European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 55-61
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 0.53136/9791221807981 07

*The Regulation (EU) 2018/1807 on a Framework for the Free Flow of non-Personal Data in the European Union and its Implementation by Public Administrations**

Joel A. Alves
(Researcher at the Research Centre for Justice and Governance of the University of Minho)

ABSTRACT This article has a two-fold objective: (i) firstly, it aims to present the main features of the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union; (ii) secondly, it seeks to reflect on how those may affect public administrations – one of the most relevant players in the European data economy.

1. *Introduction*

Back in 2014, the European Commission expressed its belief that a thriving data-driven economy could bring huge benefits for people, business, and public administrations.[1] Since then, that conviction has not been weakened, but rather reinforced. Nevertheless, one thing came clear: for this to happen, any Member-State action affecting data storage or processing should be guided by a *principle of free movement of data within the internal market*.[2]

Building on these premises, the European Parliament and the Council have adopted the Regulation (EU) 2018/1807,[3] which aims to ensure the *free flow of data other than personal data within the European 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*.[4] The idea was to fill the gaps in the existing legal framework,[5] providing for a coherent set of rules that cater for the free movement of different types of data within the Union's borders.[6] This is because the General Data Protection Regulation already prohibited restrictions on the free flow of data within the European Union *on grounds connected with the protection of personal data*.[7] However, limitations based on *other reasons* – e.g. restrictions provided for under tax or accounting laws for purposes of regulatory control[8] – were not covered by such legal instrument.[9] Furthermore, *data other than*

* Article submitted to double-blind peer review.
This article was written with a support of a PhD Research scholarship from the Portuguese national funding agency for science, research and technology (fellowship no. 2022.13673.BD).

[1] See European Commission, COM(2014) 442 final, *Towards a thriving data-driven economy*, 2 July 2014, 12.

[2] See European Commission, COM(2017) 9 final, *Building a European Data Economy*, 10 January 2017, 7.

[3] 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, hereinafter, referred to as "Regulation (EU) 2018/1807" or simply "the Regulation".

[4] See article 1 of the Regulation.

[5] See P.J. Muñoz, *Algunas reflexiones acerca de la propuesta de Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*, in F. Galindo (ed.), *¿Como poner en práctica el gobierno abierto?*, Madrid, Editorial Reus, 2019, 52 f.

[6] See recital 10 of the Regulation. In the same vein, see European Commission, COM(2019) 250 final, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, 29 May 2019, 2.

[7] See article 1(3) of the General Data Protection Regulation, where the following is stated: "the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data". For further developments, see J.L.P. Mañas, *Objecto del Reglamento*, in J.L.P. Mañas, M.A. Caro and M.R. Gayo (eds.), *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad*, Madrid, Editorial Reus, 2016, 51 f. and 55 ff.

[8] An example of such a restriction would be a national law that requires payroll accounts to be located in a particular Member State, for reasons connected to regulatory control, e.g., by the national tax authority. See European Commission, COM(2019) 250 final, 13.

[9] See European Commission, COM(2017) 228 final, "A

personal data were equally left outside of its material scope.[10]

In this vein, this article has a two-fold objective: (i) firstly, it aims to present the main features of this (still) recent piece of legislation: (ii) secondly, it seeks to reflect on how those may affect public administrations – one of the most relevant players in the data economy.[11]

2. *Main features*

2.1. *The principle of free flow of non-personal data across borders*

Aligned with the Commission communication "Building a European Data Economy",[12] Regulation (EU) 2018/1807 openly recognizes that enabling data to flow freely across borders is almost a precondition to achieve data-driven growth and innovation.[13] Accordingly, the mentioned legal instrument proposes to establish, with regard to *non-personal data*, the *principle of free movement within the European Union* similar to the one provided for, under the General Data Protection Regulation, *vis-à-vis personal data.*[14]

Conversely to the latter, the restrictions on the free flow of data that the Regulation (EU) 2018/1807 intends to tackle do not, however, originate from the existence of different national standards, between the Union's Member States, concerning the protection of the rights and freedoms of natural persons.[15] They rather arise from certain "requirements in the laws of Member States to locate data in a specific geographical area or territory for the purpose of data processing".[16] But also, from "other rules or administrative practices [that] 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".[17]

In the light of the above, article 4(1) of the Regulation sets out that "data localisation requirements[18] shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality". This means that, as a general rule, Member States should not be able to force organisations to locate the storage or processing of data within their borders.[19] Restrictions will only be justified for reasons of public security.[20] And, even in that case,

Connected Digital Single Market for All", 10 May 2017, 10.

