Council of the European Union

Brussels, 19 December 2017
(OR. en)

Interinstitutional File:
2017/0228 (COD)

15724/1/17
REV 1

LIMITE

TELECOM 359
COMPET 870
MI 957
DATAPROTECT 216
JAI 1203
CODEC 2072

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
No. prev. doc.:	15112/17 TELECOM 327 COMPET 825 MI 890 DATAPROTECT 195 JAI 1131 CODEC 1948
No. Cion doc.:	12244/17 TELECOM 213 COMPET 615 MI 637 DATAPROTECT 143 JAI 791 IA 141 CODEC 1407 + ADD 1 + ADD 2 + ADD 3
Subject:	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

INTRODUCTION

1. On 13 September 2017, the Commission adopted and transmitted to the Council and to the European Parliament the above-mentioned proposal for a regulation whose aim is to set a framework for the free flow of non-personal data[1]. This proposal is key for completing the Digital Single Market and harnessing the growth potential of the European Data Economy.

[1] The Proposal exclusively covers non-personal data to avoid overlap with the General Data Protection Regulation (2016/679/EC), which already provides for the free flow of personal data in the EU. This implies that in the case of mixed data sets, the General Data Protection Regulation will apply to the personal data part of the set, and the Proposal will apply to the non-personal data part of the set.

2. Following a consultation process with European stakeholders on the European Data Economy, structured dialogues with Member States, and various studies on data flows, localisation restrictions, data porting, and cloud services, the Commission finalised its impact assessment and initiative.

3. The impact assessment[2] analyses four different policy options. The preferred option chosen by the Commission is a principles-based legislative initiative and cooperation framework to ensure the trustworthy free flow of data across borders and facilitate switching and porting data between providers and IT systems.

4. The Commission's proposal contains 4 main elements:

- A principle for the free flow of non-personal data with clear scope and definition of data other than personal data;
- a limited exemption for cases justified on grounds of public security, with an obligation to notify these cases to the Commission;
- a provision to ensure the necessary access to data to the relevant competent authorities, accompanied by an additional cooperation mechanism; and
- a provision to encourage and facilitate the switching of providers and porting of data.

5. Political support for the principle of the Free Flow of Data is very strong: in December 2016, 16 Heads of State and Government called for this proposal; in October 2017, the European Council called for co-legislators to reach an agreement on this proposal by June 2018.

WORK WITHIN THE COUNCIL

6. The Commission presented this proposal and its impact assessment (IA) to the Working Party on Telecommunication and Information Society (hereinafter referred to as the "Working Party") on 25 September 2017, followed by an examination of the impact assessment in the Working Party on 17 October.

[2] Doc. 12244/17 ADD 1

7. Some delegations raised several points on the impact assessment, in particular: the quality of data used to build the IA, including the methodology for defining the European market for data storage; doubts about the impact of data localisation requirements on businesses; the underestimation of costs and burden of the notification or cooperation procedures; the weakness of the assessment regarding the identification of exceptions, about the lack of analysis on liability or data ownership issues, or about the link between this proposal and other Union law on free movement of personal data.

8. However, in general, delegations welcomed the proposal in the context of the Digital Single Market.

9. On 4 December 2017, Ministers in the TTE Council held a debate on the proposal. All supported the principle of free flow of data, and shared ideas in particular on the cooperation mechanism and the possible restrictions. While most supported the scope of the proposal and exceptions as proposed by the Commission, a few Ministers called for further exemptions from the scope or possibilities to justify localisation restrictions.

10. Throughout the months of October – December 2017, the Working Party examined the Commission's proposal as well as Presidency compromise proposals. Delegations provided many useful comments that allowed the Presidency to improve the scope, the definitions, the cooperation and notification mechanisms, as well as the principles of free flow of data and porting themselves and to make smaller technical improvements and clarifications.

11. The most discussed topics have been:

a) the scope exceptions (Article 2(2)) and the reasons for justified exemptions from the prohibition on localisation requirements (Article 4(1)); and

b) the need for a simple mechanism for competent authorities to access data across borders where appropriate.

12. On the basis of WP TELE of 18 December, the Presidency has amended the mandate for the COREPER meeting of 20 December. The Presidency introduces the changes to Art 2(2)(b) and Art 4(1) as a package. All further changes to the Presidency text are **bold underlined**, and all deletions compared to the previous text are in ~~**bold underline strikethrough**~~.

SCOPE – Art 2(2)(b).

