EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 495 final

2017/0228 (COD)

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

{SWD(2017) 304 final}
{SWD(2017) 305 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

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 learning[1].

As indicated in the 2017 Communication "Building a European Data Economy"[2], 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 2020[3].

To unlock this potential, the proposal aims to address the following issues:

- Improving the mobility of non-personal 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 the powers of competent authorities to request and receive access to data for regulatory control purposes, such as for inspection and audit, remain unaffected; and
- Making it easier for professional users of data storage or other processing services to switch service providers and to port data, while not creating an excessive burden on service providers or distorting the market.

The Mid-Term Review on the implementation of the Digital Single Market Strategy (DSM Strategy)[4] announced a legislative proposal on a EU free flow of data cooperation framework.

The general policy objective of the initiative is to achieve a more competitive and integrated internal market for data storage and other processing services and activities by addressing the above areas. In this proposal, data storage and other processing is used 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 or other processing service provider[5].

• Consistency with existing policy provisions in the policy area

The proposal pursues the objectives set out in the DSM Strategy[6], 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"[7].

---

1 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.

2 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.

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

4 Commission Communication adopted on 10 May 2017 (COM(2017) 228 final).

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

6 COM/2015/0192 final.

7 Opening Statement in the European Parliament Plenary Session, Strasbourg, 22 October 2014.

This proposal focuses on provision of data hosting (storage) and other processing services, and is coherent **with existing legal instruments**. The initiative pursues the creation of an effective EU single market for such services. It is thus consistent with the **E-commerce Directive**[8] which aims at a comprehensive and effective EU single market for the broader categories of information society services, and with the Services Directive[9] which furthers the deepening of the EU single market for services in a number of sectors.

A number of relevant sectors are expressly excluded from the ambit of application of such legislation (i.e. E-commerce and Services Directives), so that only the general provisions of the Treaty would be applicable to the totality of data hosting (storage) and other processing services. However, the existing barriers to these services cannot be effectively removed solely by relying on direct application of Articles 49 and 56 of the Treaty on the Functioning of the European Union (TFEU), since, on the one hand, addressing them on a case-by-case basis through infringement procedures against the Member States concerned would be extremely complicated for national and Union institutions, and, on the other hand, the lifting of many barriers requires specific rules tackling not only public but also private barriers and calls for the setting up of administrative cooperation. Moreover, the ensuing enhancement of legal certainty seems to be particularly important for users of new technologies[10].

Since this proposal concerns electronic data other than personal data, it does not affect the Union data protection legal framework, in particular Regulation 2016/679 (GDPR)[11], Directive 2016/680 (Police Directive)[12] and Directive 2002/58/EC (ePrivacy Directive)[13], which ensure a high level of protection for personal data and the free movement of personal data within the Union. Together with that legal framework, the proposal aims to put in place a comprehensive and coherent EU framework enabling free movement of data in the single market.

The proposal will require the notification of draft measures on data localisation under the Transparency Directive 2015/1535[14] for enabling the assessment whether such localisation restrictions are justified.

Regarding cooperation and mutual assistance between competent authorities, the proposal foresees that all such mechanisms should apply. Where no cooperation mechanisms exist, the

---

8 Directive (EC) 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

9 Directive (EC) 2006/123 of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36).

10 LE Europe Study (SMART 2015/0016) and IDC Study (SMART 2013/0063).

11 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).

12 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

13 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).

14 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).

proposal introduces measures aimed at enabling competent authorities to exchange and access data stored or otherwise processed in other Member States.

- **Consistency with other Union policies**

In light of the DSM, this initiative intends to reduce barriers to a competitive data-driven economy in Europe. In line with the DSM mid-term Review Communication, the Commission is exploring separately the 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[15].

The policy intervention also builds upon the **Digitising European Industry** (DEI) policy package that included the **European Cloud initiative**[16] 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 Framework**[17], 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**[18].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

This proposal falls within the area of shared competence in accordance with Article 4(2)(a) TFEU. It aims to achieve a more competitive and integrated internal market for data storage and other processing services by ensuring the free movement of data within the Union. It lays down rules relating to data localisation requirements, the availability of data to competent authorities and data porting for professional users. The proposal is based on Article 114 TFEU which is the general legal basis for the adoption of such rules.

