



EUROPEAN
COMMISSION

Brussels, XXX
[...] (2017) XXX draft

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

EXPLANATORY MEMORANDUM

The Mid-Term Review on the implementation of the Digital Single Market Strategy¹ adopted by the Commission on 10 May 2017 announced a legislative proposal on the EU free flow of data cooperation framework.

This proposal 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 General Data Protection Regulation (GDPR), the proposal would put in place a comprehensive and consistent EU framework enabling free movement of data in the single market.

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

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.

New digital technologies, such as cloud computing, big data, artificial intelligence and the Internet of Things (IoT) are designed 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 learning².

As indicated in the 2017 Communication "Building a European Data Economy"³, the value of the EU data market was estimated in 2016 at almost EUR 60 billion, showing a growth of 9.5% compared to 2015. According to a study, the EU data market could potentially amount to more than EUR 106 billion in 2020⁴.

To unlock this potential, the proposal offers resolution, in the short term, of 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;
- 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, while not creating burden to service providers or distorting the market;
- 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.

¹ COM(2017) 228 final;

² Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed.

³ 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.

⁴ IDC and Open Evidence, European Data Market, Final Report, 1 February 2017 (SMART 2013/0063).

The proposal addresses these four areas and concerns data storage and processing in a broad sense, encompassing the usage of all types of IT systems, whether located on the premises of the user or outsourced to a data storage/processing service providers⁵.

- **Consistency with existing policy provisions in the policy area**

The scope of this initiative is limited in order to ensure consistency with existing legal instruments. The initiative is consistent with the E-commerce Directive⁶ and the Services Directive⁷; it pursues the creation of 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 will rely on the notification regime under the Transparency Directive⁸ for addressing unjustified localisation restrictions. It is also consistent with the NIS Directive⁹ in so far as it builds on the implementation mechanisms provided therein to enhance cyber resilience of cross-border storage and processing of data.

The initiative focuses on aspects of data flows within the EU that are not regulated by the GDPR or the ePrivacy Directive: 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.

It also takes into account the existing solutions, of cooperation and mutual assistance in Union law on exchange and access to information.

- **Consistency with other Union policies**

In light of the Digital Single Market Strategy, this initiative intends to remove remaining barriers to a competitive data-driven economy in Europe. In line with the DSM mid-term Review Communication, the Commission is exploring separately these issues of accessibility and re-use of public and publicly funded data and privately held data which are of public interest and liability in cases of damage caused by data-intensive products and the issues of liability.

The policy intervention also builds upon the Digitising European Industry (DEI) policy package that included the European Cloud initiative¹⁰ aiming to deploy a high capacity cloud solution for storing, sharing and re-using scientific data. Furthermore, the initiative builds upon the revision of the European Interoperability Framework¹¹, 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 Internet¹².

⁵ Other data processing services include providers of data-based services like data analytics, data management systems, etc.

⁶ Reference

⁷ Reference

⁸ Reference

⁹ Reference

¹⁰ COM(2016) 178 final, "European Cloud Initiative - Building a competitive data and knowledge economy in Europe", 19 April 2016.

¹¹ COM(2017) 134 final, "European Interoperability Framework – Implementation Strategy", 23 March 2017.

¹² COM(2014) 72 final, "Internet Policy and Governance Europe's role in shaping the future of Internet Governance", <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2014:0072:FIN>

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

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.

This proposal introduces a common approach in the Union to ensure the free movement of data by laying down rules on data localisation restrictions, on the availability of data to competent authorities, and security of data storage and processing.

• Subsidiarity (for non-exclusive competence)

The proposal complies with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. The objective of this proposal and the free movement of data within the Union cannot be achieved by the Member States at national level, as the core problem is cross-border data mobility.

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.

However, divergent approaches would lead to multiplication of regulatory requirements across the EU single market, and tangible additional costs for enterprises, especially SMEs.

• Proportionality

The proposal complies with the principle of proportionality as set out in Article 5 of the Treaty on European Union, as it consists of an effective cooperation framework, suitable to all four intervention areas of this initiative, does not go beyond what is necessary to solve the identified problems and is proportionate to achieve its objectives.

The proposal will rely to a high degree on the existing EU instruments and frameworks: the Transparency Directive for notifications of data localisation restrictions and different frameworks ensuring data availability for regulatory control by 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 security interests of Member States as well as balance between EU regulation and self/co-regulation by the market. Thirdly, even though the proposal would necessitate action on the part of the public authorities of the Member States due to the notification / review requirements, the transparency requirements and the administrative cooperation, the proposal is designed to minimise such action to the most important cooperation needs and to avoid unnecessary administrative burden.

• Choice of the instrument

The Commission propose a Regulation. A regulation would best implement the policy choices as 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. This is particularly important to remove existing restrictions and prevent new ones to be enacted by Member States, to guarantee the legal certainty to enterprises and public sector organisations and to raise trust.