The Presidency compromise text proposes a new version of Art 2(2)(b) that explicitly enables delegations to allocate and provide for the implementation of powers and responsibilities for processing among public authorities and bodies governed by public law as defined in point 4 of Article 2(1) of the Procurement Directive. Recitals 7b and 11 have been modified accordingly, with previous text from recital 11 moved to recital 7b.

As a technical change, the Presidency text deletes the word "and" and introduces the word "or" between paragraphs 2(a) and 2(b).

FREE MOVEMENT OF DATA – Art 4(1)

To achieve a balance, the Presidency text reverts to a previous version, removing exemptions for public policy and activities connected with the exercise of official authority. Recitals 12b, 12c and 12d are deleted and recital 12 modified accordingly.

OTHER CHANGES

Wording on functional requirements for access to data is moved from Recital 17 to 16.

The following changes were introduced into the text during the Working Party of 18 December:

- The compromise proposal reintroduces "professional users" to Art 6. Also, Art 6(1)(c) deletes "schemes" and introduces wording agreed in WP TELE on national and international norms.

- Recital 1 is modified by emphasising further work on liability.

- Recital 10 is updated to further clarify the relationship between this regulation and the GDPR.

CONCLUSION

13. This text constitutes a balanced compromise that gives Member States flexibility to address core public responsibilities while respecting the principle of free flow of data. The Presidency is therefore of the view that this text is a good basis for a mandate to begin negotiations with the European Parliament as soon as possible.

14. In the light of the above, the Permanent Representatives Committee is invited to examine and confirm the Presidency compromise text as set out in the Annex and to grant a negotiating mandate to begin negotiations with the European Parliament.

ANNEX

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[3],

Having regard to the opinion of the Committee of the Regions[4],

Acting in accordance with the ordinary legislative procedure,

Whereas:

[3] OJ C , , p. .
[4] OJ C , , p. .

(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. **Considering, at the same time, that the rapid development of <u>the</u> data economy and emerging technologies such as Artificial Intelligence, Internet of Things products and services, autonomous systems, and 5G raise novel legal issues surrounding questions of data ownership, liability, ethics and solidarity. <u>Furthermore, work should be considered notably in the area of liability, in particular through self-regulatory codes and other best practices, taking into account recommendations, decisions and actions taken without human interaction along the entire value chain of data processing. Such work may also consider inter alia appropriate mechanisms for determining liability, responsibility transfers among cooperating services, insurance and auditing.</u>**

(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 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.

(7a) This Regulation should not affect data ~~storage or other~~ processing in so far as it is part of an activity which falls outside the scope of Union law. In particular, in accordance with Article 4 of the Treaty on European Union, national security is the sole responsibility of each Member State.

(7b) ~~In order not to interfere with the internal administrative organisation of Member States and not to impose disproportionate communication obligations on competent authorities~~, ~~t~~This Regulation is without prejudice to the internal organisation of Member States and should therefore not apply to laws, regulations, and administrative provisions ~~of general nature~~ allocating and providing for the implementation of powers and responsibilities for processing data among public authorities and bodies governed by public law. ~~the task of processing electronic data other than personal data among public authorities. However, data localisation requirements imposed on such processing should not be excluded from the scope of this Regulation.~~ While public authorities are encouraged to consider the economic and other benefits of outsourcing to external service providers, there may be legitimate reasons to choose self-provisioning of services or insourcing within public administration. Consequently, nothing in this Regulation obliges Member States to contract out or externalise the provision of services that they wish to provide themselves or to organise by means other than public contracts.

(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. **This Regulation should therefore not apply to ~~data storage or other~~ processing taking place outside the Union and to data localisation requirements relating to such data.**

(8a) This Regulation does not lay down rules relating to the determination of applicable law in commercial matters and is therefore without prejudice to Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). In particular, to the extent that the law applicable to the contract has not been chosen in accordance with Article 3 of Regulation No 593/2008, a contract for the provision of services shall in principle be governed by the law of the country where the service provider has his habitual residence.

(9) The legal framework on the protection of natural persons with regard to the processing of personal data, in particular Regulation (EU) 2016/679[5], Directive (EU) 2016/680[6] and Directive 2002/58/EC[7] should not be affected by this Regulation.

---

5 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).

6 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).

7 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).