- **Subsidiarity**

The proposal complies with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). The objective of this proposal to ensure the smooth functioning of the internal market for the abovementioned services which is not limited to the territory of one Member State and the free movement of non-personal 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 location restrictions, but are likely to do so to different extents, and under different conditions, 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 small and medium-sized enterprises (SMEs).

---

15 COM(2017) 228 final.

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

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

18 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

- **Proportionality**

The proposal complies with the principle of proportionality as set out in Article 5 TEU, as it consists of an effective framework that does not go beyond what is necessary to solve the identified problems and is proportionate to achieve its objectives.

In order to remove obstacles to the free flow of non-personal data within the Union limited by localisation requirements and enhance trust in cross-border data flows as well as data storage and other processing services, the proposal will rely to a high degree on existing EU instruments and frameworks: the Transparency Directive for notifications of draft measures on data localisation requirements, different frameworks ensuring data availability for regulatory control by Member States. It is only in the absence of other cooperation mechanisms, and when other means of access have been exhausted, that the cooperation mechanism of the proposal will be used to address issues of data availability for national competent authorities.

The proposed approach to movement of data across Member States' borders and across service providers / in-house IT systems seeks a balance between EU regulation and public security interests of Member States as well as a balance between EU regulation and self-regulation by the market.

Specifically, in order to alleviate the difficulties of professional users to switch service providers and port data, the initiative encourages self-regulation by codes of conduct on information to be provided to users of data storage or other processing services. Also, the modalities of switching and porting should be addressed through self-regulation to define best practices.

The proposal recalls that security requirements imposed by national and Union law should also be ensured when natural or legal persons outsource their data storage or other processing services, including in another Member State. It also recalls the implementing powers conferred upon the Commission by the Network and Information Security Directive in order to address security requirements which also contribute to the functioning of this Regulation. Finally, 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 hence avoid unnecessary administrative burden.

By establishing a clear framework accompanied by cooperation between and with Member States, as well as by self-regulation, this proposal aims to enhance legal certainty and increase trust levels, while staying relevant and effective in the long term because of the flexibility of the cooperation framework, based on the single points of contact in Member States.

The Commission intends to set up an expert group to advise it on matters covered by this Regulation.

- **Choice of the instrument**

The Commission puts forward a proposal for a Regulation which can ensure that uniform rules for the free flow of non-personal data are applicable throughout the Union at the same time. This is particularly important to remove existing restrictions and prevent new ones to be enacted by Member States, to guarantee the legal certainty to the concerned service providers and users and thereby increase trust in cross-border data flows as well as data storage and other processing services.

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

- **Stakeholder consultations**

During a **first round of evidence gathering,** a **public consultation** on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy was carried out in 2015. Two thirds of respondents – with an even distribution across all stakeholder groups, including SMEs – found that restrictions on the localisation of data have affected their business strategy.[19] Other information gathering activities consisted of meetings and events, targeted workshops with key stakeholders (e.g. the Cloud Select Industry Group) and dedicated workshops in the context of studies.

A **second round of evidence gathering,** from end 2016 until the second half of 2017, included 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, 61.9% of stakeholders believed that data localisation restrictions should be removed. 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[20]. IT service providers of all sizes, established both within and outside the EU, show the highest support for regulatory action. Stakeholders also identified negative impacts of data localisation restrictions. Next to increased costs for business, these are on the provision of a service to private or public entities (69.6% of all participating 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'). Stakeholders from all different backgrounds respond to these questions in similar percentages. The public online consultation also showed that the problem with switching providers is widespread, as 56.8% of SME respondents indicated that they experienced difficulties when intending to switch.

The structured dialogue meetings with Member States facilitated a common understanding of the challenges. 16 Member States have explicitly called for a legislative proposal in a letter addressed to President Tusk.