By establishing clear legal principles to be continuously developed and accompanied by cooperation between and with Member States, as well as self/co-regulation, this proposal will enhance legal certainty and raise trust levels in the short term, while staying relevant and effective in the long term because of the flexibility of the cooperation framework of the single

points of contacts in Member States. Since this proposal 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. This proposal also combines measures that are supported by stakeholders as best ways to foster the free movement of data in the EU single market.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

Stakeholder consultations

During a **first round of evidence gathering**, from the 2nd half of 2015 until the 2nd half of 2016, two studies on data location restrictions were commissioned. These two studies aimed at identifying data location restrictions in Member States and quantifying the impact of those data location restrictions on the functioning of the internal market. Further, 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. Two thirds of respondents – with an even distribution across all stakeholder groups, including SMEs – found that restrictions on the location of data have affected their business strategy. Additional economic evidence was targeted with one study on the economic impact of cloud computing in Europe. Other information gathering activities consisted of meetings and events, targeted workshops with key stakeholders (e.g. Cloud Select Industry Group) and dedicated workshops in the context of studies.

A **second round of evidence**, from end 2016 until the 2nd half of 2017, consisted in a **public consultation launched in the context of the Communication 'Building a European Data Economy'** on 10 January 2017. 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'). 61.9% of respondents indicated that data localisation restrictions should be removed and 55.3% argues for a legislative approach. The public online consultation also 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.

Three collective structured dialogue meetings with Member States and national representatives facilitated a common understanding of the challenges and opportunities at hand, and the bilateral engagement with a selected number of Member States helped to verify data localisation restrictions identified and address individual concerns. 16 Member States have explicitly called for a legislative proposal in a letter addressed to President Tusk. In addition a dedicated study on the issue of data portability/switching of cloud providers and a dedicated study on cloud certification schemes and security were launched.

The proposal takes on board a number of concerns signalled by stakeholders, in particular: the need for a cross-cutting free movement of data principle providing for legal certainty; guaranteeing safeguards with regards to the security of data and data availability for regulatory purposes; facilitating switching of data service provider for users of such services by giving more transparency in contracts with respect to the conditions of transfer at the end of the contract, but not imposing standards for switching /portability of data on service providers or imposing obligations on them at this stage.

- **Collection and use of expertise**

Legal and economic studies have been relied on various aspects of data mobility, including data localisation restrictions¹³, switching data providers/data portability¹⁴ and data security¹⁵. Further studies have been commissioned on the impacts of cloud computing¹⁶ and cloud uptake¹⁷, as well as on the European data market¹⁸. Studies have also been carried out concerning co- or self-regulatory actions in the cloud computing sector¹⁹. The Commission also relied on additional external sources, including market reviews and statistics (e.g. Eurostat).

- **Impact assessment**

An impact assessment was carried out for this proposal. A number of options were considered and the following set of options was considered in the impact assessment: a baseline scenario (no policy intervention) and three policy options. Option 1 consists of guidelines on the existing EU instruments and entailed strengthening of enforcement vis-à-vis different categories of unjustified or disproportionate data localisation restrictions imposed by Member States. Option 2 would lay down principles on the four policy intervention areas, including envisages the designation by Member States of single points of contact policy group, for discussing common approaches and practices, and provide guidance on, the principles introduced under the option. A Sub-option 2a was also considered to allow for the assessment of a combination of legislation establishing the free flow of data principle and the policy group and self-regulatory measures addressing data porting and security (rather than co-regulation and implementing measures on these two issues as in the main option 2). Option 3 consisted of a detailed legislative initiative, to establish, inter alia, 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).

On 28 September 2016, the Regulatory Scrutiny Board delivered its first opinion on the Impact Assessment and asked for its resubmission. This was subsequently revised and resubmitted to the Regulatory Scrutiny Board on 11 August 2016, which issued a second negative opinion on 25 August but did not ask for the Impact Assessment to be further revised and resubmitted.

¹³ SMART 2015/0054, TimeLex, Spark and Tech4i, "Cross-border Data Flow in the Digital Single Market: Study on Data Location Restrictions", D5. Final Report (Ongoing) [TimeLex Study (SMART 2015/0054)]; SMART 2015/0016, London Economics Europe, Carsa and CharlesRussellSpeechlys, "Facilitating cross-border data flow in the Digital Single Market", 2016 (Ongoing) [LE Europe Study (SMART 2015/0016)]

¹⁴ SMART 2016/0032, IDC and Arthur's Legal, "Switching between Cloud Service Providers", 2017 (Ongoing) [IDC and Arthur's Legal Study (SMART 2016/0032)]

¹⁵ SMART 2016/0029 (Ongoing), Tecnia, "Certification Schemes for Cloud Computing", D6.1 Inception Report

¹⁶ SMART 2014/0031, Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016 [Deloitte Study (SMART 2014/0031)]

¹⁷ 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; SMART 2011/0045, IDC, "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake" (July 2012)

¹⁸ 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)]

¹⁹ SMART 2015/0018, TimeLex, Spark, "Clarification of Applicable Legal Framework for Full, Co- or Self-Regulatory Actions in the Cloud Computing Sector" (Ongoing).