[10] See article 2(1) of the General Data Protection Regulation, read in conjunction with article 4(1) thereof. For further developments, see A. von dem Bussche and P. Voigt, *The EU General Data Protection Regulation (GDPR): a practical guide*, Cham, Springer, 2017, 9 ff.

[11] This idea is supported by recital 8 of Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public-sector information, where it reads: "The public sector in Member States collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, political, economic, legal, geographical, environmental, meteorological, seismic, touristic, business, patent-related and educational areas. Documents produced by public sector bodies of the executive, legislature or judiciary constitute a vast, diverse and valuable pool of resources that can benefit society". Similarly, recital 9 states: "Public sector information represents an extraordinary source of data that can contribute to improving the internal market and to the development of new applications for consumers and legal entities".

[12] See European Commission, COM(2017) 9 final, 7.

[13] See recital 13 of the Regulation.

[14] See recital 10 of the Regulation.

[15] See P.A.M. Asensio, *Servicios de almacenamiento y tratamiento de datos: el Reglamento (EU) 2018/1807 sobre libre circulación de datos no personales*, in *La Ley Unión Europea*, n. 66, 2019, 4.

[16] See recital 4 of the Regulation.

[17] Idem.

[18] Pursuant to article 4(1) of the Regulation a "data-localisation requirement" should be understood as "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". This means that, for the purposes of the Regulation, "data-localisation requirements" can take various forms: they may be set out in laws, in administrative regulations and provisions or even result from general and consistent administrative practices. Also, they may consist either in direct or indirect restrictive measures. Examples of the formers would be an obligation to store data in a specific geographic location (e.g. servers must be located in a particular Member State) or an obligation to comply with unique national technical requirements (e.g. data must use specific national formats). Regarding the latter, they may include requirements to use technological facilities that are certified or approved within a specific Member State or other requirements that have the effect of making it more difficult to process data outside of a specific geographic area or territory within the European Union. For further developments, see European Commission, COM(2019) 250 final, 11 f.

[19] See European Commission, *State of the Union 2017: A framework for the free flow of non-personal data in the EU*, 19 September 2017.

[20] See recital 18 of the Regulation. In any case, recital 19 recalls that the concept of "public security", as defined by Union law and as interpreted by the Court of Justice, presupposes "the existence of a genuine and

they (i) must be suitable for attaining the objectives pursued, and (ii) must not got beyond what is necessary to attain these objectives.[21]

It follows that, after a transitional period of 24 months from the data of application of the Regulation – which has already lapsed[22] – any existing data-localisation requirements that are not in compliance with the aforesaid conditions shall be repealed.[23] Besides that – "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"[24] – Member States are also required to communicate to the Commission any draft act[25] which introduces new data-localisation requirements or make changes to existing data-localisation requirements in conformity with the procedures set out in articles 5, 6 and 7 of 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.[26]

Furthermore – and so as to promote transparency *vis-à-vis* natural and legal persons, including *service providers* and *users of data-processing services*[27] – the Regulation obliges Members States to make the details of any data-localisation requirements applicable in their territory publicly available via a national online single information point, which shall be kept up-to-date. Or, alternatively, to provide up-to-date details on such requirements to a central information point established under another Union act.[28] In any case, the same legal instrument sets out that Member States should notify to the Commission the address of such single information points. Subsequently, for the convenience of businesses and to provide for their easy access to relevant information across the Union, the Commission shall publish the links to these information points on its website (i.e., the Your Europe portal[29]), along with a regularly-updated and consolidated list of all data-localisation requirements, including summary-information on those requirements.[30]