The proposal takes on board a number of concerns signalled by Member States and industry, in particular, the need for a cross-cutting free movement of data principle providing for legal certainty; making progress on data availability for regulatory purposes; making it easier for professional users to switch data storage or other processing service providers and port data by encouraging more transparency on the applicable procedures and conditions in contracts, but not imposing specific standards or obligations on service providers at this stage.

- **Collection and use of expertise**

Legal and economic studies have been relied on for various aspects of data mobility, including data localisation requirements[21], switching providers / data porting[22] and data

19 Additional economic evidence was sought via a study on the economic impact of cloud computing in Europe (SMART 2014/0031, Deloitte, "Measuring the economic impact of cloud computing in Europe", 2016).

20 289 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.

21 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

security[23]. Further studies have been commissioned on the impacts of cloud computing[24] and cloud uptake[25], as well as on the European data market[26]. Studies have also been carried out examining co- or self-regulatory actions in the cloud computing sector[27]. 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. The following set of options was considered in the impact assessment: a baseline scenario (no policy intervention) and three policy options. Option 1 consisted of guidelines and/or self-regulation to address the different identified problems 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 legal principles concerning the different identified problems and would envisage the designation by Member States of single points of contact and creation of an expert group, to discuss 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 framework and the single points of contact and an expert group as well as self-regulatory measures addressing data porting. 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 and a new data porting right.

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 2017. In its second opinion, the Regulatory Scrutiny Board noted the widening of the scope, following the Commission Communication (2017)9 on Building a European Data Economy, as well as the additional material on stakeholder views and on the shortcomings of the current framework. The Board, however, issued a second negative opinion on 25 August 2017, noting in particular lacking evidence in support of a new right to cloud services portability. In line with its operational practices, the Board considered its opinion as final.

The Commission considered it opportune to table a proposal while further improving its impact assessment analysis to take due account of the comments expressed by the Regulatory Scrutiny Board in its second opinion. The scope of the proposal is limited to the free flow of non-personal data in the European Union. In line with the Board's finding that the evidence

---

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)].

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

[23] SMART 2016/0029 (Ongoing), Tecnalia, "Certification Schemes for Cloud Computing", D6.1 Inception Report.

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

[25] 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).

[26] 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)].

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

seems to point towards a less stringent 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. Instead, the Commission retained a less burdensome option, consisting in self-regulatory measures facilitated by the Commission. The proposal is proportionate and less stringent as it does not create a new right of porting between data storage or other processing service providers but relies on self-regulation for transparency on the technical and operational conditions relating to portability.

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 cybersecurity framework.

The impact assessment showed that the preferred option, sub-option 2a, would ensure the effective removal of existing unjustified localisation restrictions and would effectively prevent the future ones, as a result of a clear legal principle combined with the review, notification and transparency, while at the same time enhancing legal certainty and trust in the market. The burden on Member States' public authorities would be modest, leading to approximately EUR 33.000 annually in terms of human resources cost to sustain the single points of contact as well as a yearly cost of between EUR 385 and EUR 1925 for the preparation of notifications.

The proposal will have a positive effect on competition as it will stimulate innovation in data storage or other processing services, attract more users to them and make it considerably easier, particularly for new and small service providers, to enter new markets. The proposal will also promote cross-border and cross-sector use of data storage or other processing services and the development of the data market. Therefore, the proposal will help transform the society and economy and open up new opportunities for European citizens, businesses and public administrations.

- **Regulatory fitness and simplification**

The proposal applies to citizens, national administrations and to all enterprises, including micro-enterprises and SMEs. All enterprises can benefit from the provisions addressing obstacles to data mobility. In particular, SMEs will benefit from the proposal, as free movement of non-personal data will directly reduce their costs and favour a more competitive market position. Exempting SMEs from the rules would undermine their effectiveness, as SMEs represent an important part of the providers of data storage or other processing and drivers of innovation in those markets. Since, in addition, costs resulting from the rules are not likely to be substantial, micro-enterprises or SMEs should not be excluded from their scope of application.

- **Fundamental rights**

The proposed Regulation respects fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union. The proposed Regulation should positively impact on the freedom to conduct a business (Article 16) as it 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 the cooperation between Member States through the 'single points of contact', and for complying with the notification, review and transparency provisions.