Against this background, the Commission has considered it opportune to go ahead with a revised proposal for a framework for the free flow of data in the European Union while taking into due account the reservation expressed by the Regulatory Scrutiny Board in its second opinion. In particular, this has led to a reconsideration of the selected option as regards data porting. The preferred option initially put forward in the Impact Assessment to have an obligation for providers to facilitate the switching or porting of users' data has been abandoned. The Commission has opted instead for a more proportionate and less burdensome option, in order not to put excessive requirements on service providers and not to distort the competitive and innovative nature of their market. The proposal is less stringent and more proportionate as it does not create a new right of cloud services portability and relies on self-regulation facilitated by the Commission. The proposal has also taken account of the Board's opinion in order to ensure that there is no overlap or duplication with the review of the mandate of the European Union Agency for Network and Information Security (ENISA) and the creation of a European ICT security framework. The proposal will not affect the creation of a European ICT security framework setting rules on how to organise the ICT security certification in the EU. The proposed provision is also fully compatible with the existing implementing power of the Commission under the NIS Directive and reflects that Commission may exercise this power in the context of this Regulation to the extent it considers that common EU operational or contractual requirements applicable to the security and integrity of data storage and/or further processing are needed.

- **Regulatory fitness and simplification**

The proposal applies equally to all enterprises, including micro-enterprises and SMEs. All enterprises can benefit from the mechanism addressing obstacles to data mobility. In particular, SMEs will benefit from the efficiency of the measure, as many SMEs could gain most. The free movement of data will directly cut costs for them and therefore lead to a more competitive market position. As the proposal does not entail any substantial costs for SMEs, there is no need to minimise compliance costs for micro-enterprises or SMEs.

The proposal will have positive effects on competitiveness as it will help innovation in data services and attract more users to them.

The proposal will promote cross-border and cross-sector use of data services and will promote technological innovation and the development of the data market. Therefore, the proposal will help transform our society and economy and open up new opportunities for European citizens, businesses and public administrations.

- **Fundamental rights**

The proposed Regulation also takes full account of the fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union. It 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 of data services, such as cloud services, as well as configuration of in-house IT systems.

4. BUDGETARY IMPLICATIONS

A moderate administrative burden for Member States' public authorities will emerge, caused by the allocation of human resources for structured cooperation between Member States in the 'single points of contact' group, and for complying with the notification and review process of the transparency mechanism. In total, this could lead to an average annual cost of EUR 34.539 per Member State.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

A comprehensive evaluation will take place five years after the start of application of the rules.

- **Detailed explanation of the specific provisions of the proposal**

Article 1 specifies the **objective** of the proposal. The Regulation introduces a common approach in the Union ensuring the free movement of data by laying down rules for the availability of data to competent authorities, and security of data storage and processing.

Article 2 specifies the **scope of application** of the Regulation. The Regulation applies to electronic data stored and/or further processed within the Union, and to users established in the Union. The Regulation is without prejudice to the GDPR, the ePrivacy Directive, the eCommerce Directive, and the Police Directive. Finally, the Regulation does not apply to activities which fall outside the scope of Union law.

Article 3 provides for the **definition** of the following terms: 'a competent authority', 'data storage', 'further processing', 'provider', which means a data storage and processing service provider; 'data localisation requirement', 'user' and the concept of 'professional user'.

Article 4 establishes the **principle of free movement of data** across border within the Union. This principle prohibits any restriction to the localisation of data for storage and/or further processing within the Union for reasons other than national security.

Furthermore, it imposes the obligation to **notify draft acts that would introduce new data localisation requirements** in accordance with the procedures set out in Directive (EU) 2015/1535, and to abolish existing unjustified restrictions within one year after the start of application of the Regulation. If a Member State considers that a data localisation requirement for reasons of national security should remain in force, it will have to notify the corresponding measure to the Commission, together with a justification for maintaining such requirement.

Moreover, Article 4 provides that Member States make **information on any data localisation requirements freely available via a single online information point** accessible to the public and up-to-date. Member States will inform the Commission of the location of those single information points, which will disclose such information in a central place on a Commission website.

Article 5 aims to ensure **data availability for regulatory control by competent authorities**. To this effect, users may not refuse to provide access to data to competent authorities on the basis that data is stored and/or further processed in another Member State or on the basis of contractual clauses they have entered into. Finally, without prejudice to existing mechanisms of cooperation, where a competent authority has exhausted all existing means to obtain access to the data, **that competent authority may request the assistance** of an authority in another Member State in accordance with Article 8.

