December 2002. - Law concerning the register of businesses and companies, and concerning accounting and annual accounts of companies, modifying certain other legal provisions; 23 January 2003. – Grand Ducal Regulation relating to the execution of the law of 19 December 2002 concerning the register of businesses and companies, and concerning accounting and annual accounts of companies	Legislation	Public and government data	Yes	Yes	No	No	No	SMART 2015/0054; SMART 2015/0016;

LU	Circular CSSF 12/552 on central administration, internal governance and risk management, as amended by Circulars CSSF 13/563 and CSSF 14/59, issued by the Luxembourg Supervisory Commission of the Financial Sector (Commission de Surveillance du Secteur Financier - CSSF), Section 5.2.3, Sub-section 7.4.2.1, Sub-section 7.4.2.3;	Administrative guideline	Financial data	No	Yes	Yes	No	No	SMART 2015/0054; SMART 2015/0016;
LU	Loi du 10 août 1915 concernant les sociétés commerciale Section IV, Paragraph 3, Art. 39; Section IV, Paragraph 6, Art. 73; Section XIV, Art. 267(1), ARt. 281 (1)b), 295(1), etc.	Legislation	Tax, accounting, company data	Yes	No	No	Yes	No	SMART 2015/0016;
NL	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties - Kamerbrief over cloud computing; (Ministry of Internal Affairs and Kingdom Relationships – Chamber letter on cloud computing),; issued by the Minister of Internal Affairs and Kingdom Relationships, M. Donner, on 20 April 2011	Administrative guideline	Financial data	No	Yes	Yes	Yes	No	SMART 2015/0054;
NL	The Public Records Act 1995 (Archiefwet 1995), Public Records Decree 1995(Archiefbesluit 1995) and the Public Records Regulation 2009; (Archiefregeling 2009); Chamber letter on cloud computing, Issued by the Minister of Internal Affairs and Kingdom Relationships, M. Donner, on 20 April 2011	Legislation in conjunction with administrative guideline	Public and government data	Yes	Yes	Yes	No	No	SMART 2015/0054;
PT	(Article 4(1) of Decree-Law No 16/93) (as amended by Law No 14/94 of 11 May)	Legislation	Public and government data	No	Yes	Yes	No	No	SMART 2015/0054;

RO	Government Decision no. 111/2016 approving the Norms of application of 24 February 2016 on gambling, Articles 2, 127 and 136.;	Legislation	Tax, accounting, company data	Yes	Yes	Yes	Yes	No	SMART 2015/0054;
RO	Government Decision no. 585/2002 approving the national standards for the protection of classified information; Law no. 182/2002 on the protection of classified information; And Order issued by a public authority - the National Registry Office for Classified Information;	Legislation	Public and government data	No	Yes	Yes	No	No	SMART 2015/0054;
SI	1. Zakon o tajnih podatkih (Uradni list RS, št. 60/11) (IS); 2. Uredba o varovanju tajnih podatkov (Uradni list RS, št. 74/2005); 3. Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov (Uradni list RS, št. 71/06 in 138/06) ;	Legislation	Public and government data	Yes	Yes	Yes	No	No	SMART 2015/0054;
SI	Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (Uradni list RS, št. 30/2006) (IS);	Legislation	Public and government data	No	Yes	Yes	Yes	No	SMART 2015/0054;
UK	Regulator approach	Administrative practice	Health data	No	Yes	No	No	No	Public Consultation; Stakeholder Engagement;
UK	Companies Act 2006	Legislation	Tax, accounting, company data	Yes	No	No	Yes	No	SMART 2015/0016; Public Consultation; Stakeholder Engagement;

ANNEX 7: APPLICABILITY ASSESSMENT OF SECONDARY EU LEGISLATION

Relevant provisions	Uncertain applicability (out of 45 measures)	Potentially applicable (out of 45 measures)
Article 16 TFEU & Articles 1(1) and 1(3) of the GDPR "Free Movement of Personal Data"	7	0
Article 9(4) of the GDPR "Limitations to Free Movement of Personal Data"	3	0
Articles 1 and 2 of the E-Commerce Directive "Scope & Information Society Service"	25	8
Article 1(5) of the E-Commerce Directive "Exemptions"	5	8
Article 3 of the E-Commerce Directive Free Movement of Information Society Services	6	4
Article 3(3) and Annex of the E-Commerce Directive "Exempted fields"	0	0
Article 3(4) of the E-Commerce Directive "Conditions for justified restrictions"	4	4
Article 4 of the E-Commerce Directive "Principle excluding prior authorisation"	6	2
Articles 1 and 2 of the Services Directive "Scope"	5	28
Article 2(2) of the Services Directive "Exemptions"	21	9
Articles 16-18 of the Services Directive "Freedom to provide services"	7	3

Articles 9-13 of the Services Directive "Authorisation schemes"	3	2
Articles 14-15 of the Services Directive "Prohibited requirements"	6	0
Articles 19-21 of the Services Directive "Rights of recipients of services"	12	5
Article 1 of the Single Market Transparency Directive "Scope"	28	3
Article 1(2) and Annex of the Single Market Transparency Directive "Exemptions & Derogations"	12	0
Articles 4 and 5 of the Single Market Transparency Directive "Duty to Notify"	10	0
Public Procurement Directive "Principle of Non-Discrimination, Equal Treatment and Transparency"	14	0

ANNEX 8: EXISTING MECHANISMS FOR COOPERATION BETWEEN PUBLIC AUTHORITIES IN RELATION TO ACCESS TO DATA

1. Criminal Matters

For the purposes of examining cooperation in the area of criminal matters, extensive use has been made of the analyses developed by the Commission Services on cross-border access to electronic evidence for criminal investigations.[112] The overview of related measures developed by the research project the "Evidence Project"[113], funded by the European Commission, has also been consulted. This has been complemented by desk research on the Cyber Crime Convention, as well as on the European Investigation Order Directive.

Guidance from colleagues at DG Justice and DG Home has facilitated identification of mechanism in intelligence gathering, in the area of prevention of organized crime.

Mutual Assistance and the European Investigation Order Directive

The Directive regarding the European Investigation Order (EIO) in criminal matters, to have been transposed by 22 May 2017,[114] replaces the framework of cooperation for obtaining cross-border access to electronic evidence in the Convention on Mutual Assistance in Criminal Matters. The EIO Directive allows for the issuance of an EIO, *i.e.* "a judicial decision which has been issued or validated by a judicial authority of a Member State to have one or several specific investigative measure(s) carried out in another Member State to obtain evidence."[115] Member States have the obligation to "execute an EIO on the basis of the principle of mutual recognition".

To facilitate the cooperation among judicial authorities foreseen in the EIO Directive, certain practical improvements are being developed by the Commission. "Electronic user-friendly version of the form set out in Annex A of the EIO Directive to request the securing and obtaining of e-evidence" is being worked on by the Commission.[116] The Commission is also working on Council's request for "a secure platform for the online exchange of electronic evidence between EU judicial authorities".[117] It is expected that the platform should be functional towards summer of 2019.

Following the 9 June 2016 Council Conclusions on improving criminal justice in cyber-space[118], and the subsequent mandate given to the Commission by the Justice and Home Affairs Council on 8 June 2017[119], a legislative initiative on cross-border access to electronic

---

[112] See: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

[113] http://www.evidenceproject.eu/.

[114] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

[115] EIO Directive, Article 1(1). Further, "EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State."

[116] Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace at p. 14, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf;

[117] Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace at p. 15.

[118] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf

[119] http://www.consilium.europa.eu/en/meetings/jha/2017/06/08-09/

evidence by law enforcement authorities for criminal investigations is now being considered and developed by the Commission Services[120] in two key respects: direct cooperation with Service Providers (creating a framework for production requests or production orders directed at Service Providers) and direct access to electronic evidence stored remotely. Further, practical measures could be implemented, such as streamlining of providers' procedures when responding to access requests.

