Basic information

2017/0228(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Free flow of non-personal data in the European Union **Subject** 1.20.09 Protection of privacy and data protection 2.40 Free movement of services, freedom to provide 2.80 Cooperation between administrations 3.30.06 Information and communication technologies, digital technologies 3.30.25 International information networks and society, internet	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
IMCO Internal Market and Consumer Protection	CORAZZA BILDT Anna Maria (PPE)	25/10/2017
	Shadow rapporteur SCHALDEMOSE Christel (S&D) DALTON Daniel (ECR) CHARANZOVÁ Dita (ALDE) REDA Felix (Verts/ALE) ZULLO Marco (EFDD)	

Committee for opinion	Rapporteur for opinion	Appointed
ITRE Industry, Research and Energy	KRASNODĘBSKI Zdzisław (ECR)	09/11/2017
JURI Legal Affairs	The committee decided not to give an opinion.	
LIBE Civil Liberties, Justice and Home Affairs	The committee decided not to give an opinion.	

Council of the European Union

Council configuration	Meetings	Date
Foreign Affairs	3647	2018-11-09
Transport, Telecommunications and Energy	3581	2017-12-04

European Commission	Commission DG: Communications Networks, Content and Technology — Commissioner: GABRIEL Mariya
European Economic and Social Committee	
European Committee of the Regions	

Key events

Date	Event	Reference	Summary
13/09/2017	Legislative proposal published	COM(2017)0495	Summary
23/10/2017	Committee referral announced in Parliament, 1st reading		
04/12/2017	Debate in Council		
04/06/2018	Vote in committee, 1st reading		
04/06/2018	Committee decision to open interinstitutional negotiations with report adopted in committee		
06/06/2018	Committee report tabled for plenary, 1st reading	A8-0201/2018	Summary
11/06/2018	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 72)		
13/06/2018	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 72)		
12/07/2018	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	PE639.846	
03/10/2018	Debate in Parliament		
04/10/2018	Decision by Parliament, 1st reading	T8-0381/2018	Summary
04/10/2018	Results of vote in Parliament		
09/11/2018	Act adopted by Council after Parliament's 1st reading		
14/11/2018	Final act signed		
14/11/2018	End of procedure in Parliament		
28/11/2018	Final act published in Official Journal		

Technical information

Procedure reference	2017/0228(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Legal basis	Treaty on the Functioning of the European Union TFEU 114
Other legal basis	Rules of Procedure EP 165

Mandatory consultation of other institutions	European Economic and Social Committee European Committee of the Regions
Stage reached in procedure	Procedure completed
Committee dossier	IMCO/8/11036

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE619.038	01/03/2018	
Amendments tabled in committee		PE619.414	09/04/2018	
Committee opinion	ITRE	PE613.537	26/04/2018	
Committee report tabled for plenary, 1st reading/single reading		A8-0201/2018	06/06/2018	Summary
Text adopted by Parliament, 1st reading/single reading		T8-0381/2018	04/10/2018	Summary
Text agreed during interinstitutional negotiations		PE639.846	24/07/2019	

Council of the EU

Document type	Reference	Date	Summary
Draft final act	00053/2018/LEX	14/11/2018	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2017)0495	13/09/2017	Summary
Document attached to the procedure	SWD(2017)0304	13/09/2017	
Document attached to the procedure	SWD(2017)0305	13/09/2017	
Commission response to text adopted in plenary	SP(2018)755	21/11/2018	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	ES_PARLIAMENT	COM(2017)0495	21/11/2017	
Contribution	PT_PARLIAMENT	COM(2017)0495	07/12/2017	
Reasoned opinion	FR_SENATE	PE615.357	12/12/2017	
Contribution	CZ_SENATE	COM(2017)0495	14/12/2017	
Contribution	DE_BUNDESRAT	COM(2017)0495	02/05/2018	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EESC	Economic and Social Committee: opinion, report	CES4820/2017	15/02/2018	

Additional information

Source	Document	Date
European Parliament	Briefing	
European Commission	EUR-Lex	

Final act

Regulation 2018/1807
OJ L 303 28.11.2018, p. 0059 Summary

Free flow of non-personal data in the European Union

2017/0228(COD) - 04/10/2018 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 520 votes to 81 with 6 abstentions a legislative resolution on the 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.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amended the Commission proposal as follows:

Purpose: the proposed Regulation aims to ensure the **free flow of data other than personal data within the Union** by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.