2.2. *The principle of data availability for regulatory control*

Notwithstanding the foregoing, the legislator seemed to be conscious that data-localisation requirements frequently stemmed from a lack of trust in cross-border data processing, founded on the presumed unavailability of data for regulatory purposes.[31] This is because, as previously pointed out by the European Commission, a number of Member States apparently believed that data would be more easily accessible for their national competent authorities if they were stored or processed locally[32] – even if, in practice, data-localisation restrictions rarely proved to be a measure suitable to achieve that objective.[33]

In this vein, the Regulation seeks to overcome this problem, by establishing a new cooperation mechanism, aiming to ensure that competent authorities stay able to exercise any rights they have to access data that are being processed in other Member States.[34] The idea is simple: the prohibition of data-location restrictions shall not affect the powers of

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 interest". So that, to make use of that exception, Member States must give evidence that the data localisation requirements they want to put in place are justified on one of such grounds.

[21] See recital 18 of the Regulation.

[22] As follows from article 4(3) of the Regulation, the referred transitional period ended on 30 May 2021.

[23] See article 4(3) of the Regulation, read in conjunction with recital 21 thereof.

[24] See recital 20 of the Regulation.

[25] For the purposes of the Regulation, "draft act" should be understood as any "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". See article (2)(3) of the Regulation.

[26] See article 4(2) of the Regulation. In our view also existing data-localisation requirements that, despite being considered as legitimate, were not communicated to the Commission, for the purposes and in accordance with article 4(3) of the Regulation, by 30 May 2021, should be covered by subject to this requirement.

[27] See recital 23 of the Regulation.

[28] See article 4(4) of the Regulation.

[29] See European Commission, COM(2019) 250 final, 13. The said portal is available at https://europa.eu/youreurope/index.htm.

[30] See article 4(5) of the Regulation, read in conjunction with recital 23 thereof.

[31] See recital 24 of the Regulation.

[32] See European Commission, COM(2017) 9 final, 6.

[33] Idem, ibidem.

[34] See European Commission, COM(2019) 250 final, 3.

competent authorities[35] to request or obtain access to data for the performance of their official duties in accordance with Union or national law.[36] So that, such authorities cannot be refused access to data on the basis that the data are processed in another Member State.[37]

As a result, where a natural or legal person is subject to an obligation to provide data and fails to comply with that obligation, the competent authority may request assistance from a competent authority in another Member State, by submitting a fully-justified request to the latter's designated single point of contact.[38] Nevertheless, it will only be able to make use of this power in the absence of specific cooperation instruments in Union law or under international agreements.[39] Still, whereas a request for assistance entails obtaining access to any premises of 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.[40]

At any rate, it is stressed that the Regulation should not allow users to attempt to evade the application of national law.[41] This is why article 5(4) of such legal instrument stipulates that "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". Moreover, the same provision equally states that, in urgent cases, where users abuse their right, Member States should also be able to impose strictly proportionate interim measures, such as requiring the (temporary) re-localisation of the data.[42]

2.3. *Porting data and switching between data-processing services*

While removing data-localisation restrictions was considered the most important factor to unleash the full potential of the data economy in the European Union,[43] recital 2 of the Regulation still notes that there were other obstacles to data mobility and to the internal market that demanded attention – namely, *vendor lock-in practices in the private sector*, i.e., practices hindering users of data-processing services from switching between service providers, by «locking» their data in the provider's system (e.g. due to a specific data format or contractual arrangements) and making it unable to be transferred outside of that.[44]

On this point, though, the said legal instrument does not provide for specific obligations.[45] Instead, it limits to stimulate industry self-regulation,[46] by establishing that the Commission shall encourage the development of codes of conduct at Union level, covering, *inter alia*, the following aspects: (i) *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;[47] (ii) *minimum information requirements* to ensure that professional users are provided,

[35] For the purposes of the Regulation, "competent authority" should be understood as any "authority of a Member State or any other entity authorized 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. See article 3(6) of the Regulation.

[36] See article 5(1) of the Regulation, read in conjunction with recital 24 thereof.

[37] See article 5(1) of the Regulation, read in conjunction with recital 24 thereof.

[38] See article 5(2) of the Regulation, read in conjunction with article 7 and recital 32 thereof.