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 with a view to assessing their effectiveness and proportionality. This evaluation will be conducted in line with the Better Regulation Guidelines.

It will notably need to examine whether the Regulation contributed to reducing the number and range of data localisation restrictions and to enhancing legal certainty and transparency of remaining (justified and proportionate) requirements. The evaluation will also have to assess whether the policy initiative has contributed to improving the trust in free flow of non-personal data, whether the Member States can reasonably have access to data stored abroad for regulatory control purposes and whether the Regulation has led to the improvement of transparency on conditions for data porting.

It is planned that the single points of contact of the Member States should serve as a valuable source of information during the ex-post evaluation phase of the legislation.

Specific indicators (as proposed in the impact assessment) would serve to measure progress in those areas. It is also planned to use Eurostat data and the Digital Economy and Society Index. A special edition of Eurobarometer may also be considered for this purpose.

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

Articles 1 to 3 specify the **objective** of the proposal, the **scope of application** of the Regulation and the **definitions** applicable for the purposes of the Regulation.

Article 4 establishes the **principle of free movement of non-personal data** in the Union. This principle prohibits any data localisation requirement, unless it is justified on grounds of public security. Furthermore, it provides for the review of existing requirements, notification of remaining or new requirements to the Commission and transparency measures.

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 or otherwise processed in another Member State. Where a competent authority has exhausted all applicable means to obtain access to the data, **that competent authority may request the assistance** of an authority in another Member State, if no specific cooperation mechanism exists.

Article 6 states that the Commission shall encourage **service providers and professional users to develop and implement codes of conduct** detailing the information on data porting conditions (including technical and operational requirements) that providers should make available to their professional users in a sufficiently detailed, clear and transparent manner before a contract is concluded. The Commission will review the development and effective implementation of such codes within two years after the start of application of this Regulation.

Pursuant to **Article 7**, each Member State shall designate a **single point of contact** who shall liaise with the points of contact of other Member States and the Commission regarding the

application of this Regulation. Article 7 also provides for procedural conditions applicable to the assistance between competent authorities envisaged under Article 5.

According to **Article 8** the Commission shall be assisted by the Free Flow of Data Committee within the meaning of Regulation (EU) No 182/2011.

Article 9 stipulates a **review** within five years after the start of application of the Regulation.

Article 10 provides that the Regulation will start to apply six months after the day of its publication.

2017/0228 (COD)

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

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 Committee[28],

Having regard to the opinion of the Committee of the Regions[29],

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 and societies. Electronic data is at the centre of those systems and can generate great value when analysed or combined with services and products.

(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. The effective and efficient functioning of data storage and other processing 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, in particular, by two types of obstacles to data mobility and to the internal market.

(3) The freedom of establishment and the freedom to provide services under the Treaty on the Functioning of the European Union apply to data storage or other processing services. However, the provision of those services is hampered or sometimes prevented by certain national requirements to locate data in a specific territory.

(4) Such obstacles to the free movement of data storage or other processing services and to the right of establishment of data storage or other processing providers originate from requirements in the national laws of Member States to locate data in a specific geographical area or territory for the purpose of storage or other processing. Other rules or administrative practices have an equivalent effect by imposing specific requirements which make it more difficult to store or otherwise process data outside a specific geographical area or territory within the Union, such as requirements to use

[28] OJ C , , p. .
[29] OJ C , , p. .

technological facilities that are certified or approved within a specific Member State. Legal uncertainty 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 or other processing.

(5) At the same time, data mobility in the Union is also inhibited by private restrictions: legal, contractual and technical issues hindering or preventing users of data storage or other processing services from porting their data from one service provider to another or back to their own IT systems, not least upon termination of their contract with a service provider.

(6) 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 uniform rules applicable in all Member States.

(7) In order to create a framework for the free movement of non-personal data in the Union and the foundation for developing the data economy and enhancing the competitiveness of European industry, it is necessary to lay down a clear, comprehensive and predictable legal framework for storage or other processing of data other than personal data in the internal market. A principle-based approach providing for cooperation among Member States as well as self-regulation should ensure that the framework is flexible so that it can take into account the evolving needs of users, providers and national authorities in the Union. In order to avoid the risk of overlaps with existing mechanisms and hence to avoid higher burdens both for Member States and businesses, detailed technical rules should not be established.