The Fourth Anti-Money-Laundering Directive

The fourth Anti-Money Laundering Directive[121] provides for "exchange of information or the provision of assistance between EU Financial Intelligence Units (FIUs)."Pursuant to Article 53(1), "Member States shall ensure that FIUs exchange, spontaneously or upon request, any information that may be relevant for the processing or analysis of information by the FIU related to money laundering or terrorist financing and the natural or legal person involved, even if the type of predicate offences that may be involved is not identified at the time of the exchange." The use of such information thus obtained is limited to "the accomplishment of the FIU's tasks as laid down in this Directive." (Art. 54). Further, "when exchanging information and documents [pursuant to the Directive], the transmitting FIU may impose restrictions and conditions for the use of that information", with which the receiving FIU must comply.

2. Taxation

The following overview of Member States' cooperation in the area of VAT monitoring was produced jointly with colleagues from TAXUD.

Council Regulation (EU) 904/2010 of 7 October 2010,[122] allows cooperation and exchange of "any information that may help to effect a correct assessment of VAT, monitor the correct application of VAT, particularly on intra-Community transactions, and combat VAT fraud"[123]

Such exchanges can take place on request,[124] where requests can be refused on specific grounds defined in the regulation,[125] are submitted in standard forms and information must be

[120] Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace : https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf; Non – paper; Non-paper from the Commission Services: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

[121] Directive (EU) 2015/849 of the European Parliament and of The Council of 20 May 2015 on The Prevention of The Use of The Financial System For The Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 Of The European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849

[122] OJ L268 of 12/10/2010, p.1

[123] Council Regulation (EU) 904/2010 of 7 October 2010, OJ L268 of 12/10/2010, p.1 [hereinafter the "VAT Cooperation Regulation"] at Article 1; European Court of Auditors, Special Report No. 24 "Tackling intra-Community VAT fraud : More action needed", December 2015.

[124] VAT Cooperation Regulation at Article 7, where under Art. 7(2) " For the purpose of forwarding the information referred to in paragraph 1, the requested authority shall arrange for the conduct of any administrative enquiries necessary to obtain such information."

[125] VAT Cooperation Regulation at Article 7(4) and Article 54.

provided to the requesting Member State "as quickly as possible and no later than three months following data of receipt of the request."[126]

Automatic exchanges of information also take place pursuant to the VAT Cooperation Regulation, where the categories of information shared have been determined under Commission Implementing Regulation 79/2012.

Storage of certain VAT data by the Member States for exchange between Member States

The Regulation also imposes an obligation on Member States to store electronically specific categories of information (collected pursuant to the VAT Directive, *e.g.* cross-border transaction data (VAT ID-number and value of the transaction) declared in the recapitulative statement by the traders; data when the VAT ID-number becomes invalid)[127], without requiring storage of the invoices by the trader within the given Member State's territory. Each Member State must grant the competent authority of any other Member State access to this information[128]. Article 18 requires that the "information [be] made available for at least five years from the end of the first calendar year [in which] access is to be granted.", and that Member State adopt "the measures necessary to ensure that the data provided by taxable persons and non-taxable legal persons […] are, in their assessment, complete and accurate."

A VAT information exchange system (VIES) has been established for transferring data stored in the Member States databases between the competent authorities of the Member States.

The Regulation also provides for the possibility of competent authorities from one Member State to be present **in the offices of the administrative authorities**[129] of another Member State (or in "any other places where those authorities carry out their duties"), "by agreement", and "with a view to exchanging information" for VAT monitoring/application. Also "by agreement, one Member State's officials may be present "**during the administrative enquiries**" carried out in the territory of the requested Member State, and "Such administrative enquiries shall be carried out exclusively by the officials of the requested authority."[130] "The officials of the requesting authority shall not exercise the powers of inspection conferred on officials of the requested authority. They may, however, have access to the same premises and documents as the latter, through the intermediation of the officials of the requested authority and for the sole purpose of carrying out the administrative enquiry".

Member States may also agree to conduct **simultaneous controls**, "whenever they consider such controls to be more effective than controls carried out by only one Member State."[131] For that purpose an expert group – the MLC (multilateral controls) Platform - has been set up. In practice, simultaneous controls are carried out in relation to cross border transactions, i.e. transactions between different traders located in different Member States (an example is the so-called VAT-carousel fraud).

Storage of invoices by the taxable person

[126] VAT Cooperation Regulation at Article 10.
[127] VAT Cooperation Regulation at Article 17.
[128] VAT Cooperation Regulation at Article 21.
[129] VAT Cooperation Regulation, Article 28(1).
[130] VAT Cooperation Regulation, Article 28(2).
[131] VAT Cooperation Regulation, Article 29(1).

This obligation is set out in the VAT Directive 2006/112/EC[132]. Invoices can be stored in a Member State other than where VAT is due provided the taxable person makes the invoices or information contained therein available to the competent authorities without undue delay whenever they so request (Article 245 of VAT Directive). Member States can forbid this if the country where invoices are stored is a third country with which no agreement on administrative cooperation exists.

Article 249 further specifies that in case there are electronic invoices, the competent authorities of both the Member State of establishment and the Member State where the VAT is due shall have the right to access, download and use those invoices.

Example: If a taxable person located in Member State A stores the data relevant to VAT compliance, in a data centre (own premises or third party premises) located in another Member State B, and must make this data available for control purposes in his Member State, several options are possible:

- First, the tax administration of Member State A can request the taxable person to make the data available in the premises located in Member State A or in the premises of the tax administration. [Note: Under Article 249 VAT Directive, in case taxable person stores invoices electronically, the competent authorities of both the Member State of establishment and the Member State where the VAT is due shall have the right to access, download and use those invoices.]

- Second, the tax administration of Member State A goes to the premises of the taxable person in the other Member State B (if the company agrees with this approach), but in this case they have to follow the rules on administrative cooperation (send out request for presence in the administrative enquiry, in order to inform the other tax administration).[133]

- Third, the tax administration authorities in Member State A can request, on the basis of the administrative cooperation rules, an administrative enquiry conducted by Member State B.

In the Report from the Commission to the Council and the European Parliament on the Application of Council Regulation (EU) no 904/2010 concerning administrative cooperation and combating fraud in the field of value added tax,[134] the Commission contemplated the mechanism of joint audits (where Germany and the Netherlands had launched a pilot bilateral project) and an assessment of such an option is underway.

The following overview of administrative cooperation in the area of direct taxation is the product of desk research and helpful exchanges with colleagues in DG TAXUD.

In the area of direct taxation, Council Directive 2011/16/EU has provided for three types of exchange of information between Member State tax administrations: exchange upon request; mandatory automatic exchange;[135] and spontaneous exchanges, whereby a Member State authority must communicate information in certain cases, where another Member State is

[132] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, OJ L 347, 11.12.2006, pp. 1–118.

[133] The proposed recast of the VAT Cooperation Regulation considers the option to allow authorities of Member State A to carry out controls without the presence of authorities from Member State B.

[134] COM/2014/071 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2014:0071:FIN "The OECD describes a joint audit as two or more countries joining together to form a single audit team to examine an issue(s) / transaction(s) of one or more related taxable persons (both legal entities and individuals) with cross-border business activities, perhaps including cross-border transactions involving related affiliated companies organized in the participating countries, and in which the countries have a common or complementary interest; where the taxpayer jointly makes presentations and shares information with the countries, and the team includes Competent Authority representatives from each country[10]."

[135] "Automatic exchange consists of the automatic provision of information by one country to another on income of residents of the second country," pursuant to specified timelines.

concerned.[136] The automatic sharing of information (usually in electronic form[137]) applies to income data (including five non-financial categories of income and capital) and to "interest, dividends and similar type of income, gross proceeds from the sale of financial assets and other income, and account balances". Financial account information and cross-border tax rulings/advance pricing arrangements must now also be automatically exchanged between Member States.[138]

The Directive also envisages administrative cooperation in the form of presence of officials of the Member State which has made a request for information to be present in the offices of the tax authorities of the requested Member State, or to be present during administrative enquiries carried out by the requested Member State.[139]

Under the recent "country-by-country reporting" amendment,[140] Member States in which a large multi-national entity[141] is resident for tax purposes, must distribute a country-by-country report, concerning latter entity. Such report must include "information for every tax jurisdiction in which the MNE group does business on the amount of revenue, the profit (loss) before income tax, the income tax paid and accrued, the number of employees, the stated capital, the retained earnings and the tangible assets."

