Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance)

REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 November 2018

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

(Text with EEA relevance)

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[(1)],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure[(2)],

Whereas:

(1) The digitisation of the economy is accelerating. Information and Communications Technology is no longer a specific sector, but the foundation of all modern innovative economic systems and societies. Electronic data are at the centre of those systems and can generate great value when analysed or combined with services and products. At the same time, the rapid development of the data economy and emerging technologies such as Artificial Intelligence, Internet of Things products and services, autonomous systems, and 5G are raising novel legal issues surrounding questions of access to and reuse of data, liability, ethics and solidarity. Work should be considered on the issue of liability, in particular through the implementation of 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 might also include appropriate mechanisms for determining liability, for transferring responsibility among cooperating services, for insurance and for auditing.

(2) Data value chains are built on different data activities: data creation and collection; data aggregation and organisation; data processing; data analysis, marketing and distribution; use and re-use of data. The effective and efficient functioning of data processing is a fundamental building block in any data value chain. However, the effective and efficient functioning of data processing, 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: data localisation requirements put in place by Member States' authorities and vendor lock-in practices in the private sector.

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

(4) Such obstacles to the free movement of data processing services and to the right of establishment of service providers originate from requirements in the laws of Member States to locate data in a specific geographical area or territory for the purpose of data processing. Other rules or administrative practices have an equivalent effect by imposing specific requirements which make it more difficult to 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 processing. This Regulation in no way limits the freedom of businesses to conclude contracts specifying where data are to be located. This Regulation is merely intended to safeguard that freedom by ensuring that an agreed location can be situated anywhere within the Union.

(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 processing services from porting their data from one service provider to another or back to their own information technology (IT) systems, not least upon termination of their contract with a service provider.

(6) The combination of those obstacles has led to a lack of competition between cloud service providers in the Union, to various vendor lock-in issues, and to a serious lack of data mobility. Likewise, data-localisation policies have undermined the ability of research and development companies to facilitate collaboration between firms, universities, and other research organisations with the aim of driving innovation.

(7) For reasons of legal certainty and because of 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 necessary to adopt uniform rules applicable in all Member States.

(8) The legal framework on the protection of natural persons with regard to the processing of personal data, and on respect for private life and the protection of personal data in electronic communications and in particular Regulation (EU) 2016/679 of the European Parliament and of the Council[(3)] and Directives (EU) 2016/680[(4)] and 2002/58/EC[(5)] of the European Parliament and of the Council are not affected by this Regulation.

(9) The expanding Internet of Things, artificial intelligence and machine learning, represent major sources of non-personal data, for example as a result of their deployment in

automated industrial production processes. Specific examples of non-personal data include aggregate and anonymised 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. If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly.

(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 is justified by public security reasons. Regulation (EU) 2016/679 and this Regulation provide a coherent set of rules that cater for free movement of different types of data. Furthermore, this Regulation does not impose an obligation to store the different types of data separately.

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

(12) This Regulation should not affect data processing in so far as it is carried out as part of an activity which falls outside the scope of Union law. In particular, it should be recalled that, in accordance with Article 4 of the Treaty on European Union ('TEU'), national security is the sole responsibility of each Member State.

(13) The free flow of data within the Union will play an important role in achieving data-driven growth and innovation. Like businesses and consumers, Member States' public authorities and bodies governed by public law stand to benefit from increased freedom of choice regarding data-driven service providers, from more competitive prices and from a more efficient provision of services to citizens. Given the large amounts of data that public authorities and bodies governed by public law handle, it is of the utmost importance that they lead by example by taking up data processing services and that they refrain from making data localisation restrictions when they make use of data processing services. Therefore, public authorities and bodies governed by public law should be covered by this Regulation. In this regard, the principle of the free flow of non-personal data for which this Regulation provides should apply also to general and consistent administrative practices and to other data localisation requirements in the field of public procurement, without prejudice to Directive 2014/24/EU of the European Parliament and of the Council[(6)].

(14) As in the case of Directive 2014/24/EU, this Regulation is without prejudice to laws, regulations, and administrative provisions which relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as the laws, regulations and administrative provisions of Member States that provide for the implementation of those powers and responsibilities. While public authorities and bodies governed by public law are encouraged to consider the economic and other benefits of outsourcing to external service providers, they might have legitimate reasons to choose self-provisioning of services or insourcing. 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.