(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-personal data except when a restriction or a prohibition would be justified for security reasons. **The Regulation (EU) 2016/679 and this Regulation provide a coherent set of rules that cater for free movement of different types of data. In the case of mixed data sets, the Regulation (EU) 2016/679 will apply to the personal data part of the set, and this Regulation will apply to the non-personal data part of the set. Where non-personal and personal data are inextricably linked, this Regulation should not prejudice the application of Regulation (EU) 2016/679. Furthermore, this Regulation does not impose an obligation to store the different types of data separately.**

(10a) A large source of non-personal data is the expanding Internet of Things, for example as it is deployed in automated industrial production processes. Specific examples of non-personal data include aggregate and anonymized datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines.

(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)). **~~However, nothing in this Regulation obliges Member States to contract out or externalise the provision of services that they wish to provide themselves or to organise by means other than public contracts.~~ ~~this Regulation~~ ~~does not prevent~~ ~~Member State's authorities from deciding whether or not to outsource to external service providers data storage or other processing.~~** ~~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 ~~**imperative**~~ grounds of public security ~~**or public policy**~~, ~~as defined by Union law, in particular~~ **within the meaning of** 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~~**, or concern activities which are connected with the exercise of official authority within the meaning of Article 51 of the Treaty on the Functioning of the 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 ~~**imperative grounds of**~~ public security ~~**and public policy, except when the activity is connected with the exercise of official authority. It should be noted that Union law does not impose on Member States a uniform scale of values as regards the assessment of conduct which may be considered to be contrary to public security and public policy**~~.

(12a) The concept of 'public security', within the meaning of Article 52 of the TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in particular to allow for the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as by the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests.

~~**(12b) The concept of 'public policy', within the meaning of Article 52 of the TFEU and as interpreted by the Court of Justice, covers the protection against a genuine and sufficiently serious threat affecting one of the fundamental interests of society and may include, in particular, issues relating to human dignity, the protection of minors and vulnerable adults.**~~

~~**(12c) The notion of 'imperative ground' presupposes a threat to public security or policy that is of a particularly high degree of seriousness.**~~

~~**(12d) The European Court of Justice has repeatedly held that the concept of 'activities which are connected with the exercise of official authority' within the meaning of Article 51 must be restricted to activities which in themselves are directly and specifically connected with the exercise of official authority.**~~

(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~~ **immediately communicate** to the Commission any draft act that contains a new data localisation requirement or modifies an existing data localisation requirement. ~~Those notifications~~ **Those draft acts** should be submitted and assessed in accordance with ~~the procedure laid down in~~ Directive (EU) 2015/1535[8].

(14) Moreover, in order to eliminate potential existing barriers, during a transitional period of ~~12~~**24** months, Member States should carry out a review of existing ~~national~~ **laws, regulations or administrative provisions of a general nature laying down** data localisation requirements and ~~notify~~ **communicate** to the Commission, together with a justification, any **such** data localisation requirement that they consider being in compliance with this Regulation. ~~These notifications~~ **This** should enable the Commission to assess the compliance of any remaining data localisation requirements.

(14a) The obligations to communicate existing ~~measures~~ data localisation requirements and draft acts to the Commission established by this Regulation should apply to regulatory ~~measures~~ data localisation requirements and drafts of a general nature and not to decisions addressed to a specific natural or legal person.

(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 **or provide those up-to-date details to an information point established under another Union act**. 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.

---

8 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. **Such lack of trust cannot be overcome solely by the nullity of contractual terms prohibiting lawful access to data by competent authorities for the performance of their official duties.** 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. **Competent authorities could impose functional requirements to support access to data, such as requiring that system descriptions and passwords have to be kept in the Member State concerned.**

(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 **~~(such as requiring that system descriptions and passwords has to be kept in the Menber State)~~** 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[9], Directive 2014/41/EU of the European Parliament and of the Council[10], the Convention on Cybercrime of the Council of Europe[11], Council Regulation (EC) No 1206/2001[12], Council Directive 2006/112/EC[13] and Council **Regulation (EU) No 904/2010**[14]. 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.

---

9 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).

10 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).

11 Convention on Cybercrime of the Council of Europe, CETS No 185.

12 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).

13 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).

14 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).

(19a) This Regulation should not allow users to ~~wrongly~~ attempt to evade the application of national legislation. Provision should therefore be made for the imposition by Member States of effective, proportionate and dissuasive penalties on users which ~~fraudulently~~ prevent competent authorities from receiving access to their data necessary for the performance of the competent authorities' official duties under Union and national law.

(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 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. **Consistent technical requirements across the Union, whether through technical harmonisation, mutual recognition or voluntary harmonisation also contribute to developing a competitive an internal market for data processing services.**

(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, **through a designated single point of contact,** 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 **transmission of the request** ~~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.[15]~~

(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.