Article 6 states that **service providers should provide information prior to the conclusion of a contract for data storage or processing.** Such information would include the following details: processes and location of any data back-up; available data formats and supports; required IT configuration and minimum network bandwidth; time required prior to initiating the porting process and the time during which the data will remain available for porting; and guarantees for accessing data in the case of the bankruptcy of the provider.

The Regulation provides for the **adoption of codes of conduct** detailing the conditions of data porting by market players through self-regulation. Nonetheless, if sufficient self-regulatory measures were not put in place within a reasonable period of time, it should remain possible for the Commission to establish the conditions for the porting of data in an implementing act.

Article 7 provides that, to the extent that common EU operational or contractual requirements applicable to the **security and integrity of data storage and/or further processing** are needed for the functioning of this Regulation, any necessary implementing measures for that purpose shall be adopted in accordance with Article 16(8) of Directive 2016/1148.

In order to contribute to a **smooth cooperation across Member States** on the issues addressed by this Regulation, **Article 8** requires each Member State to designate a **single contact point** responsible for coordinating the application of this Regulation in the Member State concerned as well as liaising with the contact points of other Member States and the Commission regarding the application of this Regulation/ In this latter respect, Article 8 provides for a specific procedure of assistance between competent authorities with a view to obtain access to data through the designated single point of contact.

Article 9 establishes the **EU Free Flow of Data Policy Group (FFDPG)** which shall **advise and assist the Commission** in its work to ensure a consistent application of this Regulation in Member States. It will also exchange experience and good practice and at the Commission's request, give opinions and develop guidelines.

The Group will be composed of the single points of contact referred to in Article 8 and will be chaired by a representative of the Commission.

According to **Article 10** the Commission shall be assisted by the Free Flow of Data Committee within the meaning of Regulation (EU) No 182/2011.

Article 11 stipulates a review within five years after the applicability and a report thereof to be presented to the European Parliament, the Council and the European Economic and Social Committee.

Article 12 provides for the entry into force on the twentieth day following that of the Regulation's publication in the Official Journal of the European Union and for its start of application six months after the day of publication the Regulation.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article [114] thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee²⁰, Having regard to the opinion of the Committee of the Regions²¹, Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) The digitisation of the economy is accelerating. Information and Communications Technology (ICT) is no longer a specific sector but the foundation of all modern innovative economic systems. Electronic data is at the centre of these systems and can generate great value when mined, aggregated and processed or combined with services.
- (2) Data value chains are built on different data activities: data creation and collection; data aggregation and organisation; data storage and processing; data analysis, marketing and distribution; use and re-use of data. Effective and efficient functioning of data storage and processing aspects is a fundamental building block in any data value chain. However, such effective and efficient functioning and the development of the data economy in the Union are hampered by two types of obstacles to data mobility and the internal market.
- (3) Obstacles to the free movement of data storage and/or processing services and to the right of establishment of data storage and/or processing entities, undertakings or activities²² originate from requirements in Member State national laws to locate data in a specific geographical area or territory for storage and/or processing purposes. Other rules have an equivalent effect by imposing specific requirements or administrative practices which make it more difficult to store or process data outside a specific geographical area or territory within the Union, such as requirements to use technological facilities that are certified or approved within a specific Member State. Legal uncertainty as to which Member State's law applies to data, and as to the extent of legitimate and illegitimate data localisation requirements further limits the choices available to market players and to the public sector regarding the location of data storage and processing.

²⁰ OJ C [...], [...], p. [...].

²¹ OJ C [...], [...], p. [...].

²² The freedoms guaranteed by Articles 49 and 56 of the Treaty on the Functioning of the European Union (TFEU).

- (4) On the other hand, data mobility in the Union is also inhibited by private restrictions: legal, contractual and technical issues preventing users of data storage and processing services from porting, without hindrance, their data from one service provider to another or back to their own IT systems. At the same time, additional regulatory burden on service providers would risk to damage the competitive and innovative nature of the market.
- (5) For reasons of legal certainty and the need for a level playing field within the Union, a single set of rules for all market participants is a key element for the functioning of the internal market. In order to remove obstacles to trade and distortions of competition resulting from divergences between national laws and to prevent the emergence of further likely obstacles to trade and significant distortions of competition, it is therefore necessary to adopt a regulation establishing uniform rules applicable in all Member States.
- (6) This Regulation should provide a framework for the free movement of data in the Union and the foundation for developing the data economy and enhancing the competitiveness of European industry. Its objective is to create a clear, comprehensive and predictable legal framework for storage and/or processing of data in the internal market. The principle-based approach encompassing cooperation between and with Member States as well as self-regulation should ensure that the framework is, at the same time, flexible and can take into account the evolving needs of the Union, Member States and the industry. Also, in order to avoid the risk of overlaps with existing mechanisms in place (e.g. via sectoral cooperation) and hence to avoid higher burdens both for Member States and businesses this Regulation should not foresee detailed technical specifications.
- (7) This Regulation should apply to users established in the Union. It shall apply to legal or natural persons who provide data storage and/or processing services to users having their place of residence or establishment in the Union, including those who provide services in the Union from a third country without an establishment in the Union. The Regulation is without prejudice to the mechanisms ensuring access to data stored and/or processed outside of the Union, such as mutual legal assistance agreements with countries outside the Union.
- (8) The General Data Protection Regulation (GDPR)²³ provides a single set of rules for the entire Union ensuring a high level of protection for personal data. The processing of personal data by businesses and public sector entities that fall under its scope must comply with these rules. The GDPR will enable individuals to better control their personal data. At the same time, the 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.
- (9) This Regulation focuses on data flows within the Union that are not regulated by the GDPR: on the one hand, those triggered by decisions of businesses or public sector entities on the choice of a geographical location for data storage and/or processing, and, on the other hand, those triggered by the choice of a business or public sector user 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