(15) This Regulation should apply to natural or legal persons who provide data processing services to users residing or having an establishment in the Union, including those who provide data processing services in the Union without an establishment in the Union. This Regulation should therefore not apply to data processing services taking place outside the Union and to data localisation requirements relating to such data.

(16) 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[(7)]. In particular, to the extent that the law applicable to a contract has not been chosen in accordance with that Regulation, a contract for the provision of services is, in principle, governed by the law of the country of the service provider's habitual residence.

(17) This Regulation should apply to data 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 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)).

(18) Data localisation requirements represent a clear barrier to the free provision of data processing services across the Union and to the internal market. As such, they should be banned unless they are justified on grounds of public security, as defined by Union law, in particular within the meaning of Article 52 TFEU, and satisfy the principle of proportionality enshrined in Article 5 TEU. 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, the processing of data in multiple locations across the Union, and since this Regulation provides for measures to ensure data availability for regulatory control purposes, Member States should only be able to invoke public security as a justification for data localisation requirements.

(19) The concept of ‘public security’, within the meaning of Article 52 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 order, in particular, to facilitate 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 the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests. In compliance with the principle of proportionality, data localisation requirements that are justified on grounds of public security should be suitable for attaining the objective pursued, and should not go beyond what is necessary to attain that objective.

(20) 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 immediately communicate to the Commission any draft act that introduces a new data localisation requirement or modifies an existing data localisation requirement. Those draft acts should be submitted and assessed in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council[(8)].

(21) Moreover, in order to eliminate potential existing barriers, during a transitional period of 24 months from the date of application of this Regulation, Member States should carry out a review of existing laws, regulations or administrative provisions of a general nature laying down data localisation requirements and communicate to the Commission any such data localisation requirement that they consider being in compliance with this Regulation, together with a justification for it. This should enable the Commission to examine the compliance of any remaining data localisation requirements. The Commission should be able, where appropriate, to make comments to the Member State in question. Such comments could include a recommendation to amend or repeal the data localisation requirement.

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

(23) In order to ensure the transparency of data localisation requirements in the Member States laid down in a law, regulation or administrative provision of a general nature for natural and legal persons, such as service providers and users of data processing services, Member States should publish information on such requirements on a national online single information point, and regularly update that information. Alternatively, Member States should provide up-to-date information on such requirements to a central information point established under another Union act. In order to appropriately inform natural and legal persons of data localisation requirements across the Union, Member States should notify to the Commission the addresses of such single information points. The Commission should publish this information on its own website, along with a regularly updated consolidated list of all data localisation requirements in force in Member States, including summarised information on those requirements.

(24) Data localisation requirements frequently stem from a lack of trust in cross-border data 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 stipulate that it does not affect the powers of competent authorities to request or obtain access to data in accordance with Union or national law, and that competent authorities cannot be refused access to data on the basis that the data are processed in another Member State. Competent authorities could impose functional requirements to support access to data, such as requiring that system descriptions are to be kept in the Member State concerned.

(25) 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 are processed. Such access can be ensured through concrete terms and conditions in contracts between the natural or legal person subject to the obligation to provide access and the service provider.

(26) Where a natural or legal person is subject to an obligation to provide data and fails to comply with that obligation, 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 under 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, Council Framework Decision 2006/960/JHA[(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 providing access to the data sought, through designated single points of contact.

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

(28) This Regulation should not allow users to attempt to evade the application of national law. It should therefore provide for the imposition, by Member States, of effective, proportionate and dissuasive penalties on users which prevent competent authorities from receiving access to their data necessary for the performance of the competent authorities' official duties under Union and national law. In urgent cases, where a user abuses its right, Member States should be able to impose strictly proportionate interim measures. Any interim measures requiring the re-localisation of data for longer than 180 days following the re-localisation would deviate from the free movement of data principle for a significant period and should, therefore, be communicated to the Commission for the examination of their compatibility with Union law.

(29) The ability to port data without hindrance is a key factor in facilitating user choice and effective competition on markets for data processing services. The real or perceived

difficulties in porting data cross-border also undermine the confidence of professional users when taking up cross-border offers, and thereby their confidence in the internal market. Whereas individual consumers benefit from existing Union law, the ability to switch between service providers is not facilitated for those users who act in the course of their business or professional activities. Consistent technical requirements across the Union, whether concerning technical harmonisation, mutual recognition or voluntary harmonisation, also contribute to developing a competitive internal market for data processing services.

