Opinion of the European Economic and Social Committee on 'Communication from the Commission to the European Parliament and the Council — Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union'

(COM(2019) 250 final)

(2020/C 14/18)

Rapporteur: **Laure BATUT**

Referral	European Commission, 22.7.2019
Legal basis	Article 304 of the Treaty on the Functioning of the European Union
Section responsible	Transport, Energy, Infrastructure and the Information Society
Adopted in section	11.9.2019
Adopted at plenary	25.9.2019
Plenary session No	546
Outcome of vote (for/against/abstentions)	162/2/6

1. Recommendations

1.1. The EESC recommends that the Commission:

— provide clear and simple information on the criteria for defining non-personal data and the scope of the Regulation on a framework for the free flow of non-personal data (the Free Flow of Non-Personal Data Regulation) in order to remove uncertainty and increase confidence;

— inform actors about overlaps between EU data legislation;

— while promoting free movement, ensure that personal data do not gradually come to be seen as non-personal data and that the General Data Protection Regulation (GDPR) retains its full scope, if necessary merging the two regulations in the medium term for the purposes of stronger data protection rather than increased commodification of data;

— encourage the establishment and development of federations of pan-European cloud computing services;

— help Europeans in the very short term to use algorithms capable of processing the vast amounts of non-personal data in the single market for data; encourage the Member States to improve lifelong education in the areas of IT and artificial intelligence (AI) at all levels (school, university and work);

— encourage actors to develop a sense of responsibility, ethical awareness and solidarity; not allow self-regulation and the "amicable" settlement of disputes to give rise to conflicting interpretations of legislative texts;

— not hesitate to use regulation where necessary;

— promote sanctions for breach of self-regulation;

— draw up a road map to verify whether companies actually have legal certainty regarding the free use of their data as provided for in the Free Flow of Non-Personal Data Regulation;

— take stock of the current situation in the 27 Member States and assess the work of the national contact points after twelve months of operation;

— scrupulously carry out its responsibilities with regard to informing, communicating with and providing alerts to all concerned;

— ask the Member States to inform actors about the criteria they use to define "public security";

— call on the Member States to disperse their storage facilities for non-transferable data;

— review competition policy in good time to ensure that, as currently configured, it is geared to the free flow of data.

2. **Introduction**

2.1. The EESC takes note of the Commission's aim to provide guidance to the companies affected by the transfer of non-personal data before the negotiation of codes of conduct between stakeholders in the course of 2020. The fact that data are frequently mixed, i.e. comprise both non-personal and personal data, can create uncertainty for businesses as regards the measures to be taken to protect such data. The main principles of the existing rules should be outlined here before looking at the points on which the EESC wishes to make comments.

2.2. The Commission found that the lack of competitiveness between cloud computing services in the EU, and thus the lack of data mobility in an environment characterised by oligopolies, had a negative impact on the data market. The Free Flow of Non-Personal Data Regulation requires the Member States to minimise both their data localisation requirements and legislative fragmentation in this field, in order to stimulate growth and unleash businesses' innovation capacity.

2.3. With the adoption of the Regulation on the free movement of non-personal data, which complements the GDPR, a "fifth freedom of movement" (in the words of Anna-Maria Corazza Bildt, MEP and rapporteur) applying to all forms of data has been introduced into 21st century EU texts. If its owner so wishes, it must be possible to transfer this intangible commodity, so to speak, for management purposes to hosting service providers in countries other than the EU Member State in which it was created and/or used (Article 1, Free Flow of Non-Personal Data Regulation). This will make processing easier for data owners and will enhance their competitiveness.

The Free Flow of Non-Personal Data Regulation

2.4. Regulation (EU) 2018/1807 of the European Parliament and of the Council [1] promotes the free movement of non-personal data in the EU in order to develop artificial intelligence, cloud computing and big data analytics. It stipulates (Article 6) that the Commission shall guide, encourage and assist operators working with non-personal data in developing self-regulatory codes of conduct at EU level.

2.5. Aimed at professionals working in micro-enterprises and SMEs, this guidance is intended to give them a better understanding of how the Free Flow of Non-Personal Data Regulation and the GDPR interact. For illustrative purposes, the Commission cites numerous examples.

2.6. The codes of conduct currently being drafted should be ready sometime between November 2019 and May 2020 (recitals 30 and 31, Article 6(1)), and will reflect the opinions of all parties. Two public consultations are underway and two working groups, made up of professionals, are assisting the Commission: one on cloud security certification (CSPCERT) and the other on data porting and switching between cloud service providers (SWIPO). Their input covers Infrastructure-as-a-Service and Software-as-a-Service. In May 2020, the Commission will propose encouraging the industry to develop model contractual terms and, in 2022, will brief the European Parliament, the Council and the EESC on the implementation of the regulation, particularly the use of mixed datasets.