²³

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

extent this Regulation deals with mixed data sets that also include personal data, the provisions of the GDPR have to be fully complied with in respect of the personal data part of the set.

- (10) Directive 2002/58/EC²⁴ (ePrivacy Directive) lays down rules regarding the protection of fundamental rights and freedoms in the context of electronic communications, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data. It complements the GDPR by laying down specific rules in the area of electronic communications. This Regulation focuses on aspects of data flows within the Union that are not regulated by the ePrivacy Directive, such as security, availability of data stored and/or processed. To the extent this Regulation deals with activities also covered by the ePrivacy Directive, the provisions of the latter Directive have to be fully complied with.
- (11) The Regulation applies to data storage and processing in the broadest sense, encompassing the usage of all types of IT systems, whether located on the premises of the user or outsourced to a data storage and processing service provider. It also covers data processing of different levels of intensity, from data 'storage' (Infrastructure-as-a-Service (IaaS)) to the processing of data on platforms (Platform-as-a-Service (PaaS)) or in applications (Software-as-a-Service (SaaS)).
- (12) Data localisation requirements and measures having an equivalent effect represent a clear barrier to the free provision of data storage and processing services across the Union and to the internal market. As such, they should be banned unless they are justified based on the grounds of public security, as defined by Union law and interpreted by the Court of Justice of the European Union, and satisfy the criteria of necessity and proportionality as enshrined in Art. 5 TEU. In order to give effect to the principle of free flow of data across borders, to ensure the swift removal of existing data localisation requirements and to enable for operational reasons storage and processing of data in multiple locations across the EU and since this Regulation provides for measures to ensure data security and data availability for regulatory control purposes, Member States should not be able to invoke justifications other than public security.
- (13) In order to ensure the effective application of the principle of free flow of data across borders, and to prevent the emergence of new barriers to the smooth functioning of the internal market, Member States should notify to the Commission any draft act that contains a new data localisation requirement or modifies an existing data localisation requirement. These notifications should be submitted and assessed in accordance with Directive 2015/1535²⁵.
- (14) Moreover, in order to eliminate potential existing barriers, during a transitional period of 12 months, Member States should carry out a review of existing national data localisation requirements and notify to the Commission, together with a justification, any data localisation requirement that they consider being in compliance with this Regulation and therefore remaining in force. In order to enable the Commission to

²⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

²⁵ 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 (OJ L 241, 17.9.2015, p. 1).

assess the compliance of any remaining data localisation requirements Member States should notify those remaining national data localisation requirements to the Commission.

- (15) In order to ensure the transparency of data localisation requirements in the Member States for natural and legal persons, such as providers and users of data storage and processing services, Member States should publish in an aggregated form on a central website and regularly update the information on such measures. In order to appropriately inform legal and natural persons of data localisation requirements across the Union, Member States should notify to the Commission the address of such websites. The Commission should publish this information on its own website.
- (16) Data localisation requirements are frequently underpinned by a lack of trust in cross-border data storage and processing, deriving from the presumed unavailability of data for the purposes of the competent authorities of the Member States, such as for inspection and audit for regulatory or supervisory control. To realise the full potential of the data economy, this Regulation should clearly establish that it does not prejudice the obligations of natural or legal persons who are subject to regulatory/administrative obligations to provide data to competent authorities, and that such natural or legal persons may not refuse such access on the basis that the data is stored and/or further processed in another Member State, or on the basis of their contractual relationships with data storage or processing service providers.
- (17) Natural or legal persons who are subject to regulatory/administrative obligations to provide data to competent authorities can comply with such obligations by providing and guaranteeing effective and timely electronic online access to the data to competent authorities, regardless of the Member State in the territory of which the data is stored and/or further processed. Such access may be ensured through concrete terms and conditions in contracts between the natural or legal person subject to the obligation to provide access and the data storage and processing service providers.
- (18) Where a natural or legal person subject to regulatory/administrative obligations fails to comply with its obligation to provide access to data stored and/or further processed in another Member State, the competent authority should be able to seek assistance from competent authorities in other Member States. In such cases, competent authorities should use existing cooperation instruments in Union law, depending on the subject matter in a given case, such as, in the area of criminal or civil justice or in administrative matters respectively, Directive 2014/41/EU²⁶, Regulation 1206/2001²⁷, Council Directive 2006/112/EU²⁸ and Regulation (EU) No 904/2010²⁹. This Regulation shall be without prejudice to cooperation mechanisms and instruments on mutual assistance or exchange of information in Union law, provided that existing means of cooperation have been exhausted by the requested authority, competent authorities should cooperate with each other with a view to provide access to the data sought, to the extent permitted under the powers of a requested authority, through designated single points of contact.