(30) In order to take full advantage of the competitive environment, professional users should be able to make informed choices and to easily compare the individual components of various data processing services offered in the internal market, including in respect of the contractual terms and 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 service providers and professional users of data processing services, the detailed information and operational requirements for data porting should be defined by market players through self-regulation, encouraged, facilitated and monitored by the Commission, in the form of Union codes of conduct which might include model contractual terms and conditions.

(31) In order to be effective and to make switching between service providers and data porting easier, such codes of conduct should be comprehensive and should cover at least the key aspects that are important during the process of porting data, such as the processes used for, and the location of, data back-ups; 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 service provider. The codes of conduct should also make clear that vendor lock-in is not an acceptable business practice, should provide for trust-increasing technologies, and should be regularly updated in order to keep pace with technological developments. The Commission should ensure that all relevant stakeholders, including associations of small and medium-sized enterprises (SMEs) and start-ups, users and cloud service providers are consulted throughout the process. The Commission should evaluate the development, and the effectiveness of the implementation, of such codes of conduct.

(32) Where a competent authority in one Member State requests assistance from another Member State in order to obtain access to data pursuant to this Regulation, it should submit, through a designated single point of contact, a duly justified request to the latter's designated single point of contact, which should include a written explanation of the reasons and the legal bases for seeking access to the data. The single point of contact designated by the Member State whose assistance is requested should facilitate the transmission of 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 experienced in fulfilling such request, or on its grounds for refusing it.

(33) Enhancing trust in the security of cross-border data 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 as regards compliance with the applicable security requirements when they outsource their data processing activities to service providers, including to those in other Member States.

(34) Any security requirements related to data processing that are applied in a justified and proportionate manner on the basis of Union or national law in compliance with Union law in the Member State of residence or establishment of the natural or legal persons whose data are concerned should continue to apply to processing of that data in another Member State. Those natural or legal persons should be able to fulfil such requirements either themselves or through contractual clauses in contracts with service providers.

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

(36) Directive (EU) 2016/1148 of the European Parliament and of the Council[(15)] provides for legal measures to boost the overall level of cybersecurity in the Union. Data processing services constitute one of the digital services covered by that Directive. According to that Directive, Member States are 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.

(37) The Commission should submit a report on the implementation of this Regulation, in particular with a view to determining the need for modifications in the light of technological or market developments. That report should in particular evaluate this Regulation, especially its application to data sets composed of both personal and non-personal data, as well as the implementation of the public security exception. Before this Regulation starts to apply, the Commission should also publish informative guidance on how to handle data sets composed of both personal and non-personal data, in order that companies, including SMEs, better understand the interaction between this Regulation and Regulation (EU) 2016/679, and to ensure that both Regulations are complied with.

(38) 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, the freedom of expression and information and the freedom to conduct a business.

(39) Since the objective of this Regulation, namely to ensure the free flow of data other than 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 TEU. 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 aims to ensure the free flow 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 the porting of data for professional users.

Article 2

Scope

1 This Regulation applies to the 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 service 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 In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.

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

This Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law defined in point (4) of Article 2(1) of Directive 2014/24/EU, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as the laws, regulations, and administrative provisions of Member States that provide for the implementation of those powers and responsibilities.

Article 3

Definitions

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

(1) ‘data’ means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679;

(2) ‘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;

(3) 'draft act' means a text drafted for the purpose of being 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;

(4) 'service provider' means a natural or legal person who provides data 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 a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the 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 to exercise official authority, that has the power to obtain access to data processed by a natural or legal person for the performance of its official duties, as provided for by Union or national law;

(7) 'user' means a natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service;

(8) 'professional user' means a natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service for purposes related to its trade, business, craft, profession or task.

Article 4

Free movement of data within the Union

1 Data localisation requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality.

The first subparagraph of this paragraph is without prejudice to paragraph 3 and to data localisation requirements laid down on the basis of existing Union law.

2 Member States shall 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 Articles 5, 6 and 7 of Directive (EU) 2015/1535.

3 By 30 May 2021, Member States shall ensure that any existing data localisation requirement that is laid down in a law, regulation or administrative provision of a general nature and that is not in compliance with paragraph 1 of this Article is repealed.

By 30 May 2021, if a Member State considers that an existing measure containing a data localisation requirement is in compliance with paragraph 1 of this Article and can therefore remain in force, it shall communicate that measure to the Commission, together with a justification for maintaining it in force. Without prejudice to Article 258 TFEU, the Commission shall, within a period of six months from the date of receipt of such communication, examine the compliance of that measure with paragraph 1 of this

Article and shall, where appropriate, make comments to the Member State in question, including, where necessary, recommending the amendment or the repeal of the measure.