[39] See recital 26 of the Regulation. Pursuant to that provision, examples of such specific cooperation instruments would be, "in the area of police cooperation, criminal or civil justice or in administrative matters respectively, the Council Framework Decision 2006/960/JHA, Directive 2014/41/EU of the European Parliament and of the Council, the Convention on Cybercrime of the Council of Europe, Council Regulation (EC) No. 1206/2001, Council Directive 2006/112/EC, and Council Regulation (EU) No 904/2010".

[40] See article 5(3) of the Regulation, read in conjunction with recital 27 thereof.

[41] See recital 28 of the Regulation.

[42] See article 5(4) of the Regulation. Nonetheless – and according to this provision – if the re-localisation of data is imposed for a duration that is longer than 180 days following re-localisation, it should be communicated to the Commission, within that 180-day period, for the examination of their compatibility with Union Law.

[43] See European Commission, *State of the Union 2017: A framework for the free flow of non-personal data in the EU*.

[44] See European Commission, COM(2019) 250 final, 16 f.

[45] See P.A.M. Asensio, *Servicios de almacenamiento y tratamiento de datos: el Reglamento (EU) 2018/1807 sobre libre circulación de datos no personales*, 7.

[46] Idem, ibidem.

[47] See article 6(1)(a) of the Regulation.

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 professional users want to switch to another service provider or port data back to their own IT systems;[48] (iii) *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;[49] and (iv) *communication roadmaps* taking a multi-disciplinary approach to raise awareness of the codes of conduct among relevant stakeholders.[50] Also, the Regulation requires the Commission to ensure that such codes be developed in close cooperation with all relevant stakeholders, including associations of SMEs and start-ups, users and cloud service providers.[51]

3. *Impact on public administrations*

3.1. *General obligations*

That said, Regulation (EU) 2018/1807 leaves no room for doubts in what regards the applicability of its provisions to public administrations. In fact, recital 13 thereof is unambiguous: "public authorities and bodies governed by public law should be covered by [the scope of] this Regulation".[52] This is confirmed by article 2(1) of the same legal instrument, where the following is stated: "the 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 European Union; or; (b) *carried out by a* natural or *legal person* residing or *having an establishment in the Union for its own needs*" (italics added).

To put it simply: pursuant to the referred legal provision, Regulation (EU) 2018/1807 should apply to *service providers*, who provide data-processing services to users residing or having an establishment in the European Union (including those who provide data-processing services in the Union without an establishment in that legal area).[53] But also, to *any natural or legal person residing or having an establishment in the European Union who processes data for its own needs.* Consequently, the decision of whether public administrations should, or should not, be subject to the obligations laid down in such legal instrument, in a particular case, would be exclusively dependent on the interpretation of two key terms: the notion of "processing";[54] and the notion of "data other than personal data".[55]

At any rate, article 2(2) of the Regulation makes clear that those obligations shall also apply to the processing of *mixed data sets*[56] –

[48] See article 6(1)(b) of the Regulation.
[49] See article 6(1)(c) of the Regulation. Pursuant this provision, "such approaches may include, inter alia, quality management, information security management, business continuity management and environmental management".
[50] See article 6(1)(d) of the Regulation.
[51] See article 6(2) of the Regulation.
[52] This solution is consistent with the General Data Protection Regulation, who also applies both to public and private entities. For further developments, see J.A. Alves, *The General Data Protection Regulation and its application to the public sector*, in *PoLaR – Portuguese Law Review*, vol. 4, n. 2, 2020, 179 ff.
[53] See recital 15 of the Regulation.
[54] Pursuant to article 3(2) of the Regulation, the concept of "processing" should be understood as "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, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". This provision closely follows the concept of processing of personal data enshrined in article 4(2) of the General Data Protection Regulation, stating: "processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".
[55] As already explained by the European Commission, this concept is defined by opposition (*a contrario)* to the notion of personal data, provided for under article 4(1) of the General Data Protection Regulation. See article 3(1) of the Regulation. For further developments, see European Commission, COM(2019) 250 final, 4 ff. On the concept of "personal data" see also Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 6 ff.
[56] Nonetheless – and according to the aforementioned provision – those obligations will only apply to the *non-personal data* part of the data set. The remaining part – i.e., the *personal-data* part – shall be subject to the relevant rules and principles provided for under the General Data Protection Regulation. Furthermore, if the *non-personal data* part and the *personal-data part* are "inextricably linked", the General Data Protection Regulation should fully apply to the whole mixed set, even if personal data represent only a small part of the data set. For further developments, see European Commission, COM(2019) 250 final, 9.