(8) This Regulation should apply to legal or natural persons who provide data storage or other processing services to users residing or having an establishment in the Union, including those who provide services in the Union without an establishment in the Union.

(9) The legal framework on the protection of natural persons with regard to the processing of personal data, in particular Regulation (EU) 2016/679[30], Directive (EU) 2016/680[31] and Directive 2002/58/EC[32] should not be affected by this Regulation.

(10) Under Regulation (EU) 2016/679, Member States may neither restrict nor prohibit the free movement of personal data within the Union for reasons connected with the protection of natural persons with regard to the processing of personal data. This Regulation establishes the same principle of free movement within the Union for non-

---

30 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).

31 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

32 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).

personal data except when a restriction or a prohibition would be justified for security reasons.

(11) This Regulation should apply to data storage or other 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 or other processing service provider. It should cover 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)). These different services should be within the scope of this Regulation, unless data storage or other processing is merely ancillary to a service of a different type, such as providing an online marketplace intermediating between service providers and consumers or business users.

(12) Data localisation requirements represent a clear barrier to the free provision of data storage or other 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, in particular Article 52 of the Treaty on the Functioning of the European Union, and satisfy the principle of proportionality enshrined in Article 5 of the Treaty on European Union. In order to give effect to the principle of free flow of non-personal data across borders, to ensure the swift removal of existing data localisation requirements and to enable for operational reasons storage or other processing of data in multiple locations across the EU, and since this Regulation provides for measures to ensure 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 non-personal 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. Those notifications should be submitted and assessed in accordance with the procedure laid down in Directive (EU) 2015/1535[33].

(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. These notifications should enable the Commission to assess the compliance of any remaining data localisation requirements.

(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 or other processing services, Member States should publish on a single online information point 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 addresses of such online points. The Commission should publish this information on its own website.

[33] 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).

(16) Data localisation requirements are frequently underpinned by a lack of trust in cross-border data storage or other 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. Therefore, this Regulation should clearly establish that it does not affect the powers of competent authorities to request and receive access to data in accordance with Union or national law, and that access to data by competent authorities may not be refused on the basis that the data is stored or otherwise processed in another Member State.

(17) Natural or legal persons who are subject to obligations to provide data to competent authorities can comply with such obligations by providing and guaranteeing effective and timely electronic access to the data to competent authorities, regardless of the Member State in the territory of which the data is stored or otherwise 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 or other processing service provider.

(18) Where a natural or legal person subject to obligations to provide data fails to comply with them and provided that a competent authority has exhausted all applicable means to obtain access to data, the competent authority should be able to seek assistance from competent authorities in other Member States. In such cases, competent authorities should use specific cooperation instruments in Union law or international agreements, depending on the subject matter in a given case, such as, in the area of police cooperation, criminal or civil justice or in administrative matters respectively, Framework Decision 2006/960[34], Directive 2014/41/EU of the European Parliament and of the Council[35], the Convention on Cybercrime of the Council of Europe[36], Council Regulation (EC) No 1206/2001[37], Council Directive 2006/112/EC[38] and Council Regulation (EU) No 904/2010[39]. In the absence of such specific cooperation mechanisms, competent authorities should cooperate with each other with a view to provide access to the data sought, through designated single points of contact, unless it would be contrary to the public order of the requested Member State.

(19) Where a request for assistance entails obtaining access to any premises of a natural or legal person including to any data storage or other processing equipment and means, by the requested authority, such access must be in accordance with Union or Member State procedural law, including any requirement to obtain prior judicial authorisation.

(20) The ability to port data without hindrance is a key facilitator of user choice and effective competition on markets for data storage or other 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

---

[34] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89).

[35] 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).

[36] Convention on Cybercrime of the Council of Europe, CETS No 185.

[37] 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).

[38] 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).

[39] Council 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).

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 or professional activities.