²⁶ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1).

²⁷ Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (OJ L 174, 27.6.2001, p. 1).

²⁸ Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax (OJ L 347, 11.12.2006, p. 1).

²⁹ Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax (OJ L268, 12.10.2010, p.1).

- (19) Cooperation between competent authorities pursuant to this Regulation should not create an undue administrative burden on a requested authority.
- (20) The ability to port data without hindrance is a key facilitator of user choice and effective competition on markets for data storage and processing services. The real or perceived difficulties to port data cross-border also undermine the confidence of professional users in taking up cross-border offers and hence their confidence in the internal market. Whereas natural persons and consumers benefit from existing Union legislation, the ability to switch between service providers is not facilitated for users in the course of their business activities.
- (21) This Regulation is without prejudice to the portability right granted to the data subjects under the GDPR and any legislation dealing with the protection of consumers' rights.
- (22) In order to take full advantage of the competitive environment, professional users should be able to make informed choices and easily compare the individual components of various data storage and processing services offered in the internal market, including as to the contractual conditions of porting data upon the termination of a contract. The users and the service providers should therefore aim at explaining in a sufficiently detailed, clear and transparent manner, prior to the conclusion of the contract, the porting processes, any technical requirements for porting data (e.g. required IT configuration and minimum network bandwidth, available data formats and support), the timeframes (the time required prior to initiating the porting process and the time during which the data will remain available for porting), charges that apply where the user wants to port data to another IT environment, the tasks the user should complete to retrieve and migrate data as well as what, if any, data access guarantee applies in the case of the bankruptcy of the service provider.
- (23) In order to align with the innovation potential of the market and to take into account the experience and expertise of the providers and users of data storage and processing services, the detailed conditions of data porting should be defined by market players through self-regulation, facilitated by the Commission, in the form of Union codes of conduct.
- (24) A number of security certification schemes for ICT products exist in the Union, but they are each effective only in a few Member States. Such certification schemes aims at demonstrating whether specific security requirements relating to a product or a service are fulfilled. However, an ICT service provider may need to undergo several certification processes in order to provide reassurance on its service in different Member States. Moreover, the different certification schemes that exist in the market are difficult to compare.
- (25) In the context of review of the mandate and tasks of the European Union Agency for Network and Information Security (ENISA), taking in particular into consideration its new role under the Directive 2016/1148, the Commission is considering the creation of a European ICT security framework setting rules on how to organise ICT security certification in the EU could both preserve trust in the internet and tackle the current fragmentation of the cybersecurity market without defining specific security requirements. The GDPR also encourages the establishment of data protection certification mechanisms for the purpose of demonstrating compliance of data processing operations by controllers and processors.
- (26) In order to enhance trust in and the security of cross-border data storage and processing and to reduce fragmentation of the single market, while at the same time

reducing the propensity of market players and the public sector to use data localisation as a proxy for data security, it is necessary to envisage the identification and establishment of common EU requirements applicable to the integrity and security of data storage and/or further processing services.

- (27) One should recall that Directive 2016/1148³⁰ provides for legal measures to boost the overall level of cybersecurity in the Union. Data storage and processing services constitute one of the digital services covered by the Directive. According to its Article 16, Member States have to ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use, which are to be specified in implementing acts; take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems and notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service
- (28) Directive 2016/1148 provides for implementing acts to specify the security measures that digital service providers, including data storage and processing service providers, should take. In accordance with Article 16 of Directive 2016/1148, those requirements should, having regard to the state of the art, ensure a level of security appropriate to the risk presented, and should take into account the security of systems and facilities, incident handling, business continuity management, monitoring, auditing and testing, and compliance with international standards. Any common EU operational or contractual requirements applicable to the security and integrity of data storage and/or further processing which may be needed for the functioning of this Regulation should be adopted through such implementing acts.
- (29) In order to contribute to a smooth cooperation across Member States on the issues addressed by this Regulation, each Member State should designate a single point of contact with a view to liaise with the contact points of the other Member States and the Commission regarding the application of this Regulation, in particular as regards the measures provided in Article 4 and Article 5. Member States should notify the designated single points of contact to the Commission. Those single points of contact should have the adequate resources necessary for the application of this Regulation.
- (30) The single point of contact designated by the Member State whose assistance is requested should facilitate the assistance between authorities by identifying and directing the request to the relevant competent authority in the requested Member State.
- (31) In order for cooperation between Member State authorities to be effective, the requested authority to which a request is directed should provide assistance in response to a given request without undue delay and the authority or should promptly provide information on difficulties in meeting a request or on its grounds of refusing a request of assistance.
- (32) In order to facilitate the application of this Regulation and to build trust for data flows between users, service providers and competent authorities, and EU Free Flow of Data Policy Group should be established. At the request of the Commission, the Data Policy group shall advise and assist the Commission, in its work to ensure a consistent