3. **General comments**

3.1. *The Commission's mission: to bring the Free Flow of Non-Personal Data Regulation into line with the General Data Protection Regulation (GDPR)*

3.1.1. In order to reconcile these two complementary regulations, the Commission explains that: (1) data localisation requirements **are now prohibited**; (2) the data remain accessible to the **competent authorities**; and (3) the data become mobile and can therefore be "ported" . The GDPR employs the term "portability", while the Free Flow of Non-Personal Data Regulation refers to "porting" . Users can transfer their data outside the country in which they were created and then retrieve them without (too many) constraints after switching service providers for the purposes of storage, processing or analysis. Unlike "portability" , which is a right for all concerned, "porting" is carried out in line with codes of conduct and is therefore part of a self-regulation process.

[1] OJ L 303, 28.11.2018, p. 59.

3.1.2. This constitutes a significant difference between the two regulations as one is based on **hard law** and the other on non-binding instruments (**soft law**), which are known to offer far fewer guarantees. However, according to the Commission itself, most datasets contain both personal and non-personal data which are **inextricably linked** and can therefore be considered "mixed" datasets.

3.1.3. The EESC welcomes this supportive approach and, as it agrees with the examples chosen, does not intend to propose others. However, it notes that the Commission's guidance for operators merely illustrates the context by providing a number of standard scenarios. The EESC would therefore like to draw the Commission's attention to some critical areas that, despite the guidance and future codes of conduct, might pose problems for users.

3.2. *Outline of principles*

3.2.1. Principle: the free movement of data

The barriers to the free movement of non-personal data are not so much geographical as functional and/or linked to the means available to companies to use IT technologies.

Under the Free Flow of Non-Personal Data Regulation, data localisation requirements for non-personal data are prohibited in a given territory (Article 4). Member States are asked to repeal any provisions to the contrary within 24 months from the date on which the Regulation comes into effect (May 2021).

The Regulation allows exceptions to be made for reasons of public security. Member States must publish detailed information online about their respective national localisation requirements. The Commission may make comments and publish links to the websites on which the Member States have placed such information.

3.2.2. Exceptions to the freedom of movement

— Member State authorities may have **access to transferred data**: the Free Flow of Non-Personal Data Regulation establishes a procedure whereby a supervisory authority in one state can obtain data processed in another. The Regulation provides for a cooperation procedure between Member States (Articles 5 and 7). However, without localisation, the EESC's fear is that certain data (accounting data, financial data, contractual data, etc.) will be outside the control of Member State authorities. The EESC reminds the Commission not to hesitate to use regulation where necessary.

— The **single "point of contact"** of each Member State will process the request together with the national supervisory authority, which may or may not provide the data if it considers the request to be admissible. In keeping with the spirit of the Free Flow of Non-Personal Data Regulation, the contact points should help actors to make an informed decision concerning transfers and service providers throughout the EU, with due regard for competition.

  The EESC believes that guidance alone cannot remove the many uncertainties surrounding the implementation of this principle. Assessing the reasons given by the Member States, the good faith of operators or the proper functioning of the contact points is not a straightforward matter. Any such assessment will be difficult.

— Prohibition of direct or indirect requirements regarding data localisation except where justified on grounds of "public security". The EESC believes that the concept of "public security" invoked in the Regulation is insufficiently precise and its scope unclear when applied to data flow and its commodification. The Free Flow of Non-Personal Data Regulation defines data localisation requirements 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 administrative practices ([2]) which would require operators to retain data within a given territory in the EU. For the Court of Justice of the European Union (CJEU) ([3]) (and recital 19, Free Flow of Non-Personal Data Regulation), public security covers both "the internal and external security of a Member State", and presupposes the existence of "a genuine and sufficiently serious threat affecting one of the fundamental interests of society". This definition includes genetic data, biometric data and data on health. The Member State's response must be proportionate.

([2]) Regulation (EU) 2018/1807, Article 3(5).

