FREE FLOW OF NON-PERSONAL DATA

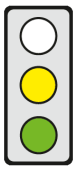
cep**PolicyBrief** No. 2017-33

Centrum für Europäische Politik

KEY ISSUES

Objective of the Regulation: The Commission wants to facilitate the free flow of non-personal data and promote competition between cloud providers and other data-processing services in the EU.

Affected parties: Providers of data storage and data-processing services; companies, authorities and private and professional users of such services.



Pro: (1) The general ban on national "data localisation restrictions" promotes cross-border competition which is likely to bring down the price of cloud services.

(2) Not giving professional users a statutory right to "data portability" is appropriate.

Contra: (1) It is disproportionate per se to prohibit Member States from relying on any justifying grounds other than "public security".

(2) It is also disproportionate that the Commission has selected a Regulation rather than a less stringent Directive as the legal form.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Proposal COM (2017) 495 of 13 September 2017 for a **Regulation on** a framework for **the free flow of non-personal data** in the European Union

Brief Summary

- **Context and objectives**
  - As part of its digital single market strategy [COM (2015) 192, see cep**PolicyBrief**], the Commission wants to realise the free flow of non-personal data in the EU and thus create a competition-based European data economy (p. 4).
  - The Regulation supplements the rules on personal data (see on this cep**Study**), inter alia the
    - General Data Protection Regulation (EU) 2016/679 ("GDPR'; see cep**PolicyBrief**) and
    - E-Privacy Directive 2002/58/EC, replaced where applicable by Regulation [COM (2017) 10, see cep**PolicyBrief**].
  - The Commission wants (p. 2 and 5, Recital 21)
    - to improve the free flow of non-personal data in the EU by removing "localisation restrictions" and to eliminate legal uncertainty,
    - to ensure that the regulatory and supervisory authorities have access to data for "regulatory control purposes" even where this data is stored in other Member States and
    - by encouraging self-regulation to make it easier for "professional users" of data storage and data-processing services to switch service providers and port data, thereby improving competition between such services.
- **Scope and definitions**
  - The Regulation applies to providers who supply storage and data processing services to users residing or having an establishment in the EU ("cloud providers") insofar as they process non-personal data. It is irrelevant whether the provider is established in the EU. (Art. 2 (1) (a))
  - The Regulation also applies where a natural or legal person residing or having an establishment in the EU stores or processes such data for its "own needs" (Art. 2 (1) (b)).
  - Non-personal "data" means data "other" than "personal data" pursuant to the GDPR (Art. 3 No. 1 in conjunction with Art. 4 (1) GDPR), i.e. all information which does not relate to an identified, or a directly or indirectly identifiable, natural person.
  - Examples of non-personal data are data from tax documents and company accounts or data gathered by industrial robots or sensors which does not relate to a person.
  - The Regulation applies to all data storage or processing whether carried out by the user or outsourced to a cloud provider (Recital 11).
- **Removal of "data localisation requirements" (DLR)**
  - The Regulation prohibits all "data localisation requirements" (DLR) unless they are "justified on grounds of public security" and proportionate (Art. 4 (1), Art. 5 TEU, Recital 12)).
  - DLRs are national legislative or administrative provisions which (Art. 3 No. 5)
    - require data to be stored or processed in the home Member State or
    - hinder the storage or processing of data in any other Member State such as by way of the obligation to use a local provider or to obtain an approval.

Authors: Dr. Anja Hoffmann, LL.M. Eur. and Philipp Eckhardt hoffmann@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-107 | www.cep.eu

– Within 18 months of publication of the Regulation, Member States must abolish all DLRs or provide the Commission with grounds to show which DLRs are justified and should therefore be maintained (Art. 4 (3), Art. 10 (2)).
– Member States can only base their justification on "public security" and not on any other grounds such as public order or health (Art. 4 (1) and Recital 12).
– They must notify the Commission of all drafts of new or amended DLRs (Art. 4 (2)).
– Each Member State must provide a website ("single information point") with the "details" of any applicable DLRs. The Commission will publish links to these sites. (Art. 4 (4) and (5))