~~[15] 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).~~

(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 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[16] 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.

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

(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~~.~~ **and to assessing the experience gained in applying this Regulation to mixed data sets**.

(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.

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**:**

   (a) an activity which falls outside the scope of Union law**; ~~and~~ or**

   ~~(b) storage or other processing of electronic data other than personal data provided without remuneration by a public authority to another public authority.~~ ~~laws, regulations, and administrative provisions, insofar as they allocate public tasks among public authorities.~~

   (b) laws, regulations, and administrative provisions relating to the internal organisation of Member States allocating and providing for the implementation of powers and responsibilities for processing data among public authorities and bodies governed by public law as defined in point 4 of Article 2(1) of Directive 2014/24/EU.

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;~~

2a. 'processing' means any operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction ~~as referred to in Article 4(2) of Regulation (EU) 2016/679;~~

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 **or resulting from general and consistent administrative practices in the Member States**, which imposes the **processing of data in** ~~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 **or any other entity authorised by national law to perform a public function or exercise public authority** 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~~ **Without prejudice to paragraph 3 and to data localisation requirements laid down on the basis of existing Union law, data localisation requirements** shall ~~not~~ be prohibited ~~or restricted~~, unless ~~it is~~ **these are** justified on **~~imperative~~** grounds of public security **~~or public policy, or concern activities which are connected with the exercise of official authority as set out in Article 51 of TFEU~~.**

2. Member States shall ~~notify~~ **immediately communicate** 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~~ **Articles 5 to 7 of** Directive (EU) 2015/1535.

3. Within ~~12~~ **24** months after the start of application of this Regulation, Member States shall ensure that any **existing** data localisation requirement**, laid down in a law, regulation or administrative provision of a general nature,** that is not in compliance with paragraph 1 is repealed. If a Member State considers that a**n existing** data localisation requirement is in compliance with paragraph 1 and may therefore remain in force, it shall ~~notify~~ **communicate** that measure to the Commission, together with a justification for maintaining it in force.

~~**3a. Where a Member State is required to communicate or notify a measure to the Commission under this Regulation and under Directive (EU) 2015/1535 or Directive 2006/123/EC, a communication or notification carried out under those Directives shall be deemed to constitute a communication under this Regulation.**~~

4. Member States shall make the details of any data localisation requirements**, laid down in a law, regulation or administrative provision of a general nature,** applicable in their territory publicly available online via a **national** single information point which they shall keep up-to-date**, or provide those up-to-date details to a central information point established under another Union act**.

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 link**(**s**)** to such point**(**s**)** 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.~~

2a. Where a ~~user fails to comply with an obligation to provide data~~ competent authority does not receive access to data pursuant to paragraph 1 and if no specific cooperation mechanism exists under Union law or international agreements to exchange data between competent authorities of different Member States, a competent authority may request the assistance from a competent authority of another Member State in accordance with the procedure set out in Article 7.

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.

3a. ~~In case of abuse of right or fraud by a specific user,~~ Member States may impose effective, proportionate and dissuasive sanctions for failure to comply with an obligation to provide data, in accordance with Union and national law. In case of abuse of right ~~or fraud~~ by a specific user, such sanctions imposed on the specific user may include measures temporarily derogating from Article 4, Paragraph 1 ~~the temporary imposition on the user of data localisation requirements~~.

~~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 contribute to a competitive data economy,** ~~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~~ **based on the principle of interoperability and taking due account of open standards, covering *inter alia*** the following ~~issues~~ **aspects**:

(aa) best practices in facilitating the switching of providers and porting data in a structured, commonly ~~used~~ and machine-readable format allowing sufficient time for ~~the~~ professional users to switch or port the data; and

(a) **minimum information requirements to ensure that professional users are provided with sufficiently detailed, clear and transparent information before a contract for data ~~storage and~~ processing is concluded, regarding** 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~~

(c) approaches to certification ~~schemes~~ for data ~~storage and other~~ processing products and services for professional users, taking into account established national or international norms, facilitating the comparability of these products and services. Such ~~schemes~~ approaches may include inter alia quality management, information security management, business continuity management and, environmental management.

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*~~ ***Procedure for cooperation between authorities***

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**a**, 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.

4a. The authority so requested shall, without undue delay **and within the timeframe proportionate to the urgency of the request, provide a response communicating the data requested or informing the requesting competent authority that it does not consider the conditions for requesting assistance under this Regulation to have been met.**

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

~~(d) 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**a** 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
The President

For the Council
The President