([3]) See Communication COM(2019) 250, footnote 13 and judgments in Case C-331/16 and Case C-366/16: *K. v Staatssecretaris van Veiligheid en Justitie and H. F. v Belgische Staat*: "42. As regards the **concept of 'public security'**, it is clear from the Court's case-law that this concept **covers both the internal and external security of a Member State** (judgment of 23 November 2010, *Tsakouridis*, C-145/09, EU:C:2010:708, paragraph 43). Internal security may be affected by, inter alia, a **direct threat to the peace of mind and physical security** of the population of the Member State concerned (see, to that effect, judgment of 22 May 2012, I., C-348/09, EU:C:2012:300, paragraph 28). As regards external security, that may be affected by, inter alia, the **risk of a serious disturbance to the foreign relations of that Member State** or to the peaceful coexistence of nations (see, to that effect, judgment of 23 November 2010, *Tsakouridis*, C-145/09, EU:C:2010:708, paragraph 44)".

3.2.3. As regards free movement and data localisation, the Committee considers that:

— the criteria selected are subject to broad interpretation;

— only the courts will be able to shed light on them on a case-by-case basis, which may undermine the trust required for business, especially in the case of sensitive data; disputes arising from codes of conduct could lead to even greater divergence;

— the courts move infinitely more slowly than the digital sphere and data flows.

The EESC believes that such an uncertain and complicated situation can have a deterrent effect on micro-enterprises and SMEs.

3.2.4. The EESC regrets the fact that the guidance does not make any reference to disputes or to ways of verifying how Member States will comply with the public security criteria and how they might be penalised, where appropriate. The EESC is concerned that the explanations contained in the Communication are not sufficient to allow micro-enterprise and SME operators to avoid all the legal pitfalls of the texts and that the attendant uncertainties impede efforts to foster the sense of trust and legal certainty needed to develop the sector.

3.2.5. The EESC acknowledges the enormous value of the Commission's Communication in disseminating information widely and in a top-down fashion regarding the situation created by the two regulations. The micro-enterprise and SME sector is in dire need of this. The EESC would like the action of the national contact points and the latter's use of the Commission's site to be assessed after six months of operation, so that corrective measures can be taken quickly should a lack of information and communication be identified.

4. **Specific comments**

4.1. *Data*

4.1.1. By default, non-personal data include all digital data which do not come under personal data as defined by the GDPR. Examples would be business data, data on precision farming, data on maintenance requirements of machines and meteorological data.

4.1.2. Data collected by public services such as hospitals, social protection or tax departments can be very close to patients' or taxpayers' personal data. Businesses that use them must ensure that the identity of the persons concerned is not revealed and that once they have been rendered anonymous the process cannot be reversed. In the case of micro-enterprises or SMEs, this may entail overly expensive and time-consuming procedures. As the two regulations (the GDPR and the Free Flow of Non-Personal Data Regulation) between them provide for the free movement of all data in the EU when they are "**inextricably linked**", the legal safeguards provided for in the GDPR apply therefore to all mixed data (recital 8 and Article 2(2) of Regulation (EU) 2018/1807). Thus, in addition to the restriction on the free flow of non-personal data relating to public security, there is a further restriction regarding the nature of the data involved. This is the crux of the Commission's Communication, which reiterates that personal and non-personal data are very close: "Mixed datasets represent the majority of datasets" (Communication, point 2.2; they can be "inextricably linked" (point 2.2); "neither of the two Regulations obliges businesses to separate the datasets" (point 2.2).

4.1.3. It is up to the company in question to determine whether the non-personal data it processes are "inextricably linked" to personal data and, if so, to ensure their protection. The preparation of "*out management*" is no easy task for a company. Establishing a general definition of mixed data would seem to be impossible, and the overlap between the two regulations will probably give rise to further overlaps with other data legislation, such as legislation relating to intellectual property: the flow of non-personal data is permitted, but if such data is reused in a work, it will no longer be subject to the same rules. The EESC believes that the links between the different texts will prove problematic. The case law already requires that the issue of inextricability be examined on the basis of a "reasonable" criterion. The EESC notes that it was clearly not possible for the Commission in its Communication to review every potential scenario and offer guidance to all concerned, with the result that big companies are at a distinct advantage. The EESC recommends that the Commission ensure that personal data do not gradually come to be treated, in practice, as non-personal data and that the GDPR retains its full scope, if necessary merging the two regulations in the medium term for the purposes of stronger data protection rather than increased commodification of data.