"Compulsory social security contributions payable to the Member State (…) or to social security institutions established under public law" are notably out of scope of the Council Directive 2011/16/EU on direct taxation (Article 2). Under social security coordination rules, however, an Electronic Exchange of Social Security Information system) (EESSI) will be made available in July 2017.[142] **The EESSI system** will enable "all communication between national institutions on cross-border social security files": "social security institutions will exchange structured electronic documents and follow commonly agreed procedures. These documents will be routed through EESSI to the correct destination in another Member State."

3. Financial Sector Mechanisms

The following information exchange provisions have been referred to in an overview of sectorial regulatory instruments provided by DG FISMA.

Banking

The fourth Capital Requirements Directive or "CRD IV" (Directive 2013/36/EU)[143] provides for close collaboration between competent authorities of Member States, for supervision of institutions operating "in particular through a branch, in one or more Member States other than that in which their head offices are situated."[144] "Member States shall supply one another

[136] The Council Directive 2011/16/EU at Article 9.
[137] http://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en
[138] Council Directive (EU) 2015/2376 of 8 December 2015 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.332.01.0001.01.ENG&toc=OJ:L:2015:332:FULL
[139] Council Directive 2011/16/EU, Chapter III, Articles 11 – 12; "Also provided for are simultaneous controls (audits), notifications to taxpayers of requests received from another MS, and sharing of best practices".
[140] Council Directive (EU) 2016/881 of 25 May 2016 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation.
[141] This applies to MNEs with total consolidated revenue equal or higher than € 750.000.000.
[142] http://ec.europa.eu/social/main.jsp?catId=869&langId=en
[143] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC ("**CRD IV**").
[144] CRD IV at Article 50.

with all information concerning the management and ownership of such institutions that is likely to facilitate their supervision and the examination of the conditions for their authorization, and all information likely to facilitate the monitoring of institutions, in particular with regard to liquidity, solvency, deposit guarantee, the limiting of large exposures, other factors that may influence the systemic risk posed by the institution, administrative and accounting procedures and internal control mechanisms." Certain information on liquidity must be provided "immediately" by Member States.[145]

In addition, Article 117(1) stipulates an obligation of close cooperation: "The competent authorities shall cooperate closely with each other. They shall provide one another with any information which is essential or relevant for the exercise of the other authorities' supervisory tasks under this Directive and Regulation (EU) No 575/2013. In that regard, the competent authorities shall communicate on request all relevant information and shall communicate on their own initiative all essential information." Essential information includes "identification of the group's legal structure and the governance structure including organisational structure, covering all regulated entities, non-regulated entities, non-regulated subsidiaries and significant branches".

"Where a request for collaboration, in particular to exchange information, has been rejected or has not been acted upon within a reasonable time", the competent authorities may refer the case to the EBA.[146] Further, pursuant to Article 50(6), the "EBA shall develop draft regulatory technical standards to specify the information referred to in this Article.", and "Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010."

With respect to the **permitted recipients of information** – the "competent authorities" - the CRD IV allows that the information so exchanged be shared between the competent authorities and a defined list of specified bodies, mostly, with a supervisory mandate in the financial sector.[147]

As for the free exchange of information within a group of companies, Article 124 requires Member States to "ensure that there are no legal impediments preventing the exchange, as between undertakings included within the scope of supervision on a consolidated basis, mixed-activity holding companies and their subsidiaries, or subsidiaries as referred to in Article 119(3), of any information which would be relevant for the purposes of supervision in accordance with Article 110 and Chapter 3."

Outsourcing requirements are not specifically addressed in CRD IV, although outsourcing is considered subject to prudent management and internal governance requirements (*e.g.* Article 74 CRD IV). Regulators' guidelines address this issue more specifically: the CEBS Outsourcing Guidelines from 2006 (para. 8) recommend a right for a supervisor to conduct on-site inspections at the premises of the service provider. Referring to this provision, the EBA's Draft Recommendations on Outsourcing to Cloud Service Providers[148] (currently under a consultation process) state that the outsourcing agreement should provide for

[145] CRD IV at Articles 50(2) and 50(3).
[146] CRD IV at Articles 50(5).
[147] CRD IV at Article 56.
[148] EBA, Consultation Paper on the Draft Recommendations on Outsourcing to Cloud Service Providers under Article 16 of Regulation (EU) No 1093/2010, EBA/CP/2017/06, 17 May 2017, available at: https://www.eba.europa.eu/documents/10180/1848359/Draft+Recommendation+on+outsourcing+to+Cloud+Service++%28EBA-CP-2017-06%29.pdf

supervisory authorities' right of access (to the cloud service provider's premises, "including in the full range of devices, systems, networks and data used for providing the services to the outsourcing institution") and right of audit ("unrestricted rights of inspection and auditing of the outsourcing institution's data") (para. 10).

Further, if a bank stores its data in another entity belong to the same banking group (subsidiary or branch), or even using the storage services of another licenced bank, in another Member State, the access for the home/host supervisors should be either automatic in accordance with their regulatory rights, or obtained via the cooperation obligations under Article 56 of CRD IV. [149]

In the example the data of the bank (subject to a supervisory authority in Member State A), is stored in another private entity outside the banking group (service provider not subject to CRD IV/banking regulation), in Member State B (*e.g.* under an outsourcing agreement). The service provider, not being a licensed entity, is not subject to CRD IV and Member State B banking supervisory authorities do not have any authority over this service provider (*at least not under the EU Directive CRD IV; they could have authority on another legal basis*). The information-sharing provisions in CRD IV only apply between competent authorities, not *governments*, and in this case, under CRD IV only, there is no competent authority in Member State B to cooperate with the banking supervisor in Member State A.

In latter scenario, pursuant to the CEBS Guidelines, access for supervisor should be ensured under outsourcing agreement concluded between bank and the service provider. Not enabling access for the supervisor would be a violation of CRD IV by the outsourcing bank.

Asset Management

Various fund frameworks contain rules for exchange of information between supervisors. This information is subject to confidentiality and professional secrecy obligations.

For example, the **UCITS** Directive[150] in its Article 101(1) provides that "The competent authorities of the Member States shall cooperate with each other whenever necessary for the purpose of carrying out their duties under this Directive or of exercising their powers under this Directive or under national law." In addition, "competent authorities shall use their powers for the purpose of cooperation, even in cases where the conduct under investigation does not constitute an infringement of any regulation in force in their Member State."

Article 101(6) allows for investigation on the territory of a Member State, requested by the authorities of another Member State: "The competent authorities of one Member State may request the cooperation of the competent authorities of another Member State in a supervisory activity or for an on-the-spot verification or in an investigation on the territory of the latter within the framework of their powers pursuant to this Directive." In that case, the receiving authority shall: "(a) carry out the verification or investigation itself; (b) allow the

[149] Article 56 CRD IV: "Article 53(1) and Article 54 shall not preclude the exchange of information between competent authorities within a Member State, between competent authorities in different Member States or between competent authorities and the following, in the discharge of their supervisory functions: (a) authorities entrusted with the public duty of supervising other financial sector entities and the authorities responsible for the supervision of financial markets; (b) authorities or bodies charged with responsibility for maintaining the stability of the financial system in Member States through the use of macroprudential rules; (c) reorganisation bodies or authorities aiming at protecting the stability of the financial system […].

[150] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS Directive), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02009L0065-20140917&from=EN .

requesting authority to carry out the verification or investigation; or (c) allow auditors or experts to carry out the verification or investigation."[151]

The latter type of cooperation may be refused "only where (a) such an investigation, on-the-spot verification or exchange of information might adversely affect the sovereignty, security or public policy of that Member State; (b) judicial proceedings have already been initiated in respect of the same persons and the same actions before the authorities of that Member State;

(c) final judgment in respect of the same persons and the same actions has already been delivered in that Member State.[152]

The Directive on Alternative Investment Fund Managers (the AIFM Directive) provides for the same type of cooperation by supervisory authorities and the same grounds for refusal.[153]

Capital Markets

The Market Abuse Regulation 596/2014 provides for an obligation on national competent authorities to cooperate with each other and with ESMA "where necessary for the purposes of the Regulation".[154] Also, they "shall render assistance to competent authorities of other Member States and ESMA. In particular, they shall exchange information without undue delay and cooperate in investigation, supervision and enforcement activities."[155]

On-site investigations or inspections, "with a cross-border effect" are foreseen in the Market Abuse Regulation, Article 25(6). In such cases, "ESMA shall, if requested to do so by one of the competent authorities, coordinate the investigation or inspection." The authority recipient of such a request from the authority of another Member State, may choose either of the following:

"(a) carry out the on-site inspection or investigation itself;

(b) allow the competent authority which submitted the request to participate in an on-site inspection or investigation;

(c) allow the competent authority which submitted the request to carry out the on-site inspection or investigation itself;

(d) appoint auditors or experts to carry out the on-site inspection or investigation;

(e) share specific tasks related to supervisory activities with the other competent authorities."