The expanding Internet of Things, artificial intelligence and machine learning, represent major sources of non-personal data. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines.

Principle of free movement of non-personal data: under the amended text, data localisation requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality.

The concept of 'public security', within the meaning of Article 52 TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety.

No later than **24 months** from the date of application of this Regulation, if a Member State considers that an existing measure containing a data localisation requirement can remain in force, it shall communicate that measure to the Commission, together with a justification for maintaining it in force.

Member States shall make the details of any data localisation requirements via a **national online single information point** which they shall keep up-to-date, or provide up-to-date details of any such localisation requirements to a central information point established under another Union act. The Commission shall publish the link(s) to such point(s) on its website, along with a regularly updated consolidated list of all data localisation requirements.

Data availability for competent authorities: access to data by competent authorities may not be refused on the basis that the data are processed in another Member State.

Where, after requesting access to a user's data, a competent authority does not obtain access and if no specific cooperation mechanism exists under Union law or international agreements to exchange data between competent authorities of different Member States, that competent authority may request assistance from a competent authority in another Member State.

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

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

- 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 professional users are provided, before a contract for data processing is concluded, with sufficiently detailed, clear and transparent information;
- approaches to certification schemes that facilitate the comparison of data processing products and services for professional users.

The Commission shall encourage suppliers to complete the development of codes of conduct no later than one year after the date of publication of the Regulation and to effectively implement them **no later than 18 months after the date of publication of the Regulation**. It should ensure that codes of conduct are developed in close cooperation with all stakeholders, including SME and start-ups associations, users and cloud service providers.
Mixed data: in the case of a mixed data set, i.e. a data set composed of both **personal and non-personal data**, the Regulation shall apply to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.

Review: no later than 4 years after the date of publication of the Regulation, the Commission shall submit a report evaluating the implementation of the Regulation, in particular as regards: (i) the application of the Regulation to data sets composed of both personal and non-personal data; (ii) the implementation by Member States of the public security exception; (iii) the development and effective implementation of codes of conduct.

Free flow of non-personal data in the European Union

2017/0228(COD) - 13/09/2017 - Legislative proposal

PURPOSE: to create a framework for the free flow of non-personal data in the European Union and the foundation for developing the data economy and enhancing the competitiveness of European industry.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: currently, data localisation restrictions by Member States' public authorities and obstacles to the movement of data across IT systems prevent business and organisations in the EU from capturing economic, social and business opportunities. Legal uncertainty and lack of trust cause additional barriers to the free flow of non-personal data.

In practice, this means a business may not be or feel free to make full use of cloud services, choose the most cost-effective locations for IT resources, switch between service providers or port its data back to their own IT systems.

With the principle of free flow of non-personal data, businesses can avoid duplication of data at several locations, may feel more confident to enter new markets, and scale up their activities more easily.

The Mid-Term Review on the implementation of the Digital Single Market Strategy (DSM Strategy) announced a legislative proposal on an EU free flow of data cooperation framework.

IMPACT ASSESSMENT: the preferred option chosen allows for the assessment of a combination of legislation establishing the free flow of data framework and the single points of contact and an expert group as well as self-regulatory measures addressing data porting. This option would ensure the **effective removal of existing unjustified localisation restrictions** and would effectively prevent the future ones, as a result of a clear legal principle combined with the review, notification and transparency, while at the same time enhancing legal certainty and trust in the market. The burden on Member States' public authorities would be modest, leading to approximately EUR 33 000 annually in terms of human resources cost to sustain the single points of contact as well as a yearly cost of between EUR 385 and EUR 1925 for the preparation of notifications

CONTENT: the proposed Regulation seeks to ensure the free movement of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and data porting for professional users.

It shall apply to the **storage or other processing of electronic data** other than personal data in the Union, which is (a) provided as a service to users residing or having an establishment in the Union, regardless of whether the provider is established or not in the Union or (b) carried out by a natural or legal person residing or having an establishment in the Union for its own needs.

The proposal:

- establishes the principle of free movement of **non-personal data** in the Union. This principle **prohibits any data localisation requirement**, unless it is justified on grounds of public security. Furthermore, it provides for the review of existing requirements, notification of remaining or new requirements to the Commission and transparency measures;
- ensures **data availability** for regulatory control by competent authorities. To this effect, users may not refuse to provide access to data to competent authorities on the basis that data is stored or otherwise processed in another Member State. Where a competent authority has exhausted all applicable means to obtain access to the data, that **competent authority may request the assistance** of an authority in another Member State, if no specific cooperation mechanism exists;

- states that the Commission shall encourage service providers and professional users to develop and implement **codes of conduct** detailing the information on data porting conditions (including technical and operational requirements) that providers should make available to their professional users in a sufficiently detailed, clear and transparent manner before a contract is concluded. The Commission will review the development and effective implementation of such codes within two years after the start of application of this Regulation;
- stipulates that each Member State shall designate a **single point of contact** who shall liaise with the points of contact of other Member States and the Commission regarding the application of this Regulation;
- provides for **procedural conditions** applicable to the assistance between competent authorities;
- states that the Commission shall be assisted by the **Free Flow of Data Committee** within the meaning of Regulation (EU) No 182/2011;
- calls for a **review** within five years after the start of application of the Regulation and that the Regulation will start to apply six months after the day of its publication.

BUDGETARY IMPLICATIONS: a moderate administrative burden for Member States' public authorities will emerge, caused by the allocation of human resources for the cooperation between Member States through the 'single points of contact', and for complying with the notification, review and transparency provisions.

Free flow of non-personal data in the European Union

2017/0228(COD) - 06/06/2018 - Committee report tabled for plenary, 1st reading/single reading

The Committee on the Internal Market and Consumer Protection adopted the report by Anna Maria CORAZZA BILDT (EPP, SE) on the 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.

As a reminder, the proposed Regulation seeks to ensure the free movement of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and data porting for professional users.

The committee recommended that the European Parliament’s position adopted at first reading under the ordinary legislative procedure should amend the Commission proposal as follows:

Principle of free movement of non-personal data: Members specified that data location requirements shall be **prohibited** unless, on an exceptional basis, and in compliance with the principle of proportionality, they are **justified on imperative grounds of public security**.

The concept of ‘imperative grounds of public security’ presupposes a threat to public security that is of a particularly high degree of seriousness. The amendment builds on the Treaty and the relevant case law of the Court of Justice to clarify the concept of public security and increase legal certainty.

Members wanted to introduce a **clear deadline** (no later than one year after the entry into force of the regulation) by which Member States must communicate the location requirements of the data they wish to maintain. The Commission shall examine the draft act within three months and decide whether or not the Member State concerned should amend or repeal the data location requirements. Any remaining data localisation requirements should be published on the Commission’s website to ensure easy accessibility of this information.

Scope: Members specified that **public sector authorities** and entities shall also benefit from the free movement of data. The Regulation shall apply to all levels of governance, including public procurement.

Mixed data sets: in the case of a mixed data set, namely a data set composed of both personal and non-personal data, the Regulation shall apply to the non-personal data of the data set. Where non-personal and personal data are inextricably linked, this Regulation should apply without prejudice to Regulation (EU) 2016/679.

Access to data for public authorities: the Commission's proposal provides that where a competent authority has exhausted all possible means of accessing data, it could request the assistance of an authority in another Member State if no specific cooperation mechanism exists. Members believe that such assistance could be requested **where a competent authority does not obtain access to the data** after contacting the user of the data processing service and where there is no specific cooperation mechanism under EU law or international agreements for the exchange of data between competent authorities of different Member States.

Members also pointed out that access to the premises where data is stored must be given in accordance with the national law of the Member State where the premises or equipment is located.

Codes of conduct: self-regulatory codes of conduct at EU level shall contribute to a competitive data economy, which are based on the principle of transparency and which establish guidelines on, *inter alia*, the following issues:

- **best practices** for facilitating the switching of providers and porting data in a structured, commonly used, interoperable and machine-readable format;
- **minimum information requirements** to ensure that professional users are provided with sufficiently detailed, clear and transparent information before a contract for data storage and processing is concluded.

The Commission shall encourage providers to effectively implement the codes of conduct by 24 months after the date of publication of this Regulation. It shall ensure that the codes of conduct are developed in **close cooperation with all relevant stakeholders**, including associations of small and medium-sized enterprises and start-ups, users and providers of cloud services.

Single point of contact: Members considered that the know-how of the single points of contact can be used not only as a link between the Member States and the Commission, but also to connect the institutions with users.

Review: no later than **3 years and 6 months** after the date of publication of the Regulation, the Commission shall submit a report evaluating the implementation of the Regulation, in particular as regards: (i) the application of the Regulation to mixed data sets; (ii) the implementation by Member States of the public security exception; (iii) the development and effective implementation of codes of conduct.

Free flow of non-personal data in the European Union

2017/0228(COD) - 28/11/2018 - Final act

PURPOSE: to remove obstacles to the free movement of non-personal data in the EU.

LEGISLATIVE ACT: Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union.

CONTENT: this Regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.

The new Regulation is designed to boost the data economy and the development of emerging technologies such as artificial intelligence, products and services related to the Internet of Things and autonomous systems and 5G that raise new legal issues regarding access to data and their reuse, liability, ethics and solidarity.

Principle of free movement of data within the Union

The Regulation prohibits restrictions related to the location of data imposed by Member States on the geographical location of the storage or processing of non-personal data, unless justified on grounds of public security.

Member States shall immediately communicate to the Commission any draft act introducing a new data localisation requirement or amending an existing data localisation requirement. By 30 May 2021 at the latest, any existing data localisation requirements shall be repealed.

Data availability for competent authorities

Competent authorities shall retain the power to request access to data for the performance of their official duties, in accordance with Union or national law. Access to data by the competent authorities may not be refused on the grounds that the data are processed in another Member State.

Where, after requesting access to a user's data, a competent authority does not obtain access and if no specific cooperation mechanism exists under Union law or international agreements to exchange data between competent authorities of different Member States, that competent authority may request assistance from a competent authority in another Member State.

Member States may impose effective, proportionate and dissuasive sanctions in the event of failure to provide data.

Codes of conduct

The Regulation encourages the development of codes of conduct to facilitate the procedure for users to switch providers and port data back to its own IT systems.

Codes of conduct shall be comprehensive and shall cover at least those aspects that are essential during the data porting process, such as (i) the processes used and location of data backups, (ii) the available data formats and supports, (iii) the required IT configuration and minimum network bandwidth, (iv) the time required prior to initiating the porting process and the length of time during which the data will remain available for porting, and (vi) data access guarantees in the event of the service provider going bankrupt.

The Commission shall encourage service providers to complete the development of codes of conduct by 29 November 2019 and to effectively implement them by 29 May 2020. It shall have to ensure that codes of conduct are developed in close cooperation with all stakeholders, including SME and start-ups and cloud service providers.

Mixed data

In the case of a mixed data set, i.e. a data set composed of both personal and non-personal data, the Regulation shall apply to the non-personal data part of the data set.

Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.

Each Member State shall have to designate a single contact point to liaise with the single contact points of the other Member States and the Commission regarding the application of the Regulation.

ENTRY INTO FORCE: 18.12.2018.

APPLICATION: from 18.6.2019.