- **Availability of data for competent authorities, assistance**
  – Regulatory and supervisory authorities that require access to the data for official purposes, retain their access rights. They must not be refused access on the basis that the data is stored or processed in another Member State. (Art. 5 (1), Recital 16)
  – Where the user of a cloud service, who is subject to obligations to provide data, fails to provide the authority with data or to allow it access, the following applies:
    - If EU law or an international agreement provides for a "specific cooperation instrument" for data sharing, the authority must use it (Art. 5 (4), Recital 18).
    - Where no "specific cooperation instrument" applies and the authority has exhausted "all applicable means", the competent authority in the country where storage is located must provide it with assistance, on request, unless this would be contrary to "public order" in the said country (Art. 5 (2), p. 5).
  – Member States must establish "single points of contact" that will take receipt of the requests for assistance from foreign authorities and pass them to the competent national authority (Art. 7 (1) - (4)).
- **Easier data transfer for "professional users"**
  – "Professional users" are all (Art. 3 No. 8)
    - natural or legal persons using a data storage or data processing service for their trade, business, craft, profession or task, and
    - public organisations that use these services to perform their duties.
  – The Commission encourages the development of EU-wide, self-regulatory codes of conduct for cloud services. Professional users of such services will (Art. 6 (1) (a) and (b))
    - be able to change provider more easily due to the development of "guidelines on best practices",
    - be informed, prior to concluding a contract, about the conditions for switching to another cloud provider or in order to port data back to their own IT systems ("portability"),
    - be able to compare the conditions of various providers more easily, such as the technical and operational requirements, processes, time limits, formats, fees and guarantees in the case of insolvency.
  – Cloud providers shall "effectively implement" the codes of conduct within 18 months of publication of the Regulation in the Official Journal of the EU, which will be checked by the Commission (Art. 6 (2) and (3)).

Main Changes to the Status Quo

- For the first time the principle of the free flow of data is applied, in legislation, to non-personal data. Until now, there have been no express EU rules on the free flow of data or the removal of DLRs.
- Member States can now only justify DLRs on grounds of public security. They can no longer rely on grounds such as public order or health.

Statement on Subsidiarity by the Commission

As the core problem is cross-border data mobility, the free movement of data and the internal market for the affected services cannot be achieved at national level.

Policy Context

The Commission announced an initiative for the free flow of non-personal data in its Strategy for the Digital Single Market [COM (2015) 192, p. 16 et seq., see cep**PolicyBrief**] and its Mid-Term Review [COM (2017) 228 final, p. 14] and in the Communication "Building a European Data Economy" [COM 2017(9), p. 8 et seq.].

Legislative Procedure

13 September 2017 Adoption by the Commission

Options for Influencing the Political Process

Directorates General:	DG Connect (Communications Networks, Content and Technology)
Committees of the European Parliament:	Internal Market (leading), Rapporteur: Anna Corazza Bildt, EVP
Federal Ministries:	Economic Affairs and Energy (BMWi) (leading)
Committees of the German Bundestag:	TBA
Decision-making mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

Formalities

Legislative competence:	Art. 114 TFEU (Internal Market)
Type of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Procedure:	Art. 294 TFEU (Ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

Nowadays, companies and authorities in the EU are forced to store and process their data in their home countries due to national DLRs. Providers from other EU countries are thus prevented from offering their services, from their own countries, to these companies and authorities. DLRs also lead to data in the EU not being stored and processed in locations where it would be most cost-effective and efficient to do so. DLRs can for example prevent data from being stored and processed in Member States in which the energy costs for operating the cloud server are low, such as Sweden, Finland or Greece. In the northern European Member States, storage and processing is often possible at lower costs due to the climatic conditions. In the case of DLRs in western European Member States, on the other hand, high wage costs arise, which make up a large proportion of the costs of these services, and would be much lower in an eastern European Member State.

The general ban on national DLRs – other than on grounds of public security – therefore strengthens the Digital Single Market, ensures a more efficient allocation of resources and **promotes cross-border competition which is likely to bring down the price of cloud services.**

The question of whether the Commission's approach will be successful, however, does not just depend on the requirements of this Regulation because not all barriers to the cross-border flow of data are statutory in nature. There is also a lack of confidence in data security and the protection of trade secrets in other EU countries. This confidence cannot be established solely by way of legislative measures but also requires confidence-building measures by the Member States and providers themselves.

Not giving professional users a statutory right, as against their cloud providers, **to have their non-personal data** – by contrast with personal data (Art. 20 GDPR) – **transferred to other providers or back to their own IT systems ("data portability")** is expressed by the fact that the industry is to impose self-regulatory codes of conduct. This **is appropriate.**

The lack of such a right certainly makes it more difficult for professional users to switch providers or to port data back to their own IT systems (lock-in effect). However, where the lack of a portability right is based on contractual agreements between user and provider, professional users do not require protection. Not only is it reasonable to expect such users to carry out legal checks prior to concluding the contract, competition between providers also prevents them from being able to force contractual provisions on their potential customers. Where the lack of data portability is due to technical reasons, a statutory right to portability is also of no help since it reduces the incentive to develop innovative services.

Legal Assessment

Legislative Competency

The Commission's basing of the Regulation on the competence to effect the approximation of laws in the internal market (Art. 114 TFEU) is justifiable. By removing obstructions (DLRs), the Regulation will create an effective single market for cloud services (p. 2 and 3).

Subsidiarity.

Unproblematic. The EU can regulate cross-border data mobility more effectively than the Member States.