Further, Directive 2014/57/EU, OJ L 173 of 12.6.2014, which should be transposed by Member States by July 2016, establishes "minimum rules for criminal sanctions for insider dealing, for unlawful disclosure of inside information and for market manipulation"[156]

---

[151] In the first scenario (a), "the competent authority of the Member State which has requested cooperation may request that its own officials accompany the officials carrying out the verification or investigation" (Article 101(5) UCITS Directive).
[152] UCITS Directive, Article 101(6).
[153] Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0061 at Article 54.
[154] Market Abuse Regulation at Article 25.
[155] Market Abuse Regulation at Article 25.
[156] Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive) at Article 1.

On jurisdiction, the Directive requires that Member States establish jurisdiction, where the offenses have been committed in whole or in part in their territory or have been committed by one of their nationals (at least where the act is an offense where it was committed). [157]

Member States must notify the Commission if they establish jurisdiction over offenses committed outside of their territory, "where the offender is a habitual resident in its territory" or "the offence is committed for the benefit of a legal person established in its territory".[158]

Insurance

Under the Solvency II Directive,[159] Article 68, certain information can be exchanged between supervisory authorities in the same Member State. Article 68 goes on to say that subject to obligations of professional secrecy, "exchanges of information [in 68(1)(b) and (c)] may also take place between different Member States." Information is not defined in Solvency II, however, Recitals (26), (36), (38) indicate this would be information required for the public authorities' supervision under the Directive, serving the two main objectives of policyholder protection and preservation of financial stability.

As under the CRD IV, national supervisors could cooperate and exchange information pursuant to Article 68 above, when the data concerns regulated entities/groups with presence in the given Member States. However, when such cooperation would involve a request for data held by a non-regulated entity, e.g. a service provider providing data processing services to a regulated entity, the national supervisor could not seek the assistance of its counterpart in the Member State where the service provider provides the data service (e.g. stores the data). The responsibility is on this national regulator and on the regulated entity to enable such data availability.

It has also been suggested that "access" per se is not really a concern for national supervisors but rather, integrity (and confidentiality) of the data, and that the national supervisor will rarely seek the assistance of a private outsourcing company, as it can rely on the obligations of the regulated insurance company.

4. Competition Law Mechanisms for National Regulators

The proposed Directive "to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market"[160] contains provisions on mutual assistance. In particular, a national competition authority (NCA) would be able to request another NCA to carry out investigative measures on its behalf to gather evidence located in another jurisdiction, and officials from the requesting NCA would have the right to attend and actively assist in that inspection.

5. Obtaining data as evidence in civil or commercial matters

The Regulation 1206/2001 on cooperation between the courts of EU countries in the taking of evidence in civil or commercial matters has created "a European system of direct and rapid transmission and execution of requests". The Regulation is applicable in all EU Member States except Denmark. With respect to Denmark, the Hague Convention on the taking of

[157] Market Abuse Directive at Article 10.
[158] Market Abuse Directive at Article 10.
[159] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), available at : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02009L0138-20140523
[160] Proposal from 22 March 2017 available at: http://ec.europa.eu/competition/antitrust/nca.html

evidence abroad in civil or commercial matters is applicable. However, not all EU countries have acceded to this Convention.

The Regulation is based on the principle of direct transmission between the courts, according to which the requests for taking evidence are transferred directly from the 'requesting court' to the 'requested court'.

As explained in the European Commission's Practical Guide on the Regulation, four elements need to be present for the Regulation to apply[161]: [1] "requests for the taking of evidence [2] evidence intended for us in judicial proceedings, commenced or contemplated, [3] in civil and commercial matters [4] by the court of a Member State".

"Civil and commercial matters" is an "autonomous concept" of EU law, interpreted by the CJEU on multiple occasions. [162] In their Practical Guide, the Commission and the EJN explain that "The Regulation applies to all civil and commercial proceedings whatever the nature of the court or tribunal in which they are taking place. It will for instance apply to litigation based on civil and commercial law, consumer law, employment law and even competition law as far as private proceedings are concerned."
In one of its more recent interpretations of the Brussels I Regulation, (applicable to " civil and commercial matters whatever the nature of the court or tribunal"), the CJEU reminds that
" [33] …'civil and commercial matters' should not be interpreted as a mere reference to the internal law of one or other of the States concerned. That concept must be regarded as an autonomous concept to be interpreted by reference, first, to the objectives and scheme of that regulation and, second, to the general principles which stem from the corpus of the national legal systems. [34] **In order to determine whether a matter falls within the scope of Regulation No 1215/2012, it is necessary to identify the legal relationship between the parties to the dispute and to examine the basis and the detailed rules governing the bringing of the action**"[163]. In that case, CJEU concluded that ""enforcement **proceedings brought by a company owned by a local authority** against a natural person domiciled in another Member State, for the purposes of recovering an unpaid debt for parking in a public car park, the operation of which has been delegated to that company by that authority, **which are not in any way punitive but merely constitute consideration for a service provided**, fall within the scope of [the Brussels I] regulation."

"There is no definition of the concept of "court" in Regulation [1206/2001]. It should, however, be given a broad interpretation, thus including **all authorities in the Member States with jurisdiction** in the matters falling within the scope of the Regulation."[164]

---

[161] European Commission and European Judicial Network for Civil and Commercial Matters, "Practical Guide for the application of the Regulation on taking of evidence", available at: http://ec.europa.eu/justice/civil/files/guide_taking_of_evidences_en.pdf

[162] Ibid, citing cases interpreting the same term in the Brussels I Regulation..

[163] CJEU C-551/15, *Pula Parking d.o.o. v Sven Klaus Tederahn* 9 March 2017 at para 34. In para. 34, the CJEU refers to the case Sunico and others, C-49/12, where it decided that "The concept of 'civil and commercial matters' within the meaning of Article 1(1) of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters must be interpreted as meaning that it covers an action **whereby a public authority of one Member State claims, as against natural and legal persons resident in another Member State, damages for loss caused by a tortious conspiracy to commit value added tax fraud in the first Member State**."

[164] European Commission, "Practical Guide for the application of the Regulation on taking of evidence", available at: http://ec.europa.eu/justice/civil/files/guide_taking_of_evidences_en.pdf

The Regulation also requires Member States to designate a "central body" (Article 3) which would be responsible for "(a) supplying information to the courts; (b) seeking solutions to any difficulties which may arise in respect of a request; (c) forwarding, in exceptional cases, at the request of a requesting court, a request to the competent court."

Two means of taking evidence in another EU country are foreseen: the court before which a case is heard in one EU country can request the competent court of another EU country to take the necessary evidence; or it can instead take evidence directly in another EU country.[165] A delay of 90 days from receipt is set for execution of requests (Article 10(1)), and for the direct taking of evidence, the competent authority of the requested Member State must inform within 30 days if the request accepted and under what conditions per its national laws (Article 17(4). Article 17(2) mandates that "**Direct taking of evidence** may only take place if it can be performed on a voluntary basis **without the need for coercive measures**." Further, "The applicable law to coercive measures for executing a request is determined in accordance with the law of the Member State of the requested court to the extent that it provides for the execution of a request made for the same purpose by the national authorities of that Member State or one of the parties concerned (Article 13)."[166]

Direct taking of evidence can be refused by the central body or the competent authority on the grounds specified in Article 17(5): "(a) the request does not fall within the scope of this Regulation as set out in Article 1; (b) the request does not contain all of the necessary information pursuant to Article 4; or (c) the direct taking of evidence requested is contrary to fundamental principles of law in its Member State."