(21) 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 or other processing services offered in the internal market, including as to the contractual conditions of porting data upon the termination of a contract. In order to align with the innovation potential of the market and to take into account the experience and expertise of the providers and professional users of data storage or other processing services, the detailed information and operational requirements for data porting should be defined by market players through self-regulation, encouraged and facilitated by the Commission, in the form of Union codes of conduct which may entail model contract terms. Nonetheless, if such codes of conduct are not put in place and effectively implemented within a reasonable period of time, the Commission should review the situation.

(22) In order to contribute to a smooth cooperation across Member States, each Member State should designate a single point of contact to liaise with the contact points of the other Member States and the Commission regarding the application of this Regulation. Where a competent authority in one Member State requests assistance of another Member State to have access to data pursuant to this Regulation, it should submit a duly motivated request to the latter's 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 designated by the Member State whose assistance is requested should facilitate the assistance between authorities by identifying and transmitting the request to the relevant competent authority in the requested Member State. In order to ensure effective cooperation, the authority to which a request is transmitted should without undue delay provide assistance in response to a given request or provide information on difficulties in meeting a request of assistance or on its grounds of refusing such request.

(23) In order to ensure the effective implementation of the procedure for assistance between Member State competent authorities, the Commission may adopt implementing acts setting out standard forms, languages of requests, time limits or other details of the procedures for requests for assistance. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[40]

(24) Enhancing trust in the security of cross-border data storage or other processing should reduce the propensity of market players and the public sector to use data localisation as a proxy for data security. It should also improve the legal certainty for companies on applicable security requirements when outsourcing their data storage or other processing activities, including to service providers in other Member States.

(25) Any security requirements related to data storage or other processing that are applied in a justified and proportionate manner on the basis of Union law or national law in compliance with Union law in the Member State of residence or establishment of the natural or legal persons whose data is concerned should continue to apply to storage or

[40] 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 (OJ L 55, 28.2.2011, p. 13).

other processing of that data in another Member State. These natural or legal persons should be able to fulfil such requirements either themselves or through contractual clauses in contracts with providers.

(26) Security requirements set at national level should be necessary and proportionate to the risks posed to the security of data storage or other processing in the area in scope of the national law in which these requirements are set.

(27) Directive 2016/1148[41] provides for legal measures to boost the overall level of cybersecurity in the Union. Data storage or other processing services constitute one of the digital services covered by that 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. Such measures should 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. These elements are to be further specified by the Commission in implementing acts under that Directive.

(28) The Commission should periodically review this Regulation, in particular with a view to determining the need for modifications in the light of technological or market developments.

(29) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, and should be interpreted and applied in accordance with those rights and principles, including the rights to the protection of personal data (Article 8), the freedom to conduct a business (Article 16), and the freedom of expression and information (Article 11).

(30) Since the objective of this Regulation, namely to ensure the free movement of non-personal 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 seeks to ensure the free movement of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and data porting for professional users.

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

Article 2
Scope

1. This Regulation shall apply to the storage or other processing of electronic data other than personal data in the Union, which is

   (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the provider is established or not in the Union or

   (b) carried out by a natural or legal person residing or having an establishment in the Union for its own needs.

2. This Regulation shall 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' means data other than personal data as referred to in Article 4(1) of Regulation (EU) 2016/679;

2. 'data storage' means any storage of data in electronic format;

3. 'draft act' means a text formulated with the aim of having it enacted as a law, regulation or administrative provision of a general nature, the text being at the stage of preparation at which substantive amendments can still be made by the notifying Member State;

4. 'provider' means a natural or legal person who provides data storage or other processing services;

5. 'data localisation requirement' means any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of the Member States, which imposes the location of data storage or other processing in the territory of a specific Member State or hinders storage or other processing of data in any other Member State;

6. 'competent authority' means an authority of a Member State that has the power to obtain access to data stored or processed by a natural or legal person for the performance of its official duties, as provided for by national or Union law;

7. 'user' means a natural or legal person using or requesting a data storage or other processing service;

8. 'professional user' means a natural or legal person, including a public sector entity, using or requesting a data storage or other processing service for purposes related to its trade, business, craft, profession or task.