Proportionality with Respect to Member States

The Regulation restricts the possibilities for Member States to justify DLRs by only recognising "public security" as grounds for justification. DLRs require justification because they restrict the freedom of establishment of cloud providers as well as their freedom to provide services. Until now, Member States have been able to rely on the protection of public order and health or on other overriding public interest objectives (cf. e.g. Art. 16 (1) (b) Services Directive [2006/123/EC], Art. 3 (4) E-Commerce Directive 2000/31/EC, Art. 49 et seq., 56 et seq. TFEU).

The proposed **restriction of the grounds for justifying DLRs to the protection of "public security" is generally lawful because it extends fundamental freedoms.** By participating in the legislative procedure via the Council, Member States can restrict their own scope for action (Müller-Graff in Streinz, EUV/AEUV, 2. Edn. 2012, Art. 49, para. 44). In relation to the Services Directive, the European Court of Justice (CJEU) has recognised that, when adopting secondary law which gives effect to a fundamental freedom enshrined in primary law, the EU legislator may restrict the grounds used to justify measures which are incompatible with the freedom. The aim of this is to rapidly and systematically remove restrictions which adversely affect the proper functioning of the internal market, which is consistent with primary law (Case C-593/13, para. 39 et seq.). Where a measure - e.g. for the protection of public order - is banned under secondary law, it cannot be justified on the basis of primary law as this would undermine harmonisation (para. 37).

It is however disproportionate to declare all motives for the adoption of DLRs, other than "public security", as illegitimate **per se** and thus at the outset **to prohibit Member States from relying,** in future, **on any other**

recognised **grounds for justification,** such as public order, health or other overriding public interest objectives**.** The Member States should, in principle, retain the right to require storage in their own country, in exceptional cases, for a legitimate interest, insofar as the relevant restriction of basic freedoms protecting this interest is proportionate. **The proportionality criterion represents a sufficient limitation on statutory exceptions**.

The duty of Member States to notify the Commission of all DLRs as early as the draft stage, creates transparency and helps to avoid protracted and complicated infringement proceedings. If - as recommended above - additional grounds to justify DLRs were permitted, Member States should then also be required to provide, in their "justification" for maintaining DLRs, sufficient information about the legitimate objective and proportionality of the DLRs.

The fact that, in future, in order to gain access to data, national authorities will, where applicable, have to rely on assistance from the country where storage is located, may lead to delays in access to data by authorities. In view of the advantages of having a choice of storage location, however, it is acceptable especially since the assistance provision only applies as an alternative and only involves limited red tape. The CJEU does not generally admit purely "administrative disadvantages" as justification (see e.g. Case C-386/04 -, para. 49, 51). **Clarification is required,** however**, as to whether authorities can also use the assistance** under this Regulation **if** existing **overriding cooperation mechanisms fail** or stall, **and how they can enforce access** where necessary. In addition, the term "data processing" should be defined.

It is disproportionate that the Commission has selected a Regulation as the legal form (Art. 5 (4) TEU). A Directive clearly regulating the principle of the free flow of data and the proposed obligations of the Member States would also provide sufficient legal certainty. These would then retain greater scope for discretion regarding implementation e.g. when creating administrative structures for assistance.

Compatibility with EU Law in other Respects

The definition of non-personal "data" as data "other" than personal data, means that overlaps with the GDPR are sensibly avoided. The boundary between personal and non-personal data can however be difficult in some cases especially since anonymised data can turn back into personal data if the data is later re-identified or linked up to other data. Clarification is required as to which rules apply to mixed data sets where some effort is required to separate personal data and non-personal data.

Impact on German Law

Germany must abolish all DLRs, contained in German legal or administrative provisions, within 18 months of publication of the Regulation or justify them to the Commission. It will be necessary to review inter alia bookkeeping and storage obligations under tax and commercial law insofar as they require consents or attach conditions to data storage in other countries, as in the case of e.g. Section 146 (2) Tax Code (AO), Section 14b (2) VAT Act (UStG) and Section 41 (1) Income Tax Act (EStG). The same applies to obligations to use local providers such as those under Art. 7 Bavarian Implementing Act relating to the Civil Status Act.

Conclusion

The general ban on national DLAs promotes cross-border competition which is likely to bring down the price of cloud services. Not giving professional users a statutory right to have their non-personal data transferred to other providers or back to their own IT systems ("data portability"), is appropriate. Restricting the grounds for justifying DLRs to the protection of "public security" is generally lawful because it extends fundamental freedoms. It is disproportionate to prohibit Member States from relying on any other justifying grounds. The proportionality criterion represents a sufficient limitation on statutory exceptions. Clarification is required as to whether authorities can also use assistance where overriding cooperation mechanisms fail. It is disproportionate that the Commission has selected a Regulation as the legal form.