4.2. *Portability, transfer, processing and storage of data*

The GDPR asserts that portability must be governed by legislation (Article 20), while the Free Flow of Non-Personal Data Regulation considers self-regulation to be the key. The EESC regrets that this could create considerable legal uncertainty, thereby disadvantaging micro-enterprises and SMEs because of the many legal risks involved. The EESC believes that if non-personal data are commodities, albeit intangible and in free circulation, then they can be imported and exported. A debate on the ownership of non-personal data would be worthwhile in the current context. However, the real value lies not in the data themselves but in the vast quantities of data. The Committee therefore believes that competition policy may not be suitable for this type of market. The EESC wonders how the current situation can enhance the productivity of micro-enterprises and SMEs. The Commission's Communication does not provide any clarification on this point.

4.3. *Service providers*

4.3.1. The EU does not have any large-scale operators nor a "European" cloud, something that the EESC has for a long time considered a major shortcoming. The much sought-after economies of scale are available only to US IT giants and some Chinese companies. This is why even the Member States' major administrations are tempted to entrust these companies with the management of their data (as France has done).

4.3.2. The EESC believes that Europeans need to create partner ecosystems and to allow cross-platform data transfers. In addition to what it proposes to do in its Communication, the Commission could help micro-enterprises and SMEs to develop their respective resources, much as it did for services of general interest (SGIs) in its 2018 project, "Pan-European Cloud Computing Services", for the provision of economic and non-economic SGIs (Function as a Service: *FaaS*) and as envisaged in its network of Digital Innovation Hubs ("A network of Digital Innovation Hubs", web/Commission/DIHs/January 2019).

4.4. *Data security* ([4])

4.4.1. At the internal level, national operators ([5]) check the nature of their data that is to be transferred and ensure that they are secure. Localisation requirements corresponded to enforceable security rules in national law. Despite the GDPR and the Free Flow of Non-Personal Data Regulation, IT security standards are not at an equivalent level across the EU. The Committee believes that national contact points should provide strong information on this matter to micro-enterprises and SMEs as well as to private and public services in different languages.

At the external level, the EESC believes that it is not certain to what extent companies outside the EU will be able to comply with codes of conduct and to return data after the data owners have requested further transfers. It fears that in the long run, it will become difficult to identify where individual responsibilities lie.

The Committee recommends that, in the very short term, the Commission help European actors to use algorithms capable of processing the vast amounts of non-personal data in the single market for data.

4.4.2. The issue of where the servers are physically located and how they are made secure will continue to be a matter for trade and diplomatic negotiations between states. This issue is paramount. Confronted with the IT giants and their respective reference states, and despite the fact that data management is a competence shared between the Member States and the EU, there would be some risk involved should the Member States decide to negotiate individually.

4.4.3. The EESC proposes that in its Communication the Commission should clarify the obligations incumbent upon service providers regarding the storage of non-personal data, the methods used, physical locations, the planned or authorised data shelf life and the use made of such data once they have been processed, as these elements are fundamental to data security and may be important for European companies in the context of global competition.

4.5. *Codes of conduct*

4.5.1. As of May 2019, all those concerned by the Free Flow of Non-Personal Data Regulation (primarily cloud service users and providers) have been invited to develop their code of conduct within 12 months. According to the Commission, best practices, approaches to certification schemes and communication roadmaps should be taken into account. The SWIPO and CSPCERT working groups will provide expertise.

4.5.2. The Commission refers to the approach taken in relation to the GDPR (Communication, page 23). Since this regulation is framed by the opinion of the EDPS ([6]), it could be used as a basis for the Free Flow of Non-Personal Data Regulation. Each industry's representative associations may draw up a code of conduct. In doing so they must demonstrate to the competent authorities that their draft code of conduct, whether national or transnational, fulfils a specific sectoral need, facilitates the implementation of the regulation and establishes effective mechanisms for monitoring compliance with the code.

([4]) OJ C 227, 28.6.2018, p. 86.
([5]) OJ C 218, 23.7.2011, p. 130.
([6]) EDPS, the European Data Protection Board; Guidelines 1/2019 on Codes of Conduct, 12.2.19, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

4.5.3. Even before the entry into force of the GDPR, the major providers of Infrastructure as a Service (*IaaS*) and Software as a Service (*SaaS*) had drawn up their own codes of conduct to define how these would be implemented, thereby removing the areas of uncertainty identified by the industry ([7]); they involved SMEs in this, believing that for many of them self-certification was preferable to the very high cost of certification.