³⁰Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

application of the Regulation. The Data Policy Group should allow the representatives of the Member States *inter alia* to exchange experience and good practices regarding the application of this Regulation and to give opinions, at the Commission's request, on the removal of data localisation requirements, on the cooperation of competent authorities in relation to data availability for regulatory control purposes, and on model contracts or guidelines concerning availability of data when stored and/or further processed in different Member States.

- (33) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers.
- (34) The Commission should periodically review this Regulation, in particular with a view to determining the need for modifications in the light of technology or market developments.
- (35) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, in particular the right to the protection of personal data (Article 8), the freedom to conduct a business (Article 16) and the right to consumer protection (Article 38). Therefore, this Regulation should be interpreted and applied in accordance with those rights and principles.
- (36) Since the objective of this Regulation, namely to ensure the free movement of data in the Union, cannot be sufficiently achieved by the Member States, but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

HAVE ADOPTED THIS REGULATION:

Article 1
Subject matter

This Regulation introduces a common approach in the Union ensuring the free movement of data by laying down rules for data localisation requirements, the availability of data to competent authorities, contractual transparency for data porting and security of data storage and processing.

Article 2
Scope

- 1. This Regulation applies to the electronic data stored and/or further processed within the Union.
- 2. This Regulation applies to users established in the Union.
- 3. This Regulation is without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC [ePrivacy Directive], Directive (EU) 2016/680 [Police Directive] and to Directive

2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

4. This Regulation also applies to data localisation requirements imposed by Member States based on reasons other than the protection of personal data³¹.

5. To the extent this Regulation deals with data sets that may include personal data, the applicable provisions of the Regulation (EU) 2016/679 (in particular, Article 20) have to be fully complied with respect to the personal data part of the data set.

6. This Regulation does not apply to an activity which falls outside the scope of Union law;

Article 3 Definitions

For the purposes of this Regulation, the following definitions shall apply:

1. 'data storage' means any storage of information in electronic format;
2. 'further processing' means any operation or set of operations which is performed on data stored or on sets of data stored, whether or not by automated means, such as collection, recording, organisation, structuring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. 'provider' means a data storage and processing service provider;
4. 'data localisation requirement' means any specifications and other requirements or rules, including the relevant administrative provisions, the observance of which is compulsory, de jure or de facto, imposing a specific location of data for the provision of services of storage and/or further processing in the territory of a specific Member State, or prohibiting storage and/or further processing of data in any other Member State;
5. 'competent authority' means an authority of a Member State that has the power to obtain access to data stored and/or further processed by a natural or legal person, as provided by national or Union law;
6. 'user' means a natural or legal person using or requesting a data storage and/or processing service.

Article 4 Free movement of data across borders within the Union

1. Location of data for storage and/or further processing within the Union shall not be restricted to the territory of a specific Member State, and storage and/or further processing in any other Member State shall not be prohibited, unless a measure restricting the location of the data to the territory of a specific Member State or a measure prohibiting the storage and/or further processing in any other Member State such restriction or prohibition (hereinafter a 'data localisation requirement' is justified on grounds of public security.

2. Member States shall notify to the Commission any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement in

³¹ Regulation (EU) 2016/679 prohibits restrictions on the free movement of personal data within the Union where these are based on grounds connected with the protection of personal data.

accordance with the procedures set out in the provisions of national law implementing Directive (EU) 2015/1535³².

3. Within 12 months after of the start of application of this Regulation, Member States shall ensure that any data localisation requirement that is contrary to paragraph 1 is repealed. If a Member State considers that a data localisation requirement is in compliance with paragraph 1 and should remain in force, it shall notify the corresponding measure to the Commission, together with a justification for maintaining such requirement.

4. Member States shall make information on any data localisation requirements applicable in their territory freely available via a single online information point which is accessible to the public and shall keep such information up-to-date.

5. Member States shall inform the Commission of the location of single information point. The Commission shall collect and disclose information on the location of such points in a central place on a Commission website.

Article 5

Data availability for regulatory control by competent authorities.

1. This Regulation shall not affect the powers of competent authorities to request and receive data from natural or legal persons in accordance with Union or national law. To this effect users:

a) shall not refuse to provide access to data to competent authorities on the basis that data is stored and/or further processed in another Member State; and

b) shall not invoke contractual clauses they have entered into with a service provider or technical reasons to deny such access to competent authorities.