The CJEU has endorsed the interpretation whereby the Regulation 1206/2001 "**does not restrict the options to take evidence situated in other Member States, but aims to increase those** options by encouraging cooperation between the courts in this area" and that "a national court **wishing to order an expert investigation which must be carried out in another member State is not necessarily required to have recourse to the method** of taking evidence in Articles (1)(1)(b) and 17 of Regulation 1206/2001".[167]

Civil cooperation is facilitated by **the European Judicial Network ("EJN")** "by interaction between national EJN contact points and [the EJN] is the most important tool available in this area. The EJN is particularly important for solving practical difficulties in concrete cases involving cross-border judicial proceedings."[168]

As for its membership, the Commission's Guide for legal practitioners explains that the EJN "consists of one or more contact points designated by each of the Member States involved together with the various bodies and central authorities specified in the EU Civil Justice instruments and in international conventions and other instruments to which Member States

[165] Recital 15 of Regulation 1206/2001 reads: "'In order to facilitate the taking of evidence it should be possible for a court in a Member State, in accordance with the law of its Member State, to take evidence directly in another Member State, if accepted by the latter, and under the conditions determined by the central body or competent authority of the requested Member State.'"
[166] Ibid.
[167] C-332/11, *ProRail BV v Xpedys and others*, 21 February 2013 at para. 44 and para. 49.
[168] European Commission, "A guide for legal practitioners – Judicial cooperation in civil matters in the European Union", available at: http://ec.europa.eu/justice/civil/files/civil_justice_guide_en.pdf

are also party. The contact points play a key role in the Network. They are available to other contact points and to local judicial authorities in their Member State to assist them to resolve cross-border issues with which they are confronted and to provide them with any information to facilitate the application of the law of the other Member States applicable under Union or international instruments. They are also at the disposal of authorities provided for in Community or international instruments relating to judicial cooperation in civil and commercial matters. The contact points assist these authorities in all practicable ways. In addition, they communicate regularly with the contact points of other Member States."

6. Obtaining data for the effective supervision of service providers

The 2006 Directive on services in the internal market (the Services Directive) provides for an elaborate administrative cooperation mechanism.[169] The Member States are obliged to cooperate with each other and give mutual assistance in the supervision of service providers. In particular, authorities from different EU Member States have to exchange information with each other and carry out checks, inspections and investigations upon request. They also have to send an alert to another EU Member State in cases where a service activity could cause serious damage to the health or safety of persons or the environment. To facilitate the cooperation, the Commission has established an electronic system for the exchange of information (IMI).

In particular, Article 29(1) of the Services Directive foresees an obligation on the Member State of establishment (of the service provider) to "supply information on providers established in its territory when requested to do so by another Member State, in particular, confirmation that a provider is established in its territory and, to its knowledge, is not exercising his activities in an unlawful manner."

Further, under Article 29(2), the "Member State **of establishment shall undertake the checks, inspections and investigations requested by another Member State** and shall inform the latter of the results." These requested checks/investigations are subject to the scope of the powers "vested in them in their Member State." And the competent authorities decide on "the most appropriate measures to be taken in each individual case in order to meet the request".

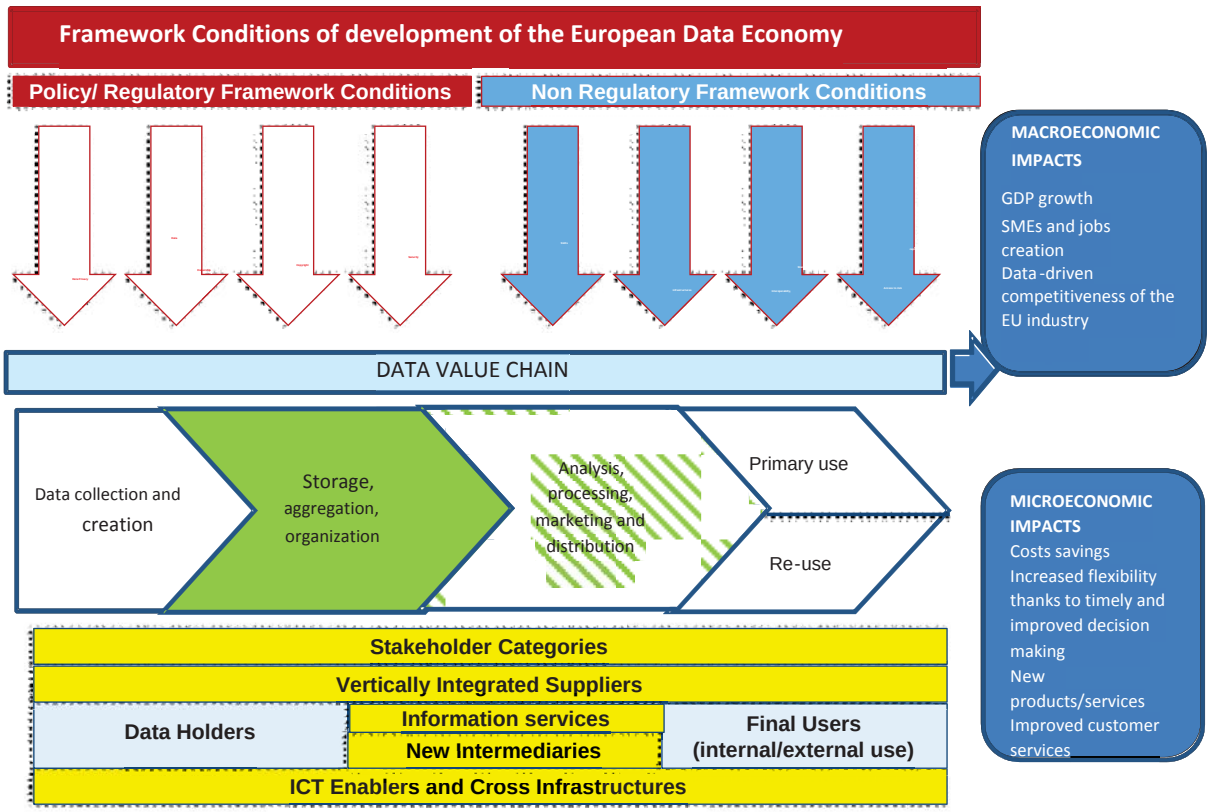
[169] Directive 2006/123/EC Of The European Parliament And Of The Council Of 12 December 2006 on services in the internal market, available at : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0123

ANNEX 9: EUROPEAN DATA ECONOMY, CLOUD SERVICES AND MARKETS

This Annex provides the reader with general but relevant background information on cloud computing in Europe. It starts with determining the place of cloud computing in the broader context of the data value chain that characterises the data economy. After this, the importance of cross-border data flows for the data economy is shown. After giving a number of definitions aimed to make the reader understand cloud computing better, the Annex concludes by giving an overview of dynamics in the European cloud market.