4.5.4. The EESC favours a sector-by-sector approach to the Free Flow of Non-Personal Data Regulation, should a one-size-fits-all approach not be appropriate. In the context of the GDPR, a non-exhaustive list of items to be covered by the codes has been established (Article 40(2)), in particular as regards the fair and transparent nature of the procedures, the security of data transfer and the settlement of disputes. In their own interest and to enhance consumer confidence in the European approach, actors should be encouraged to build on this and to develop a sense of responsibility, ethical awareness and solidarity, in particular through guidance that takes account of AI. This is one of the points that the Committee wishes to address: it recommends that the Commission not allow self-regulation and the "amicable" settlement of disputes to give rise to conflicting interpretations of the texts. On the contrary, every effort should be made to consolidate the latter, thereby creating rules that are applicable to all; moreover, this should be mentioned in its information and communication roadmaps.

5. **Evaluation**

On a regular basis, the Commission will evaluate the impact of free flow, the implementation of the regulation, the repeal of restrictive measures by the Member States and the effectiveness of the codes of conduct. The EESC feels that civil society representatives should also have the opportunity to express their views on the matter ([8]). For society as a whole to feel secure and therefore have confidence in these new digital practices, both the EU and the Member States must dispel any uncertainty relating to applicable data law, data confidentiality, data retention, loss-free data recovery, guarantees of feasibility and good faith of the actors involved, and financial guarantees. Because the inextricability of personal and non-personal data has become a source of concern and given the proportion of such data relative to all existing datasets, the EESC questions whether self-regulation really is the only way forward. It recommends that, in the medium term, the GDPR rules apply to all data and all data movements, with the exception of "genuine" non-personal data.

Brussels, 25 September 2019.

The President
of the European Economic and Social Committee
Luca JAHIER

([7]) CISPE (Cloud Infrastructure Services Providers in Europe).
([8]) OJ C 487, 28.12.2016, p. 92; OJ C 62, 15.2.2019, p. 292.

ANNEX

The following proposed amendments were rejected by the assembly but received at least one-quarter of the votes cast in favour (Rule 59(3) of the Rules of Procedure):

Point 4.1.3

Amend as follows:

It is up to the company in question to determine whether the non-personal data it processes are "inextricably linked" to personal data and, if so, to ensure their protection. The preparation of "out management" is no easy task for a company. Establishing a general definition of mixed data would seem to be impossible, and the overlap between the two regulations will probably give rise to further overlaps with other data legislation, such as legislation relating to intellectual property: the flow of non-personal data is permitted, but if such data is reused in a work, it will no longer be subject to the same rules. The EESC believes that the links between the different texts will prove problematic. The case law already requires that the issue of inextricability be examined on the basis of a "reasonable" criterion. The EESC notes that it was clearly not possible for the Commission in its Communication to review every potential scenario and offer guidance to all concerned, with the result that big companies are at a distinct advantage. The EESC recommends that the Commission ensure that personal data do not gradually come to be treated, in practice, as non-personal data and that the GDPR retains its full scope~~, if necessary merging the two regulations in the medium term~~ for the purposes of stronger data protection rather than increased commodification of data.

Point 5

Amend as follows:

On a regular basis, the Commission will evaluate the impact of free flow, the implementation of the regulation, the repeal of restrictive measures by the Member States and the effectiveness of the codes of conduct. The EESC feels that civil society representatives should also have the opportunity to express their views on the matter. For society as a whole to feel secure and therefore have confidence in these new digital practices, both the EU and the Member States must dispel any uncertainty relating to applicable data law, data confidentiality, data retention, loss-free data recovery, guarantees of feasibility and good faith of the actors involved, and financial guarantees. Because the inextricability of personal and non-personal data has become a source of concern and given the proportion of such data relative to all existing datasets, the EESC questions whether self-regulation really is the only way forward. ~~It recommends that, in the medium term, the GDPR rules apply to all data and all data movements, with the exception of "genuine" non-personal data.~~

Point 1.1, third bullet point

Amend as follows:

The EESC recommends that the Commission:

…

— *while promoting free movement, ensure that personal data do not gradually come to be seen as non-personal data and that the General Data Protection Regulation (GDPR) retains its full scope~~, if necessary merging the two regulations in the medium term~~ for the purposes of stronger data protection rather than increased commodification of data;*

…

Reason

GDPR and Regulation (EU) 2018/1807 have different legal basis, respectively Article 16 TFEU on individuals fundamental right to protection of personal data and Article 114 TFEU on approximation of laws, the two provisions allowing the EU different scope for intervention on private business (which is the reason why in the first case the EU intervened by very strict and detailed regulation while in the second case chose self-regulation as the most appropriate, proportional means of intervention). Therefore, these two instruments cannot be legally merged.

Outcome of the vote on the amendments

Votes in favour: 54

Votes against: 84

Abstentions: 18