2. Without prejudice to existing mechanisms of cooperation or mutual assistance and/or exchange of information in Union law between competent authorities of different Member States, where a competent authority has exhausted all applicable means to obtain access to the data, it may request the assistance of an authority in another Member State in accordance with Article 8, through the latter Member State's single point of contact.

3. A requested authority shall provide assistance in a timely manner, to the extent permitted under its powers under Union law or national law and provided that the request for data made by the requesting competent authority does not impose an undue administrative burden on that requested authority.

Article 6

Porting of data

1. Providers should inform professional users in a sufficiently detailed, clear and transparent manner and before a contract for data storage and processing is concluded, about the processes, technical requirements, timeframes and charges that apply in case a user wants to switch to another provider or port data back to its own IT systems. Such information shall include at least the following details:

(a) processes and location of any data back-up;

³² 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 (OJ L 241, 17.9.2015, p. 1).

- (b) available data formats and supports;
- (c) required IT configuration and minimum network bandwidth;
- (d) time required prior to initiating the porting process and the time during which the data will remain available for porting; and
- (e) guarantees for accessing data in the case of the bankruptcy of the provider.

2. The Commission shall encourage and facilitate the development of self-regulatory Union codes of conduct at the latest two years after the date of entry into force of this Regulation in order to define guidelines on best practices in facilitating switching of Providers regarding:

- (a) the information to be provided pursuant to paragraph 1; and
- (b) the operational requirements to switch or port data in a structured, commonly used and machine-readable format allowing sufficient time for the user to switch or port the data.

3. The Commission shall periodically review the development and effective adoption of such codes of conduct by Providers. The Commission may decide to adopt new measures in an implementing act if it considers that the such codes would prove to be insufficient in view of making the information set out in paragraph 1 available to users.

Article 7

Security of data storage and/or further processing

To the extent that common EU operational or contractual requirements applicable to the security and integrity of data storage and/or further processing are required for the functioning of this Regulation, any necessary implementing measures for that purpose shall be adopted in accordance with Article 16(8) of Directive 2016/1148.

Article 8

Single points of contact

1. Each Member State shall designate a single point of contact who shall liaise with the contact points of other Member States and the Commission regarding the application of this Regulation.

2. Member States shall ensure that the single points of contact have the adequate resources necessary for the application of this Regulation.

3. Member States shall notify to the Commission the designated single points of contact and any subsequent change thereto.

Where a competent authority in one Member State requests assistance of another Member State to have access to data through the latter's designated single point of contact under Article 5 paragraph 3, it shall direct a duly motivated request to the designated single point of contact [including a written explanation of its justification and legal bases for seeking access to data].

The single point of contact shall then direct the request to a relevant authority of its Member State. The authority so requested shall then respond to the request without undue delay or promptly inform the single point of contact and the requesting competent authority of difficulties or of the grounds for refusing a request of assistance.

The requested authority can decide on the most appropriate measures to be taken in each individual case in order to meet the request by another Member State's competent authority.

Any information exchanged in the context of assistance requested and provided under Article 5 paragraph 3 and this Article 8 shall be used only in respect of the matter for which it was requested.

Any further procedural rules on requests of assistance for access to data and the provision of assistance may adopted in accordance with the procedure provided for in Article 10.

Article 9

The EU Free Flow of Data Policy Group

1. The EU Free Flow of Data Policy Group (Data Policy Group) is hereby established.
2. It shall be composed of the single points of contact referred to in Article 8. A representative of the Commission shall chair the group. The Commission shall provide secretarial support.
3. The Data Policy Group shall have the following tasks:
 - (a) to advise and assist the Commission, at its request, in its work to ensure a consistent application of this Regulation in all Member States;
 - (b) to exchange experience and good practice regarding the application of this Regulation and, specifically, the cooperation of competent authorities for the purpose of ensuring data availability for regulatory control purposes, as well as the removal of data localisation requirements in accordance with the principle of free movement of data;
 - (c) at the Commission's request, give opinions on, and develop model contracts or guidelines concerning availability of data stored and/or further processed in other Member States for regulatory control purposes.

Article 10

Committee

1. The Commission shall be assisted by the Free Flow of Data Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 11

Review and evaluation

1. No later than [5 years after the date mentioned in Article X (2)], the Commission shall carry out an evaluation of this Regulation and present a Report on the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall be conducted according to the Commission's Better Regulation Guidelines.
2. The Commission shall forward the evaluation report together with its conclusions to the European Parliament, to the Council and the European Economic and Social Committee. The findings of the evaluation shall be made public.
3. Member States shall provide the Commission with the information necessary for the preparation of this Report.

Article 12
Final provisions

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall apply six months after its publication.

This Regulation shall be binding in its entirety and directly applicable in all Member States.
Done at Brussels,

For the European Parliament
The President

For the Council
The President