i.e., data sets composed of both *personal* and *non-personal data*[57], which represent the majority of the data sets used in the data economy.[58]

Despite the above, it should however be mentioned that, as Directive 2014/24/EU,[59] Regulation (EU) 2018/1807 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.[60] Therefore, while encouraging public administrations to consider economic and other benefits of outsourcing to external service providers, nothing in this legal instrument obliges them to contract out or externalise the provision of services that they wish to provide themselves or to organise by means other than public contracts.[61] Moreover, the Regulation also points out that it should not affect data processing in so far as it is carried out as part of activities which fall outside the scope of Union law (e.g., activities related to national security).[62]

3.2. *Indirect benefits*

Nevertheless, one must not forget that public administrations will often act as "competent authorities", in the meaning of article 3(6) of the Regulation.[63] Thus, irrespective of the referred obligations, they will still be (positively) impacted by such legal instrument when requesting or obtaining access to data for the purposes and in accordance with article 5 thereof.

Furthermore, public administrations might also be "users" of data-processing services (e.g. when outsourcing the storage of non-personal data on cloud-services providers).[64] So, like business and consumers, they are expected to take advantage from the removal of unjustified data-localisation requirements, which hampered the freedom to provide services and the freedom of establishment within the Digital Single Market.[65] After all, this will presumably result in huge benefits, ranging from an increased freedom of choice regarding data-driven service providers to access to cheaper and more innovative solutions.[66]

Finally, as "professional users",[67] public administrations stand to benefit from the ability "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",[68] provided for future self-regulatory codes of conduct, adopted under article 6 of the Regulation.[69]

4. *Final remarks*

Despite all the criticism it has been attracted,[70] Regulation (EU) 2018/1807 constitutes an important step[71] to enable the European Union to become "the most attractive, most secure and most dynamic data-agile economy in the world".[72]

[57] See European Commission, COM(2019) 250 final, cit., 8.
[58] Idem, ibidem.
[59] 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.
[60] See article 2(3) of the Regulation, read in conjunction with recital 14 thereof.
[61] See recital 14 of the Regulation.
[62] See article 2(3) of the Regulation, read in conjunction with recital 12 thereof.
[63] See P.J. Muñoz, *Algunas reflexiones acerca de la propuesta de Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*, 57 ff.
[64] Pursuant to article 2(3) of the Regulation "user" means "a natural or legal person, *including a public authority or body governed by public law*, using or requesting a data processing service" (emphasis added).
[65] See recital 18 of the Regulation. In the same vein, see European Commission, COM(2017) 9 final, 3.
[66] See recital 13 of the Regulation.
[67] Article 2(8) of the Regulation defines "professional user" as "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" (emphasis added).
[68] See recital 30 of the Regulation.
[69] See, in particular, article 6(1)(b) of the Regulation.
[70] While referring to the proposal of the European Commission on which the Regulation is founded, see, by way of example, D. Broy, *The European Commission's Proposal for a Framework for the Free Flow of Non-Personal Data in the EU*, in *European Data Protection Law Review*, vol. 3, n. 3, 2017, 383.
[71] In a similar vein, see P.J. Muñoz, *Algunas reflexiones acerca de la propuesta de Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea*, 51f and 61.
[72] This ambition has been recently restated by the European Commission, under its communication

Given the large amounts of data that public administrations handle, it is therefore of the utmost importance that they lead by example,[73] by complying fully with their obligations under such legal instrument – including those arising from the *principle of free flow of non-personal data across borders*[74] and the *principle of availability of data for regulatory control*[75].

Nonetheless, the Regulation should not be seen merely as a legal burden, but also as a chance: a chance for public administrations to make the most of digital and data technologies.

entitled *A European strategy for data*. See European Commission, COM(2020) 66 final, *A European strategy for data*, 19 February 2020, 25.

[73] See recital 13 of the Regulation.

[74] See article 4(1) of the Regulation.

[75] See article 5(1) of the Regulation.