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.