Article 4
Free movement of data within the Union

1. Location of data for storage or other processing within the Union shall not be restricted to the territory of a specific Member State, and storage or other processing in any other Member State shall not be prohibited or restricted, unless it 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 accordance with the procedures set out in the national law implementing Directive (EU) 2015/1535.

3. Within 12 months after the start of application of this Regulation, Member States shall ensure that any data localisation requirement that is not in compliance with paragraph 1 is repealed. If a Member State considers that a data localisation requirement is in compliance with paragraph 1 and may therefore remain in force, it shall notify that measure to the Commission, together with a justification for maintaining it in force.

4. Member States shall make the details of any data localisation requirements applicable in their territory publicly available online via a single information point which they shall keep up-to-date.

5. Member States shall inform the Commission of the address of their single information point referred to in paragraph 4. The Commission shall publish the links to such points on its website.

Article 5
Data availability for competent authorities

1. This Regulation shall not affect the powers of competent authorities to request and receive access to data for the performance of their official duties in accordance with Union or national law. Access to data by competent authorities may not be refused on the basis that the data is stored or otherwise processed in another Member State.

2. Where a competent authority has exhausted all applicable means to obtain access to the data, it may request the assistance of a competent authority in another Member State in accordance with the procedure laid down in Article 7, and the requested competent authority shall provide assistance in accordance with the procedure laid down in Article 7, unless it would be contrary to the public order of the requested Member State.

3. Where a request for assistance entails obtaining access to any premises of a natural or legal person including to any data storage or other processing equipment and means, by the requested authority, such access must be in accordance with Union or Member State procedural law.

4. Paragraph 2 shall only apply if no specific cooperation mechanism exists under Union law or international agreements to exchange data between competent authorities of different Member States.

Article 6
Porting of data

1. The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level, in order to define guidelines on best practices in facilitating the switching of providers and to ensure that they provide professional users with sufficiently detailed, clear and transparent information before a contract for data storage and processing is concluded, as regards the following issues:

   (a) the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another provider or port data back to

its own IT systems, including the processes and location of any data back-up, the available data formats and supports, the required IT configuration and minimum network bandwidth; the time required prior to initiating the porting process and the time during which the data will remain available for porting; and the guarantees for accessing data in the case of the bankruptcy of the provider; 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.

2. The Commission shall encourage providers to effectively implement the codes of conduct referred to in paragraph 1 within one year after the start of application of this Regulation.

3. The Commission shall review the development and effective implementation of such codes of conduct and the effective provision of information by providers no later than two years after the start of application of this Regulation.

Article 7
Single points of contact

1. Each Member State shall designate a single point of contact who shall liaise with the single points of contact of other Member States and the Commission regarding the application of this Regulation. Member States shall notify to the Commission the designated single points of contact and any subsequent change thereto.

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

3. Where a competent authority in one Member State requests assistance of another Member State to have access to data pursuant to Article 5 paragraph 2, it shall submit a duly motivated request to the latter's designated single point of contact, including a written explanation of its justification and legal bases for seeking access to data.

4. The single point of contact shall identify the relevant competent authority of its Member State and transmit the request received pursuant to paragraph 3 to that competent authority. The authority so requested shall, without undue delay:

(a) respond to the requesting competent authority and notify the single point of contact of its response and

(b) inform the single point of contact and the requesting competent authority of any difficulties or, in the event the request is refused or responded to in part, of the grounds for such refusal or partial response.

5. Any information exchanged in the context of assistance requested and provided under Article 5 paragraph 2 shall be used only in respect of the matter for which it was requested.

6. The Commission may adopt implementing acts setting out standard forms, languages of requests, time limits or other details of the procedures for requests for assistance. Such implementing acts shall be adopted in accordance with the procedure referred to in Article 8.

Article 8
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 9
Review

1. No later than [5 years after the date mentioned in Article 10(2)], the Commission shall carry out a review of this Regulation and present a report on the main findings to the European Parliament, the Council and the European Economic and Social Committee.
2. Member States shall provide the Commission with the necessary information for the preparation of the report referred to in paragraph 1.

Article 10
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	*For the Council*
The President	*The President*