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 and applicable in their territory publicly available via a national online single information point which they shall keep up-to-date, or provide up-to-date details of any such localisation requirements 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, along with a regularly updated consolidated list of all data localisation requirements referred to in paragraph 4, including summarised information on those requirements.

Article 5

Data availability for competent authorities

1 This Regulation shall not affect the powers of competent authorities to request, or obtain, 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 are processed in another Member State.

2 Where, after requesting access to a user's data, a competent authority does not obtain access and if no specific cooperation mechanism exists under Union law or international agreements to exchange data between competent authorities of different Member States, that competent authority may request assistance from a competent authority in 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 processing equipment and means, by the requested authority, such access must be in accordance with Union law or national procedural law.

4 Member States may impose effective, proportionate and dissuasive penalties for failure to comply with an obligation to provide data, in accordance with Union and national law.

In the case of abuse of rights by a user, a Member State may, where justified by the urgency of accessing the data and taking into account the interests of the parties concerned, impose strictly proportionate interim measures on that user. If an interim measure imposes re-localisation of data for a duration that is longer than 180 days following re-localisation, it shall be communicated within that 180-day period to the Commission. The Commission shall, in the shortest possible time, examine the measure and its compatibility with Union law, and, where appropriate, take the necessary measures. The Commission shall exchange information with the single points of contact of Member States referred to in Article 7 on experience gained in this regard.

Article 6

Porting of data

1 The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level (‘codes of conduct’), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards, covering, inter alia, the following aspects:

a best practices for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data;

b minimum information requirements to ensure that professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information regarding the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or port data back to its own IT systems;

c approaches to certification schemes that facilitate the comparison of data processing products and services for professional users, taking into account established national or international norms, to facilitate the comparability of those products and services. Such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management;

d communication roadmaps taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.

2 The Commission shall ensure that the codes of conduct are developed in close cooperation with all relevant stakeholders, including associations of SMEs and start-ups, users and cloud service providers.

3 The Commission shall encourage service providers to complete the development of the codes of conduct by 29 November 2019 and to effectively implement them by 29 May 2020.

Article 7

Procedure for cooperation between authorities

1 Each Member State shall designate a single point of contact which 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 Where a competent authority in one Member State requests assistance from another Member State, pursuant to Article 5(2), in order to obtain access to data, it shall submit a duly justified request to the latter's designated single point of contact. The request shall include a written explanation of the reasons and the legal bases for seeking access to the data.

3 The single point of contact shall identify the relevant competent authority of its Member State and transmit the request received pursuant to paragraph 2 to that competent authority.

4 The relevant competent authority so requested shall, without undue delay and within a 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 that the conditions for requesting assistance under this Regulation have been met.

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

6 The single points of contact shall provide users with general information on this Regulation, including on the codes of conduct.

Article 8

Evaluation and guidelines

1 No later than 29 November 2022, the Commission shall submit a report to the European Parliament, to the Council and to the European Economic and Social Committee evaluating the implementation of this Regulation, in particular in respect of:

a the application of this Regulation, especially to data sets composed of both personal and non-personal data in the light of market developments and technological developments which might expand the possibilities for deanonymising data;

b the implementation by Member States of Article 4(1), and in particular the public security exception; and

c the development and effective implementation of the codes of conduct and the effective provision of information by service providers.

2 Member States shall provide the Commission with the necessary information for the preparation of the report referred to in paragraph 1.

3 By 29 May 2019, the Commission shall publish informative guidance on the interaction of this Regulation and Regulation (EU) 2016/679, especially as regards data sets composed of both personal and non-personal data.

Article 9

Final provisions

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

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 Strasbourg, 14 November 2018.

For the European Parliament

The President

A. TAJANI

For the Council

The President

K. EDTSTADLER

(**1**) OJ C 227, 28.6.2018, p. 78.

(**2**) Position of the European Parliament of 4 October 2018 (not yet published in the Official Journal) and decision of the Council of 6 November 2018.

(**3**) 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).

(**4**) 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).

(**5**) 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).

(**6**) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

(**7**) 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) (OJ L 177, 4.7.2008, p. 6).

(**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).

(**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 L 268, 12.10.2010, p. 1).

(**15**) 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).

Status:
Point in time view as at 31/01/2020.

Changes to legislation:
There are outstanding changes not yet made to Regulation (EU) 2018/1807 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations.