Council of the
European Union

**Brussels, 12 June 2019**
**(OR. en)**

**10253/19**

**TELECOM 260**
**COMPET 486**
**MI 519**
**DATAPROTECT 168**
**JAI 683**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director |
| date of receipt: | 29 May 2019 |
| To: | Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union |
| No. Cion doc.: | COM(2019) 250 final |
| Subject: | 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 |

Delegations will find attached document COM(2019) 250 final.

Encl.: COM(2019) 250 final

EUROPEAN
COMMISSION

Brussels, 29.5.2019
COM(2019) 250 final

# 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

Contents

# 1 Introduction

In an increasingly data-driven economy, data flows are at the core of business processes in companies of all sizes and in all sectors. New digital technologies are opening up new opportunities for the general public, businesses and public administrations in the European Union (the 'EU').

To further increase the cross-border exchange of data and boost the data economy, in November 2018 the European Parliament and the Council adopted the Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union[1] (the 'Free Flow of Non-Personal Data Regulation'), based on a proposal from the European Commission (the 'Commission'). The Regulation applies from 28 May 2019. The principle of free movement of personal data is already laid down in Regulation (EU) 2016/679 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 (the 'General Data Protection Regulation')[2]. As a result, there is now a comprehensive framework for a common European data space and the free movement of all data within the European Union.[3]

The Free Flow of Non-Personal Data Regulation creates legal certainty for businesses to process their data wherever they want in the EU, raises trust in data processing services and counters vendor lock-in practices. This will increase customer's choice, improve efficiency and stimulate the adoption of cloud technologies, leading to significant savings for businesses in EU. One study shows that businesses in EU can save 20-50 % of their IT costs by migrating to the cloud[4].

Thanks to the two Regulations, data can flow freely between Member States, allowing users of data processing services to use the data gathered in different EU markets to improve their productivity and competitiveness. Users can therefore take full advantage of the economies of scale provided by the large EU market, improving their global competitiveness and increasing the interconnectivity of the European data economy.

The Free Flow of Non-Personal Data Regulation has three notable features:

- It prohibits, as a rule, Member States imposing requirements on where data should be localised. Exceptions to this rule may only be justified on grounds of public security in compliance with the proportionality principle.

---

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

[2] 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.

[3] The General Data Protection Regulation covers also the European Economic Area (EEA) which includes Iceland, Liechtenstein and Norway. In addition, the Free Flow of Non-Personal Data Regulation is marked EEA relevant.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016. Available online at: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- It establishes a cooperation mechanism to make sure that competent authorities continue to be able to exercise any rights they have to access data that are being processed in another Member State.
- It provides incentives for industry, with the support of the Commission, to develop self-regulatory codes of conduct on the switching of service providers and the porting of data.

**Purpose of this guidance**

This guidance fulfils Article 8(3) of the Free Flow of Non-Personal Data Regulation, which requires the Commission to publish guidance on the interaction between this Regulation and the General Data Protection Regulation, 'especially as regards datasets composed of both personal and non-personal data'.

This guidance aims to help users - especially small and medium-sized enterprises - understand the interaction between the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation[5]. The guidance therefore particularly addresses: (i) the concepts of non-personal data and personal data; (ii) the principles of free movement of data and the prohibition of data localisation requirements under both Regulations; and (iii) the notion of data portability under the Free Flow of Non-Personal Data Regulation. It also covers self-regulatory requirements set out in the two Regulations.

The Free Flow of Non-Personal Data Regulation only covers 'data other than personal data' as defined by the General Data Protection Regulation. The General Data Protection Regulation governs the processing of personal data, which is an essential part of the EU's data protection framework[6]. It entered into force in the Member States on 25 May 2018. The Regulation lays down harmonised rules to protect people in the EU/EEA with regard to the processing of their personal data and on the free movement of such data. The General Data Protection Regulation: (i) specifies what information constitutes personal data; (ii) establishes legal grounds for their processing; and (iii) defines the rights and obligations to be observed

---

[5] Recital 37 of the 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.

[6]
- Regulation (EU) No 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 119/1, 4.5.2016 p. 1.
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.
- Directive (EU) 2016/680 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, repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.
- 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 (currently under revision).

when processing these data[7], among other provisions. With regard to the principle of free movement of personal data, Article 1(3) of the General Data Protection Regulation provides that '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.'

In most real-life situations, a dataset is very likely to be composed of both personal and non-personal data. This is often referred to as a 'mixed dataset'. Section 2.2 below further explains the interaction between the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation with regard to mixed datasets.

For the sake of clarity, there are no contradictory obligations under the General Data Protection Regulation and the Free Flow of Non-Personal Data Regulation.

# 2 The interaction between the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation - mixed datasets

## 2.1 The concept of non-personal data in the Free Flow of Non-Personal Data Regulation

The Free Flow of Non-Personal Data Regulation[8] aims to ensure the free flow of data other than personal data. Throughout its text, the Regulation uses the term 'data', which should be understood as 'data other than personal data as defined in point 1 of Article 4 of the Regulation (EU) 2016/679 [the General Data Protection Regulation]'[9]. Such data, also being referred to as '**non-personal data**' in this document, are defined by opposition (*a contrario*) to personal data, as laid down by the General Data Protection Regulation.

Personal data

The General Data Protection Regulation reads: '"personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural

---

[7] For further guidance on various aspects of the 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) and the European data protection law, see the web page of the European Data Protection Board, which has issued a number of guidelines in accordance with Article 70 of the General Data Protection Regulation, available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en. The relevant web page has also references to guidelines, recommendations and other documents issued by the European Data Protection Board's ancestor - Article 29 Working Party. Furthermore, to raise citizens' and businesses' awareness on 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), the Commission issued a Communication on data protection - guidance on direct application of the GDPR (COM/2018/043 final) available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

[8] Article 1 of the 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.

[9] See Article 3(1) of the 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.

person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

The broad definition of personal data is intentional and has remained essentially unchanged in the General Data Protection Regulation as compared to the previous legislation[10]. Various aspects of the definition of personal data, such as 'any information', 'relating to', 'identified or identifiable', were already addressed by the Article 29 Working Party[11] in its Opinion 4/2007 on the concept of personal data as of 20 June 2007, WP 136.

It is common practice in areas like research, to pseudonymise personal data in order to disguise an individual's identity. **Pseudonymisation** is the processing of personal data in such a way that it is not possible to attribute them to a specific person without the use of additional information. This additional information is kept separately and is secured through organisational or technical measures (e.g. encryption)[12,13]. Nonetheless, data which have been pseudonymised are still considered information about an identifiable person if they can be attributed to this person by using additional information[14]. Such data **constitute personal data** in accordance with the General Data Protection Regulation.

Non-personal data

Where the data are not 'personal data' as defined in the General Data Protection Regulation, they are **non-personal**. The non-personal data can be categorised by origin as:

---

10 See Article 2(a) of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (date of end of validity: 24 May 2018, repealed by the General Data Protection Regulation). See also case law of the Court of Justice on the definition of personal data, recognising the broad interpretation of such a notion, for example judgment of the Court of Justice of 29 January 2009, *Productores de Música de España (Promusicae)* v *Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54; judgment of the Court of Justice of 24 November 2011, *Scarlet Extended SA* v *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; judgment of the Court of Justice of 19 October 2016, *Patrick Breyer* v *Bundersrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779.

11 The Article 29 Working Party was an advisory body that provided advice on data protection matters to the Commission and which helped in development of harmonised data protection policies in the EU. After the General Data Protection Regulation entered into the force on 25 May 2018, the Article 29 Working Party was succeeded by the European Data Protection Board.

12 See Article 4(5) of the 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) which defines 'pseudonymisation'.

13 For instance, a research study on the effects of a new medicine would qualify as pseudonymisation, if the personal data of study participants would be replaced by unique attributes (e.g. number or code) in the research documentation and their personal data would be kept separately with the assigned unique attributes in a secured document (e.g. in a password protected database).

14 See Recital 26 of the 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).

- Firstly; data which originally did not relate to an identified or identifiable natural person, such as data on weather conditions generated by sensors installed on wind turbines or data on maintenance needs for industrial machines.

- Secondly; data which were initially personal data, but were later made **anonymous**[15]. The 'anonymisation' of personal data is different to pseudonymisation (see above), as properly anonymised data cannot be attributed to a specific person, not even by use of additional data[16] and are therefore non-personal data.

The assessment of whether data is properly anonymised depends on specific and unique circumstances of each individual case[17]. Several examples of re-identification of datasets that were supposedly anonymised have showed that such an evaluation may be demanding[18]. To establish whether an individual is identifiable, one has to look on all means reasonably likely to be used by a controller or by another person to identify an individual directly or indirectly[19].

**Examples of non-personal data:**

- Data which are aggregated to the extent that individual events (such as a person's individual trips abroad or travel patterns which could constitute personal data) are no longer identifiable, can be qualified as anonymous data[20]. Anonymous data are used

[15] See Recital 26 of the 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), which provides that '…the principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.'

[16] See judgment of the Court of Justice of 19 October 2016, *Patrick Breyer* v *Bundesrepublik Deutschland*, C-582/14, ECLI:EU:C:2016:779. The Court of Justice held that dynamic internet protocol (IP) address may constitute personal data even if a third party (e.g. internet service provider) is in possession of additional data, which would make it possible to identify the individual. The possibility to identify the individual must constitute means reasonably likely to be used to identify the individual, whether directly or indirectly.

[17] Data anonymisation should always be performed using the latest state-of-the-art anonymisation techniques.

[18] For examples of re-identification of supposedly anonymised data see the study on future data flows conducted for the European Parliament's ITRE Committee by Blackman, C., Forge, S.: *Data Flows — Future Scenarios: In-Depth Analysis for the ITRE Committee,* 2017, p. 22, Box 2. Available online at: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] See Recital 26 of the Regulation (EU) 2016/679 the General Data Protection Regulation, pursuant to which 'to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.'

[20] See Article 29 Working Party: *Opinion 05/2014 on Anonymisation Techniques*, adopted on 10 April 2014, WP216, p. 9: 'Only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous. For example: if an organisation collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as "on Mondays on trajectory X there are 160 % more passengers than on Tuesdays", that would qualify as anonymous data.'

for instance in statistics or in sales reports (for example to assess the popularity of a product and its features).

- High-frequency trading data in the finance sector, or data on precision farming which help to monitor and optimise the use of pesticides, nutrients and water.

However, if non-personal data can be related to an individual in any way, causing them to be either directly or indirectly identifiable, the data must be considered as personal data.

For example, if a quality control report on a production line makes it possible to relate the data to specific factory workers (e.g. those who set the production parameters), then the data would qualify as personal data and the General Data Protection Regulation has to be applied. The same rules apply when developments in technology and data analytics make it possible to convert anonymised data into personal data. [21]

As the definition of personal data refers to 'natural persons', datasets containing the names and contact details of legal persons are in principle non-personal data.[22] However, in certain situations they may be personal data.[23] This will be the case, if, for example, the name of the legal person is the same as that of a natural person who owns it or if the information relates to an identified or identifiable natural person.[24]

## 2.2 Mixed datasets

The Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation approach the free movement of data in the EU from two different angles.

The Free Flow of Non-Personal Data Regulation lays down a general prohibition against data localisation requirements for non-personal data. Article 4(1) of the regulation prohibits data localisation requirements unless they are justified on grounds of public security in compliance with the principle of proportionality.

---

[21] If personal data are processed unlawfully or the processing otherwise violates the General Data Protection Regulation, the data subjects (natural persons) are entitled under the General Data Protection Regulation to lodge a complaint with a national supervisory authority (data protection authority) in the EU or to seek an effective judicial remedy before a national court. The tasks, competences and powers of national supervisory authorities are regulated in Chapter VI, Section 2 of the General Data Protection Regulation.

[22] Recital 14 of the 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) states that 'This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.' This however needs to be read in the light of the definition of personal data in Article 4(1) of the General Data Protection Regulation.

[23] See judgment of the Court of Justice of 9 November 2010 in joint cases *Volker und Markus Schecke GbR*, C-92/09 and *Hartmut Eifert*, C-93/09 v *Land Hessen*, ECLI:EU:C:2010:662, paragraph 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en

The General Data Protection Regulation, in addition to ensuring a high level of protection of personal data, ensures the free flow of personal data. In accordance with Article 1(3) of the Regulation, the free movement of personal data 'shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.' Together, the two Regulations provide for the free movement of 'all' data within the EU. The specific provisions are further addressed in Section 3.1 and 3.2.

A mixed dataset consists of both personal and non-personal data. Mixed datasets represent the majority of datasets used in the data economy and are common because of technological developments such as the Internet of Things (i.e. digitally connecting objects), artificial intelligence and technologies enabling big data analytics.

**Examples of mixed datasets:**

- a company's tax record, mentioning the name and telephone number of the managing director of the company;
- datasets in a bank, particularly those with client information and transaction details, such as payment services (credit and debit cards), partner relationship management (PRM) applications and loan agreements, documents mixing data concerning natural and legal persons;
- a research institution's anonymised statistical data and the raw data initially collected, such as the replies of individual respondents to statistical survey questions;
- a company's knowledge database of IT problems and their solutions based on individual IT incident reports;
- data related to the Internet of Things, where some of the data allow assumptions to be made about identifiable individuals (e.g. presence at a particular address and usage patterns); and
- analysis of operational log data of manufacturing equipment in the manufacturing industry.

**Example: customer relationship management services**

Some banks use customer relationship management (CRM) services provided by third parties that require a client's data to be made available in the CRM environment. Data held in the CRM service will include any information needed to effectively manage the interaction with the customer, such as their postal and email address, their phone number, the products and services they purchase, and sales reports, including aggregated data. These data can therefore include both personal and non-personal customer data.

With respect to mixed datasets, the Free Flow of Non-Personal Data Regulation[25] provides that:

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

This means that, in a case of a dataset composed of both personal and non-personal data:

- the Free Flow of Non-Personal Data Regulation applies to the non-personal data part of the dataset;
- the General Data Protection Regulation's free flow provision[26] applies to the personal data part of the dataset; and
- if the non-personal data part and the personal data parts are 'inextricably linked', the data protection rights and obligations stemming from the General Data Protection Regulation fully apply to the whole mixed dataset, also when personal data represent only a small part of the dataset[27].

This interpretation is in line with the right to personal data protection guaranteed by the Charter of Fundamental Rights of the European Union[28] and with Recital 8 of the Free Flow of Non-Personal Data Regulation[29]. Recital 8 thereof provides that 'the legal framework on the protection of natural persons with regard to the processing of personal data…, in particular [the General Data Protection Regulation]… and Directives (EU) 2016/680 and 2002/58/EC… are not affected by this Regulation.'

**Practical example:**

A company operating within the EU offers its services via a platform. Businesses (customers) upload their documents, which contain mixed datasets on the platform. As a 'controller', the business uploading the documents needs to make sure that the processing complies with the General Data Protection Regulation. By processing the dataset on behalf of the controller, the company that offers the services (the 'processor') needs to store and process the data in compliance with the General Data Protection Regulation, for instance to make sure that an appropriate level of security related to data is guaranteed, including by means of encryption.

---

25 Article 2(2) thereof

26 Article 1(3) of the 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). See also Section 3.2. hereof.

27 As recalled in the *Commission Staff Working Document, Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union* (SWD(2017) 304 final), part 1/2, p. 3, 'regardless of how much of personal data are included in mixed datasets, GDPR [the General Data Protection Regulation] needs to be fully complied with in respect to the personal data part of the set.'

28 Charter of Fundamental Rights of the European Union, OJ C 362, 26.10.2012, p. 391.

29 Recital 8 thereof

The concept of 'inextricably linked' is not defined by either of the two Regulations[30]. For practical purposes, it can refer to a situation whereby a dataset contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible. For example, when buying CRM and sales reporting systems, the company would have to duplicate its cost on software by purchasing separate software for CRM (personal data) and sales reporting systems (aggregated/non-personal data) based on the CRM data.

Separating the dataset is also likely to decrease the value of the dataset significantly. In addition, the changing nature of data (see Section 2.1) makes it more difficult to clearly differentiate and thus separate between different categories of data.

Importantly, neither of the two Regulations obliges businesses to separate the datasets they are controlling or processing.

Consequently, a mixed dataset will generally be subject to the obligations of data controllers and processors and respect the rights of data subjects established by the General Data Protection Regulation.

**Processing of health data**

Health data can be part of a mixed dataset. Examples include electronic health records, clinical trials or sets of data collected by various mobile health and wellbeing applications (such as applications for measuring our health status, for reminding us to take our medication or for tracking our fitness progress)[31]. The exact division between personal and non-personal data in these datasets is becoming increasingly blurred with technological developments. Consequently, their processing must comply with the General Data Protection Regulation, in particular (given that health data is a special category of data according to the Regulation) with Article 9, which lays out a general prohibition on the processing of special categories of data and exceptions from this prohibition.

The data in mixed datasets containing health data can be a valuable source of information, e.g. for further medical research, for measuring the side effects of a prescribed medicine, for disease statistical purposes or for developing new healthcare services or treatments. However, the General Data Protection Regulation must be complied with when carrying out the initial processing operations and when carrying out further data processing operations. Therefore, any such processing of health data must have a valid legal basis[32] and an appropriate justification, be secure and provide for sufficient safeguards.

30 The Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation.

31 Development and operation of mobile health applications requires strict compliance with the General Data Protection Regulation rules. These requirements will be further specified in the Code of Conduct on privacy for mobile health applications, currently under preparation. For more information on the status of its development see: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

32 See Article 6(1) of the 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).

Finally, it is essential for individuals and companies to have legal certainty and trust in the processing of data. This is also vital for the data economy. The two Regulations ensure this and they both pursue the aim of not altering the free movement of data.

# 3 Free flow of data and the removal of data localisation requirements

This section explains the concepts of data localisation requirements under the Free Flow of Non-Personal Data Regulation and of the free movement principle in the General Data Protection Regulation in more detail. Although these provisions target the Member States, it can be informative for businesses to have a more accurate picture of how these two Regulations contribute to the free movement of all data within the EU.

## 3.1 Free flow of non-personal data

The Free Flow of Non-Personal Data Regulation[33] provides that 'data localisation requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality.'

**Data localisation requirements** are defined[34] 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.[35]'

The definition illustrates that the measures restricting the free movement of data within the EU 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. In addition, the prohibition of data localisation requirements covers both direct and indirect measures that would restrict the free movement of non-personal data.

**Direct data localisation requirements** may consist of, for example, 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).

**Indirect data localisation requirements**, which would hinder the processing of the non-personal data in any other Member State, can come in a variety of forms. They may include

---

33 Article 4(1) thereof

34 Article 3(5) of the 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.

35 Note that legal uncertainty about the extent of legitimate and illegitimate data localisation requirements further limits the choices available to market players and to the public sector on the location of data processing (see Recital 4 of the 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).

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[36,37].

The assessment of whether a specific measure represents an indirect data localisation requirement needs to consider the specific circumstances of each case.

The Free Flow of Non-Personal Data Regulation[38] refers to the concept of **public security** as outlined by the case law of the Court of Justice of the European Union. Public security 'covers both the internal and external security of a Member State[39], 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[40], 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.'

Additionally, any data localisation requirement justified by public security reasons must be proportional. In accordance with the Court of Justice of the European Union's case law, the principle of proportionality requires that the measures adopted are appropriate for ensuring that the pursued objective is met and do not go beyond what is necessary for that purpose[41].

For the sake of clarity, the prohibition of data localisation requirements is without prejudice to already existing restrictions laid down by EU law[42].

---

36 Recital 4 of the 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.

37 See two studies on data localisation requirements conducted prior the adoption of the Free Flow of Non-Personal Data Regulation: (1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market*, SMART number 2015/2016. Available online at: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 and (2) Time.lex, Spark Legal Network and Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*. SMART number 2015/0054. Available online at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

38 Recital 19 thereof

39 See for example the judgment of the Court of Justice of 23 November 2010, *Land Baden-Württemberg* v *Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, paragraph 43 and the judgment of 4 April 2017, *Sahar Fahimian* v *Bundesrepublik Deutschland*, C-544/15, ECLI:EU:C:2017:225, paragraph 39.

40 See for example the judgment of the Court of Justice of 22 December 2008, *Commission of the European Communities* v *Republic of Austria*, C-161/07, ECLI:EU:C:2008:759, paragraph 35 and case law referred to therein and the judgment of 26 March 2009, *Commission of the European Communities* v *Italian Republic*, C-326/07, ECLI:EC:C:2009:193, paragraph 70 and case law referred to therein.

41 See for example judgment of the Court of Justice of 8 July 2010, *Afton Chemical Limited* v *Secretary of State for Transport,* C-343/09, ECLI:EU:C:2010:419, paragraph 45 and also case law referred to therein.

42 See for example Article 245(2) of the Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, which provides that 'the Member States may require taxable persons established in their territory to notify them of the place of storage, if it is outside their territory'. This requirement needs however to be read in accordance with Article 249, which states that: 'where a taxable person stores invoices which he issues or receives by electronic means guaranteeing online access to the data and where the place of storage is in a Member State other than that in which he is established, the competent authorities in the Member State in which he is established shall, for the purposes of this Directive, have the right to access those invoices

Moreover, the Free Flow of Non-Personal Data Regulation does not impose any obligations on businesses or limit their contractual freedom to decide where their data are to be processed.

The Member States are required to make details of any data localisation requirement applicable in their territory publicly available on a **national online single information point** (national websites). They must keep this up-to-date or provide up-to-date details to a central information point established under another EU act.[43] For the convenience of businesses and to provide for their easy access to relevant information across the EU, the Commission will publish links to these information points on the Your Europe portal[44].

### 3.2 Free flow of personal data

The General Data Protection Regulation[45] provides that 'the free movement of personal data within the Union cannot be restricted nor prohibited for reasons connected with the protection of natural persons with regard to processing of personal data.'

If a Member State imposes localisation requirements on personal data for reasons other than the protection of personal data, they will have to be assessed against the provisions on the fundamental freedoms and the permitted grounds to derogate from those freedoms in the Treaty on the Functioning of the European Union[46,47] and relevant EU legislation, such as the Services Directive[48] and E-commerce Directive[49].

**Example:**

A national law requires that payroll accounts are located in a particular Member State for reasons related to regulatory control e.g. by the national tax authority. Such a national provision would fall outside the scope of Article 1(3) of the General Data Protection Regulation as the reasons are other than the protection of personal data. Instead, this requirement would have to be assessed against the provisions on fundamental freedoms and

---

by electronic means, to download and to use them, within the limits set by the rules of the Member State in which the taxable person is established and in so far as those authorities require for control purposes.'

43 Article 4(4) of the 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

44 https://europa.eu/youreurope/index.htm

45 Article 1(3) of the 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)

46 Consolidated version of Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47-390.

47 See also judgment of the Court of Justice of 19 June 2008, *Commission of the European Communities* v *Grand Duchy of Luxemburg*, C-319/06, ECLI:EU:C:2008:350, paragraphs 90-91: the Court considered that an obligation to keep available and retain certain documents in a particular Member State constitutes a restriction on the freedom to provide services; a justification that it is 'generally easier for the authorities to perform their supervisory tasks' is not sufficient.

48 Directive 2006/123/EC of the European Parliament and of the Council of 12December 2006 on services in the internal market, OJ L 376, 27.12.2006, p. 36-68.

49 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1-16.

the permitted grounds to derogate from those freedoms in the Treaty on the Functioning of the European Union.

The General Data Protection Regulation[50] recognises that Member States may impose conditions, including limitations, on the processing of genetic data, biometric data or health data. However, as stated in Recital 53 such national limitations should not hamper the free flow of personal data within the EU when these conditions apply to the cross-border processing of such data. This is in line with Article 16 of the Treaty on the Functioning of the European Union, which provides the legal basis for the adoption of rules relating to the right to the protection of personal data and the rules relating to the free movement of such data.

### 3.3 Scope of the Free Flow of Non-Personal Data Regulation

As already mentioned, the Free Flow of Non-Personal Data Regulation aims to ensure the free flow of non-personal data '<u>within the Union</u>'[51]. It therefore does not apply to processing operations taking place outside of the EU and to data localisation requirements relating to such processing[52,53].

The scope of the Regulation is, in accordance with Article 2(1), therefore limited to the processing of electronic non-personal data in the EU, which is:

(a) provided as a service to users residing or having an establishment in the EU, regardless of whether or not the service provider is established in the EU; or
(b) carried out by a natural or legal person residing or having an establishment in the EU for its own needs.

**Examples**:

Article 2(1)(a) of the Free Flow of Non-Personal Data Regulation:

- A cloud service provider established in the USA provides its processing services to customers residing or established in the EU. The cloud service provider administers its activities via servers located in the EU territory, where the data of its European customers are stored or otherwise processed. The cloud service provider does not have to own EU-based infrastructure, but can e.g. also rent server space in the EU. The Free Flow of Non-Personal Data Regulation applies to such data processing.

[50] Article 9(4) of the 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)

[51] See Article 1 of the 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.

[52] See Recital 15 of the 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.

[53] The term 'processing' is defined in broad terms (Article 3(2) of the 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) and, as underlined in Recital 17, the Regulation should apply to processing in the broadest sense, encompassing the use of all types of IT systems.

- A cloud service provider established in Japan offers its services to European customers. The processing capacities of the provider are located in Japan and all the processing activities take place there. The Free Flow of Non-Personal Data Regulation does not apply in this case, if all the processing activities take place outside of the EU[54].

Article 2(1)(b) of the Free Flow of Non-Personal Data Regulation:

- A small European start-up from Member State A decides to scale-up its business by opening an establishment in Member State B. To minimise costs, this start-up chooses to centralise the data storage and processing of the new establishment in its server that is located in Member State A. Member States may not forbid such IT-centralisation efforts, except when justified on the grounds of public security in compliance with the principle of proportionality.

Although the Free Flow of Non-Personal Data Regulation does not apply if all processing activities for non-personal data are carried out outside of the EU, the General Data Protection Regulation must be respected when personal data are part of the dataset. In particular, the rules for the transfers of personal data to third countries or international organisations under the General Data Protection Regulation must be complied with in any instance[55].

### 3.4 Activities relating to internal organisation of Member States

The Free Flow of Non-Personal Data Regulation does not oblige Member States to outsource the provision of services related to non-personal data that they wish to provide themselves or to organise them by means other than public contracts[56].

Article 2(3) second subparagraph of the Free Flow of Non-Personal Data Regulation states:

'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

---

[54] Note that the 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 does not concern data localisation requirements imposed by Member States on storing of non-personal data in third countries and these may be present in national legal orders. For the sake of clarity, the General Data Protection Regulation applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union (see Article 3(2) of the General Data Protection Regulation).

[55] In relation to transfers of personal data to third countries, consult the Commission's webpage: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en and the *Communication from the Commission to the European Parliament and the Council — Exchanging and Protecting Personal Data in a Globalised World*, COM/2017/07 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN. Regarding Japan, the Commission has adopted its adequacy decision on 23 January 2019, allowing personal data to flow freely between the two economies on the basis of strong protection guarantees.

[56] Recital 14 of the 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.

2014/24/EU[57] 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.'[58]

There may be legitimate interests that would warrant choosing this kind of 'self-provisioning' of data processing services, such as 'insourcing' or mutual arrangements between public administrations. Typical examples include the use of a 'government cloud' or a government engaging a centralised IT agency to provide data processing services for public institutions and bodies.

However, the Free Flow of Non-Personal Data Regulation encourages the Member States to consider the economic efficiency and other benefits of using external service providers[59,60]. As soon as the national authorities start 'outsourcing' the data processing with the contractual remuneration of private parties, and the processing takes place in the EU, such processing is covered by the Free Flow of Non-Personal Data Regulation, meaning that the principle of the free flow of non-personal data applies to general and administrative practices of the national authorities. Notably, they have to refrain from making data localisation restrictions, e.g. in tenders for public procurement[61].

# 4 Self-regulatory approaches supporting the free flow of data

Self-regulation contributes to innovation and trust among market players and has the potential to be more responsive to changes in the market. This section gives an overview of self-regulatory initiatives for the processing of both personal and non-personal data.

## 4.1 The porting of data and switching between cloud service providers

One of the purposes of the Free Flow of Non-Personal Regulation is to avoid vendor lock-in practices. These practices occur when users cannot switch between service providers because their data is 'locked' in the provider's system, for instance due to a specific data format or

---

57 Article 2(1)(4) of the 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. 65-242 provides that '"bodies governed by public law" means bodies that have all of the following characteristics: (a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; (b) they have legal personality; and (c) they are financed, for the most part, by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law.'

58 Recital 13 of the 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 points out that the Regulation is without prejudice to Directive 2014/24/EU.

59 Recital 14 of the 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.

60 An external service provider would be any entity, which is not a 'body governed by public law', as provided for in Article 2(1)(4) of the 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. 65-242.

61 Recital 13 of the 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.

contractual arrangements, and cannot be transferred outside of the vendor's IT system. Porting data without hindrance is important to allow users to choose freely between providers of data processing services and thus ensure effective competition in the market.

Data portability between businesses is becoming increasingly important across a wide range of digital industries including cloud services.

According to Article 6 of the Free Flow of Non-Personal Data Regulation, the Commission shall encourage and facilitate the development of self-regulatory codes of conduct at EU level ('codes of conduct') in order to contribute to a competitive data economy. It provides a basis for the industry to develop self-regulatory codes of conduct on the switching of service providers and the porting of data between different IT systems.

A number of aspects should be taken into account when developing such codes of conduct on the porting of data, notably:

- **best practices** for facilitating the switching of service providers and the porting of data in a structured, commonly used and machine-readable format;
- **minimum information requirements** to ensure that the professional users, before a contract is concluded, are provided with sufficiently detailed and clear information about the processes, technical requirements, timeframes and charges that apply in case a professional user wants to switch to another service provider or the porting of data back to its own IT systems;
- **approaches to certification schemes** for better comparability of cloud services; and
- **communication roadmaps** to raise awareness of the codes of conduct.

In the cloud services market, the Commission has started to facilitate the work of the Digital Single Market (DSM) cloud stakeholder working groups, which brings together cloud experts and professional users, including small and medium-sized enterprises. At this stage, one sub-group is developing self-regulatory codes of conduct on the porting of data and switching between cloud service providers (SWIPO working group), [62] and another sub-group working on developing cloud security certification (CSPCERT working group)[63].

The SWIPO working group is developing codes of conduct covering the whole spectrum of cloud services; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

The Commission expects the different codes of conduct to be complemented by **model contractual clauses**[64]. These will allow sufficient technical and legal specificity in the practical implementation and application of the codes of conduct, which will be of particular importance for small and medium-sized enterprises. The drafting of the model contractual

62 The Cloud Switching and Porting Data Working Group

63 The European Cloud Service Provider Certification Working Group. See also Section 4.3.

64 See Recital 30 of the 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.

clauses is planned after the development of the codes of conduct (which should be done by 29 November 2019).

In line with Article 8 of the Free Flow of Non-Personal Data Regulation, the Commission will evaluate the implementation of the Regulation by 29 November 2022. This will make it possible to assess: (i) the impact on the free flow of data in Europe; (ii) the application of the Regulation, especially to mixed datasets; (iii) the extent to which the Member States have effectively repealed existing unjustified data localisation restrictions; and (iv) the market effectiveness of codes of conduct in the area of porting of data and switching between cloud service providers.

The notion of portability and the interaction with the General Data Protection Regulation

Both Regulations[65] refer to data portability and the aim to make it easier to port data from one IT environment to another one, i.e. either to another provider's systems or to on-site systems. This prevents vendor lock-in and fosters competition between service providers. However, the Regulations differ in their approach to portability when it comes to the relationship between the targeted interest groups and the legal nature of the provisions.

The right to portability of personal data under Article 20 of the General Data Protection Regulation focuses on the relationship between the data subject and the controller. It concerns the right of the data subject to receive personal data which he or she has provided to the controller, in a structured, commonly used and machine-readable format, and to transmit those data to another controller or to their own storage capacities without hindrance from the controller to which the personal data have been provided[66]. Typically, the data subjects in this relationship are consumers of various online services that wish to switch between these service providers.

Article 6 of the Free Flow of Non-Personal Data Regulation does not provide for a right for professional users to port data, but has a self-regulatory approach, with voluntary codes of conduct for the industry. At the same time, it targets a situation where a professional user has outsourced the processing of its data to a third party offering a data processing service[67]. In accordance with Article 3(8) of the Free Flow of Non-Personal Data Regulation, a 'professional user' can include 'both natural and legal persons, including public authorities or

---

65 Article 6 of the 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 and Article 20 of the 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).

66 See Article 29 Working Party: *Guidelines on the right to data portability*. WP 242 rev.01, adopted on 13 December 2016 as last revised and adopted on 5 April 2017.

67 Recital 29 of the 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 states: 'Whereas individual consumers benefit from existing Union law [i.e. General Data Protection Regulation], the ability to switch between service providers is not facilitated for those users who act in the course of their business or professional activities.'

bodies governed by public law, using or requesting a data processing service for purposes related to their trade, business, craft, profession or task.'

In practice, the portability under Article 6 of the Free Flow of Non-Personal Data Regulation concerns business-to-business interactions between a professional user (which may in cases that include processing of personal data qualify as 'controller' in accordance with the General Data Protection Regulation) and a service provider (similarly, to be qualified in some cases as 'processor').

Despite the differences, situations may arise where the porting of data would be covered by both the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation in relation to mixed datasets.

**Example:**

A business using a cloud service decides to switch its cloud service provider and to port all the data to a new provider. The switching of the service provider and porting of the data is covered in the contract between the customer and the cloud service provider. If the old cloud service provider adheres to the codes of conduct developed under the Free Flow of Non-Personal Data Regulation, the porting of data has to take place in compliance with requirements specified therein.

If the personal data are also part of the ported datasets, the porting needs to comply with all the relevant provisions of the General Data Protection Regulation, in particular ensuring that the new cloud service provider complies with the applicable requirements, such as security[68].

**Example:**

In a case where a bank decides on changing its customer relationship management (CRM) provider, it is possible that some (personal and non-personal) data must be migrated from the old provider to the new one. This data will then be subject to different regulatory requirements, some stemming from the General Data Protection Regulation and other from the Free Flow of Non-Personal Data Regulation.

### 4.2 Codes of conduct and certification schemes on personal data protection

Codes of conduct and certification schemes may by be used to demonstrate compliance with the obligations under the General Data Protection Regulation (see Articles 24(3) and 28(5)).

In accordance with Article 40(1) and 42(1) of the General Data Protection Regulation, the Member States, the supervisory authorities, the European Data Protection Board and the

[68] See Article 29 Working Party: *Opinion 05/2012 on Cloud Computing* adopted 1 July 2012, WP196, which further specifies the position and obligations of cloud users and cloud service providers in relation to processing of personal data.

Commission should encourage the industry to develop codes of conduct and to establish data protection certification mechanisms.

Associations or other bodies representing a specific category of controllers or processors, may prepare a code of conduct for the specific sector. A draft of the code needs to be submitted to the respective competent supervisory authority for approval[69]. If the draft code of conduct relates to processing activities in several Member States, the supervisory authority must submit it to the European Data Protection Board before approving it. The Board will then give its opinion on whether the draft code complies with the General Data Protection Regulation.

The European Data Protection Board published its Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under the General Data Protection Regulation[70]. The guidelines include information on drawing up codes of conduct, criteria for their approval and other useful information. Similarly, the European Data Protection Board's Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the General Data Protection Regulation provide information on certification under this Regulation and the development and approval of certification criteria[71].

**Examples of codes of conduct developed by the cloud industry:**

**The EU Cloud Code of Conduct**, whose development was facilitated by the Commission, was drafted in collaboration with the Cloud Select Industry Group (C-SIG) on the basis of the Data Protection Directive[72] and subsequently the General Data Protection Regulation. The EU Cloud Code of Conduct covers the full spectrum of cloud services — Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[73].

**The Code of Conduct of the Cloud Infrastructure Services Providers in Europe (CISPE)**[74] focuses on IaaS providers. The CISPE Code of Conduct consists of requirements concerning the IaaS providers acting as data processors under the General Data Protection Regulation. It also sets out provisions on the governance structure for the implementation and application of the code.

---

69 See Articles 40(5) and 55 of the 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).

70 European Data Protection Board: *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, adopted on 12 February 2019, version for public consultation, available online at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

71 European Data Protection Board: *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*, adopted on 23 January 2019, available online at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

72 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data (date of end of validity: 24 May 2018).

73 For more information on the EU Cloud Code of Conduct see: https://eucoc.cloud/en/home.html

74 For more information on CISPE Code of Conduct see: https://cispe.cloud/code-of-conduct/

**The Cloud Security Alliance's Code of Conduct for GDPR Compliance** targets all interested stakeholders in cloud computing and the European personal data legislation, such as cloud service providers, cloud customers and potential customers, cloud auditors and cloud brokers. The code of conduct covers the full spectrum of cloud service providers[75].

### 4.3 Enhancing trust in cross-border data processing – certification of security

As stated in Recital 33 of the Free Flow of Non-Personal Data Regulation, 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. Along with the cybersecurity package proposed by the Commission in 2017[76], the CSPCERT working group is developing recommendations for the purposes of establishing a European Cloud Certification Scheme that will be presented to the Commission. Such a scheme has the potential to facilitate the free movement of data, enable a better comparability of cloud services and promote cloud uptake. The Commission may request (ENISA (the European Union Agency for Cybersecurity) to prepare a candidate scheme in accordance with the relevant provisions of the Cybersecurity Act[77]. Such scheme may address both personal and non-personal data. In addition to the Cybersecurity Act, and as highlighted in Section 4.2, the GDPR can also be used to demonstrate the existence of appropriate safeguards on data security[78].

## Final remarks

To have legal certainty and trust in the processing of data is essential for EU's ability to use data to its fullest potential, where value chains can develop across sectors and borders. The two Regulations ensure this and they both pursue the aim of the free movement of data. Together, the Free Flow of Non-Personal Data Regulation and the General Data Protection Regulation are building the foundation for the free flow of all data within the European Union and a highly competitive European data economy.

---

75 For more information on CSA Code of Conduct see: https://gdpr.cloudsecurityalliance.org/

76 For more information, see: https://ec.europa.eu/digital-single-market/en/cyber-security

77 Regulation of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

78 See Recital 74 of the Cybersecurity Act.