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

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. (See end of Document for details) View outstanding changes*

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

***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. (See end of Document for details) View outstanding changes*

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)].

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. (See end of Document for details) View outstanding changes*

(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

***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. (See end of Document for details) View outstanding changes*

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