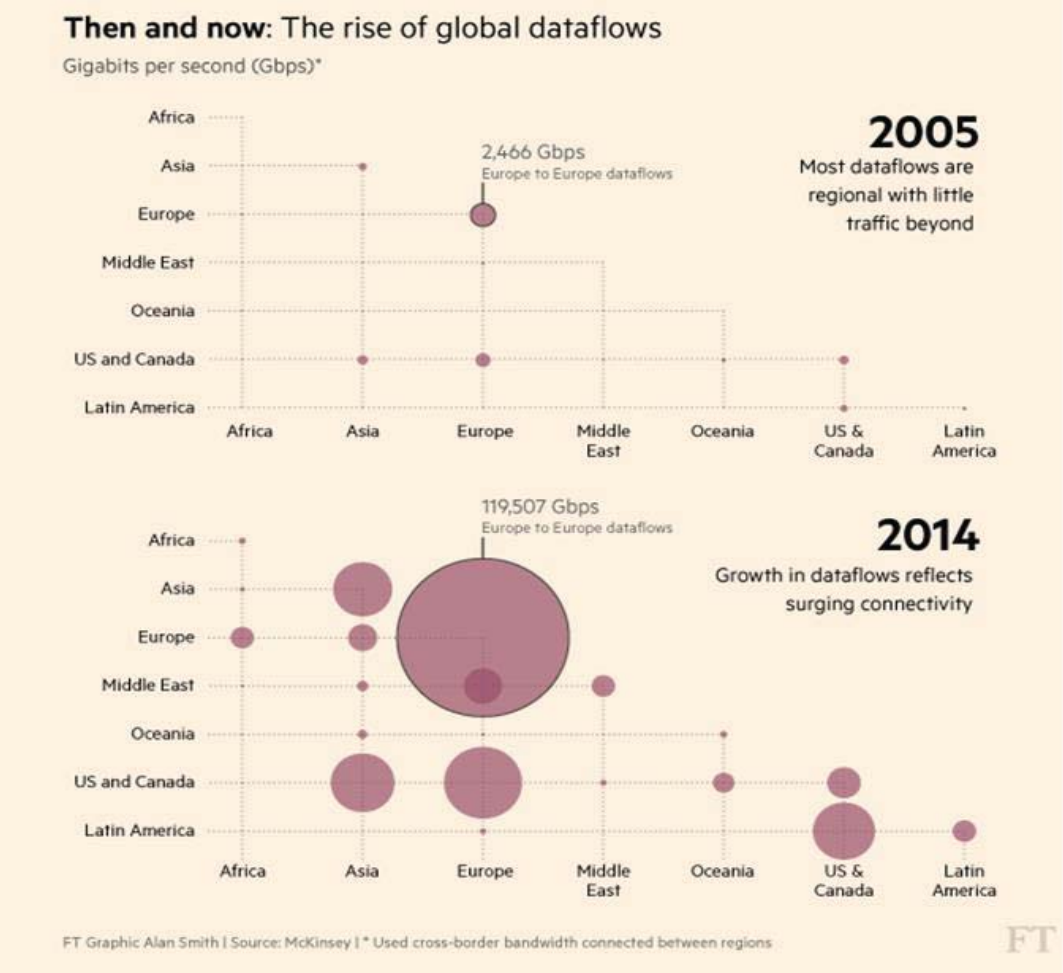
Data value chain: the "engine" of the data economy

A data lifecycle consists of four main stages: (i) data collection and creation; (ii) storage, aggregation, organisation; (iii) analysis, processing, marketing and distribution and (iv) use of data. As data moves through these stages, significant value can be added to it. The ability to use services from the entire internal market of the EU in the various processes is of importance to the data sector, in terms of the amount of services provided and also the quality and price of these services. This is one of the reasons why a free flow of data is important for a healthy and thriving European data economy. As illustrated in the figure below with a green marking, this initiative applies to the 'storage, aggregation and organisation' phase primarily, because it is in this stage where the 'data storage and processing' takes place, whether in the cloud or on in-house IT systems. Ensuring a free flow of data (across borders and IT systems) for this essential part of the data value chain is important to the existence of the entire data lifecycle.



Growing data flows, big part of data flows intra-EU

It is estimated that in 2014 alone, cross-border data flows contributed to $2.8 trillion in economic value globally, more than global trade in goods[170]. IMF data from 2008 to 2012 present cross-border information flows as the fastest growing component of US as well as EU trade[171]. A study by Mandel[172] found these flows to have increased by 49% while trade in goods and services simultaneously grew by only 2.4%.[173]



[170] McKinsey & Company, Digital globalization: The new era of global flows (2016)

[171] Aaronson, Susan Ariel (2015) Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security.

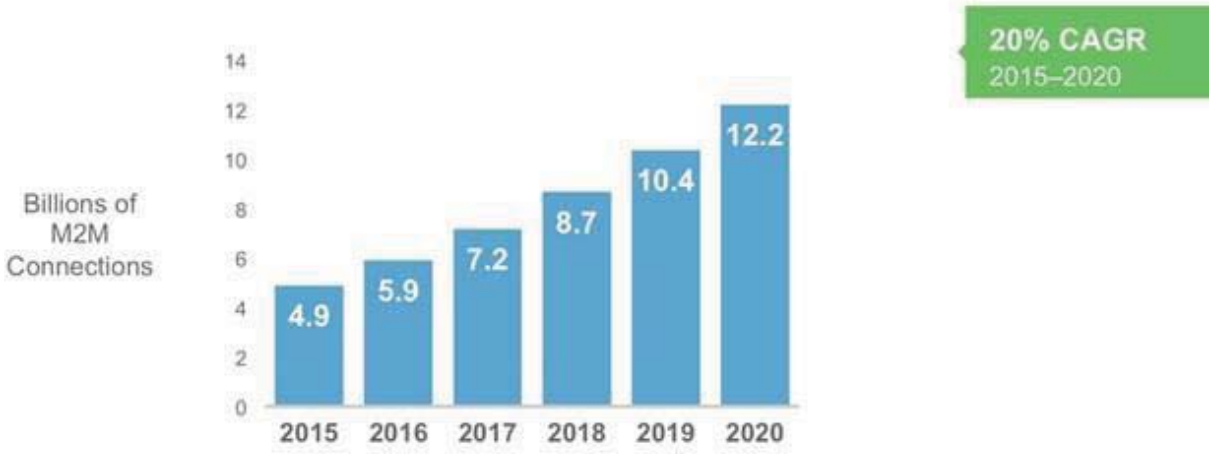
[172] Mandel, Michael (2013) Data, Trade, and Growth

[173] It is important to take into account that these figures, although consistent over time, are still estimates and are affected by the difficulty to measure cross border data flows owing to their lack of monetary footprints. The problem with measuring the financial benefits of cross border data flows is also related to its effect on the value added in terms of knowledge economy, whereby data changes hands but no money is transferred, (e.g. when downloading reports). This makes the internet a 'statistical problem' in trade. Trade statistics generally underestimate or completely ignore cross border data flows.

The figure above shows that intra-EU data flows are growing at the fastest pace globally, representing more than four times the volume of data flows between Asia and the North-America. A logical reason for this is the European internal market, which already provides for many fundamental cross-border freedoms and harmonisation. Still, barriers to data mobility could negatively effect further growth, as shown in section 6.2 of the Impact Assessment and in the problems section of Annex 5.

The largest component of future growth is expected to be non-personal machine-generated data, driven by e.g. IoT, digitising industry, satellite technology and financial transaction data, as shown by the figure below. This implies that an effective regime safeguarding the free flow and cross-server portability of non-personal data is an important element to put in place, in order to facilitate growth.

Growth in M2M (non-personal) data flows



Source: Cisco 2017

Cloud adoption or in-house data processing and storage

Organisations can choose whether they build their data infrastructure in-house or outsource storing and processing resources. With a rapid decrease of **costs for data storage** and processing services[174], cloud adoption can offer substantial opportunities facilitating economies of scale and allowing for innovative businesses and business models to emerge.

A survey of around 500 cloud-using companies[175] illustrates the cost reduction privileged by the uptake of cloud solutions: 81% of the companies admitted that their IT expenditure decreased by 10-20% with the use of the cloud, and 12% of companies saved 30% or more. An independent survey (EY, 2013) points to a significant 22% of companies surveyed, all sectors combined, using outsourced services for IT infrastructure and data centre service, with rampant outsourcing practices for cloud services and big data analytics.

[174] Understood as a "paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand" [reference]
[175] (IDC, 2014)

In 2014, 7% of SMEs and 17% of large enterprises used private cloud[176] services[177] destined for a single enterprise, either maintained in-house or supplied by a third-party. 12% of European SMEs and 24% of large enterprises use public clouds[178] offered by third-party cloud service providers (CSP) [179]. Moreover, a sector-specific analysis[180] shows that cloud computing services cover a substantial part of the market in those data-intensive sectors such as telecom/media (80% of organisations using Public cloud and 45% Private cloud), finance (76% Public cloud and 44% Private cloud), and distribution (74% Public cloud and 45% Private cloud). All the studies consulted[181] note a steady increase both in demand and offer of cloud services, with projections expecting for the EU cloud market to more than double its value by 2020[182].

Types of Cloud Services

Type	Definition	Example
Infrastructure as a Service (IaaS)	A service allowing the consumer to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. firewalls).	Gives software developers direct control over the computing and storage resources being provided by a cloud. This provides greater flexibility, at the cost of greater complexity to take advantage of all of the cloud's services. Examples include Amazon Elastic Compute Cloud, OVH vCenter, VMWare vCloud Express, etc…
Platform as a Service (PaaS)	A service allowing the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer	Enables software developers to build custom applications on clouds, taking advantage of the cloud ability to

[176] Private cloud is one of the deployment model of cloud computing. In this model, the cloud service is offered for a single client organisation and with the data being stored and processed in a private data centre. This service can be offered by a third party or in-house. Deloitte Study (SMART 2014/0031).

[177] Eurostat, "Factors limiting enterprises from using cloud computing services, by size class, EU-28", 2014 (% enterprises using the cloud); http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

[178] Public cloud services are offered by a provider to multiple organisations on a shared infrastructure (one or multiple data centres), Deloitte Study (SMART 2014/0031).Other models of cloud services exist, including hybrid (public/private) clouds.

[179] Estimates based on ESTAT survey (2014), covering the entire EU. NB: excludes sectors such as finance and public sector organisations. Eurostat, "Factors limiting enterprises from using cloud computing services, by size class, EU-28", 2014 (% enterprises using the cloud); http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises.

[180] (IDC, 2014)

[181] The high discrepancy between the two sources presented here is analysed in Deloitte Study (SMART 2014/0031) to show methodological divergences, including geographical and sector inconsistencies. This is complemented by a series of independent and industry studies, all pointing to a variation of market shares, but showing a steady increase in demand and offer.

[182] With estimates ranging from €28.4 billion - pessimistic scenario - to €59.6 billion - optimistic scenario (IDC, 2014).

	does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.	automatically provide additional computing and storage resources when required. Examples include IBM Websphere, Google App Engine, Microsoft Windows Azure, Amazon Elastic Beanstalk, etc…
Software as a Service (SaaS)	A service allowing the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through an interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	Remote software environments for example for email, word processing, customer relationship management, and many other types of applications. Examples include Google Docs, Calendar and Gmail, Spotify, Salesforce.com, Microsoft Office 365, SAP Business by Design, etc…

Cloud markets and market players

The European market for cloud computing services is a fast emerging market, as European adoption numbers are increasing sharply.[183] Despite the fact that US based providers are dominating the European market, there are patterns suggesting that there are numerous promising EU Public Cloud vendors that are working their way up in their home market.

The recent Cloud Uptake Study provides figures on the key Cloud providers in Europe.[184] Of the top 25 Public Cloud vendors in the EU, 17 are headquartered in the US, seven are based in the EU and one (Visma) is based in Norway. The US companies have on average twice the revenue of the EU based providers, which are all applications vendors. The top five European-based public cloud service providers by European market share are:

- SAP (Germany): SAP's main cloud focus is on offering SaaS applications for CRM and ERM. Even though the company made a relatively early start in the SaaS market, it initially had disappointing results. However, since then the company has made acquisitions and improved its Public Cloud offerings, and is now experiencing impressive growth, which is explained in further detail below and illustrated in figure 6. SAP is not only the leading European-based Public Cloud provider on the EU market, but also the world's largest vendor of business management software, including enterprise resource management, customer relationship management, and supply chain management;
- T-Systems (Germany): In terms of its Cloud services, T-Systems' main focus is on providing Private Cloud services. Nevertheless, it also offers a virtual Private Cloud (services based on a shared environment but with enhanced security and control compared to "standard" Public Cloud

[183] The demand of Cloud computing in Europe: drivers, barriers, market estimates. Research in Future Cloud computing workshop (IDC 2012)

[184] SMART 2013/43, "Uptake of Cloud in Europe - Follow-up of IDC Study on Quantitative estimates of the demand for Cloud computing in Europe and the likely barriers to take-up", 2014, see: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742

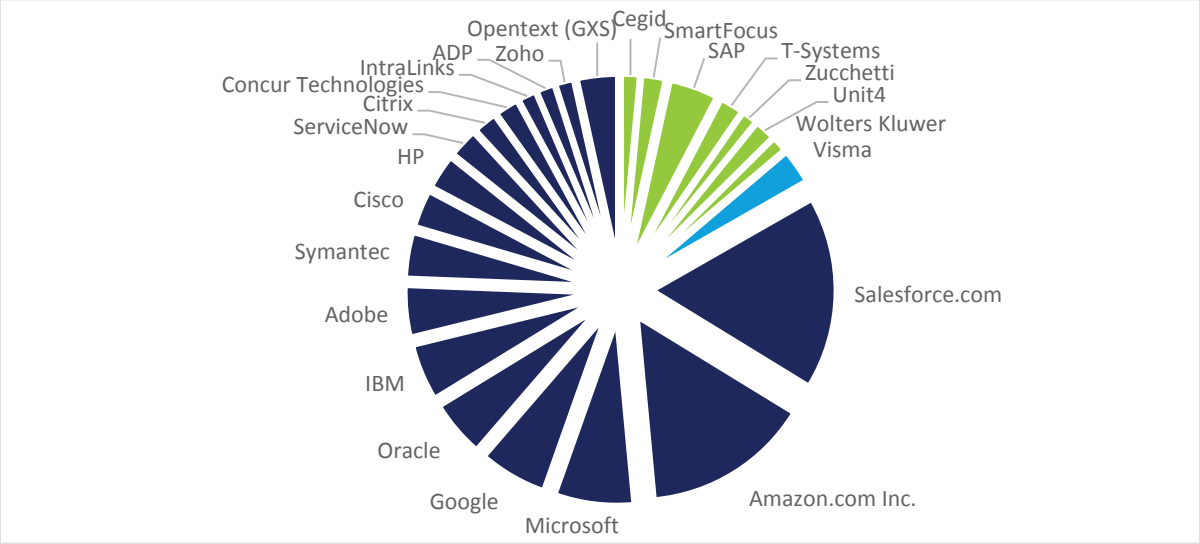
offerings), which is Public Cloud services according to IDC. T-Systems is a subsidiary of Deutsche Telekom, which has a long standing involvement in the European IT market;

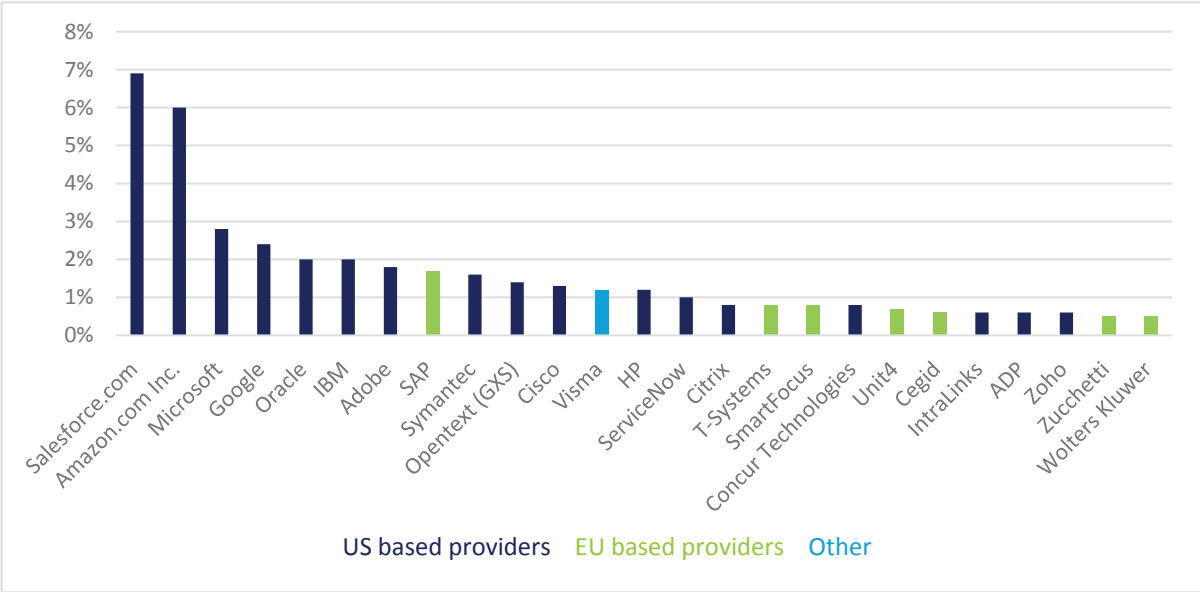
- SmartFocus (France/UK): Smartfocus is a provider of SaaS services for email, social and mobile marketing. Founded in Paris in 1999 as Emailvision, the company acquired UK-based Smartfocus in 2013 and subsequently took the SmartFocus name for the combined company and moved its group headquarters to London;
- Unit 4 (Netherlands): Unit 4 is a business applications vendor based in the Netherlands. It offers its applications as multi-tenant applications but with isolated tenant databases. Coda, its leading financial management software suite, has a range of different solutions that can be hosted on its cloud infrastructure, and it has a number of data centers for cloud hosting in different European locations;
- Cegid (France): Cegid is a long-standing French vendor of business applications that also offers SaaS applications. It says it has 24,000 small companies using its SaaS accounting services, and over 650 mid-sized and large customers for its SaaS services.

In terms of market comparison of the top 25 Public Cloud vendors by origin, the 17 US headquartered providers collectively generate 83% of the total revenue of the top 25 Public Cloud vendors, while the seven EU based providers generate only 14% as can be seen on the Figure here-under. This is equivalent to a 2% share on average per EU based provider, whereas the US providers have a share of 4.9% per provider on average.

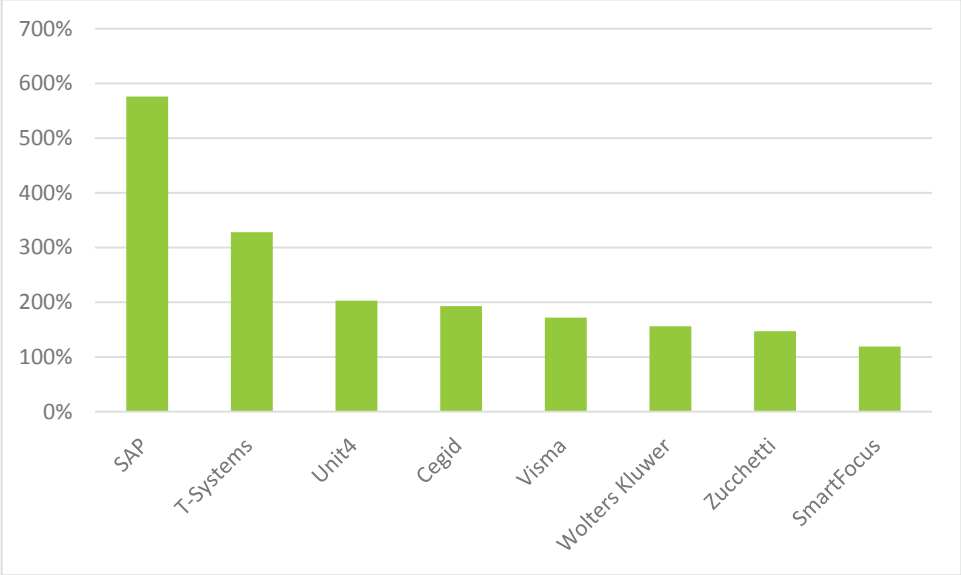
It is also worth noting that GXS (bought by Opentext) recently relocated its headquarters to the US. This highlights another ongoing issue that faces EU based IT companies. They are often the target for acquisition by US based companies or investors, resulting in an inevitable ‘westwards shift’ in ownership.

The NASDAQ stock market is also seen by many European IT business owners as being a more attractive option when looking to take their company public, again leading to EU businesses becoming foreign owned. Unfortunately, there is very little acquisition activity in reverse by EU based businesses taking over US owned companies.





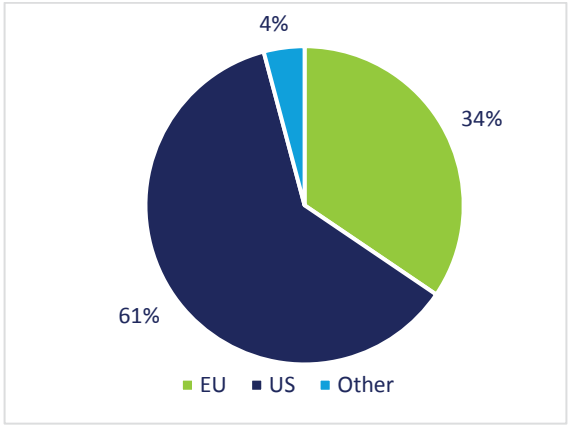
There was great disparity between the top 25 Public Cloud vendors' growth rates in EU in 2012-2013. The average growth rate was 192%, while the range was from 18% at Cisco to impressive 576% at SAP. The disparity in growth rates is mostly driven by the differences between the providers' Cloud strategies. The growth rates of the seven EU based providers are illustrated in the figure below.



Growth 2012-2013 of top 8 European Public Cloud Services Providers in EU market

Clearly, SAP (Germany) stands out from the group with almost five times higher growth than SmartFocus which experience a growth rate of 119%. According to the recent study on cloud uptake, SAP's rapid growth is associated with a change in strategy from trying to get its customers to adopt a radical vision of cloud, centred on new and untried cloud offerings, to a more pragmatic approach centred on maximising growth from its existing cloud offerings.

Expanding the focus to the top 100 Public Cloud vendors in the EU, the numbers change and we can form a slightly different picture of the EU market. The top 100 providers collectively generate 56.6% of the total revenue of all Cloud service providers in the EU. Looking more specifically at top 26-100 providers, 49 of these are US-based and 23 are EU-based. US-headquartered companies still dominate the market with a 60.7% share of the total revenue of the top 26-100 Public Cloud vendors, while European companies generate a 34.1% share of this. This is equivalent to a 1.48% share on average per EU based provider, whereas the US providers have a share of 1.24% per provider on average.



Total Share of Revenue of Top 26-100 Public Cloud Vendors

The leading EU based private cloud services providers by European market share are T-Systems (Germany), Atos (France), Capgemini, BT GS, and Orange BS. European vendors

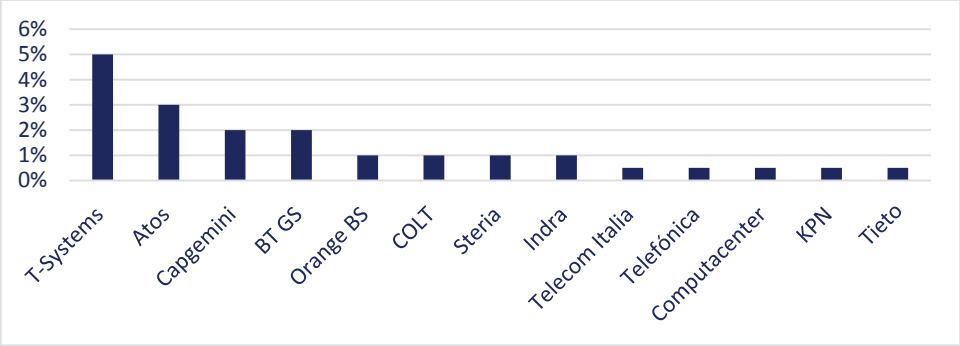
are the largest group amongst the vendors, and account for slightly under 50% of the overall revenue.[185]

European suppliers therefore have a strong presence in the private cloud market. The figure below shows the EU market share of the leading EU based private cloud service providers. It is worth nothing that even if we were to include non-EU headquartered suppliers, T-Systems would still be the largest single provider of private cloud services in the EU.

Nevertheless, according to an article by Forrester [186], IBM was the top private cloud service provider in 2013, but it was overtaken in 2014, where VMware managed to become the leading private cloud vendor in Europe. The statistics from both sources should be interpreted with caution since vendors are reluctant to separate results for their traditional hosting business and their private cloud businesses, so the estimates of revenues for these are not robust.

Moreover, the figures showing that T-Systems is the largest single provider of private cloud services in the EU is based on a separate analysis as private cloud services are not included in IDC's tracker programme[187].

EU Market Share of the leading European Private Cloud Services Providers



[185] SMART 2013/43, IDC, "Uptake of Cloud in Europe. Follow-up of IDC Study on Quantitative estimates of the demand for Cloud computing in Europe and the likely barriers to take-up ", 2014, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9742

[186] Forrester, Adoption Profile: Private Cloud In Europe, Q3 2014, March 2015.

[187] *Ibid.*