A framework for the free flow of non-personal data in the EU [updated on 04/10/2018]

Brussels, 21 June 2018

Updated Questions and Answers (*)

What will change with the newly agreed Regulation?

Today, the European Parliament adopted the Regulation on the free flow of non-personal data, which follows the political agreement reached in June 2018 on a new principle that abolishes data localisation requirements while making sure that competent authorities can access data for the purposes of regulatory control. The Council will now adopt the proposal in the coming weeks and the Regulation will come in the force by the end of 2018. Once formally adopted, Member States will have 6 months to apply the new rules.

Why is the scope of the Regulation limited to non-personal data?

The new framework for the free movement of non-personal data complements existing legislation for personal data that entered into application on 25 May 2018. While ensuring a high level of protection for personal data, the General Data Protection Regulation (GDPR) already provides for the free movement and portability of personal data within the EU. The processing and storage of personal data falls under its scope and Member States may not impose data localisation restrictions on the grounds of protecting personal data.

The new framework for the free movement of non-personal data avoids duplication and ensures consistency with existing EU legal instruments. It seeks to provide the same free movement rules to the storage and processing of electronic data other than personal data in the EU. Together with the GDPR, the new measures will ensure a comprehensive and coherent approach to the free movement and portability of data in the EU.

The Commission will publish informative guidance on the interaction between the Regulation on the free flow of non-personal data and the General Data Protection Regulation, regarding the interaction of the both regulations in the context of mixed data sets.

Why is it necessary to remove barriers to non-personal data mobility?

Data-driven innovation is a key enabler of growth and jobs and has the potential to significantly boost European competitiveness in the global market. In order to make the most of the data economy, it is essential to enable data to flow across borders and to use data beyond national borders.

Removing data localisation restrictions is considered the most important factor for the data economy to unlock its full potential and grow by up to €739 billion in 2020, doubling its value to 4% of GDP[1].

Moreover, removing existing data localisation measures will drive down the costs of data services and provide companies greater flexibility in organising their data management and data analytics, while expanding their use and choice of providers. This could boost GDP by up to €8 billion per year[2].

What are the current obstacles to the free flow of non-personal data?

Currently, data localisation restrictions by Member States' public authorities and obstacles to the movement of data across IT systems (so-called "vendor lock-in" practices) prevent business and organisations in the EU from making the most of 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 able 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 its own IT systems. With the principle of free flow of non-personal data, businesses can avoid duplication of data at several locations, feel more confident to enter new markets, and scale up their activities more easily.

What concrete examples are there of data localisation restrictions?

Through studies, stakeholder discussions and public consultations, the Commission has identified numerous restrictions to the location of data for storage or processing. Data localisation restrictions

that either directly or indirectly restrict data mobility take different forms and exist in various sectors. For example:

- Supervisory authorities advising financial service providers to store their data locally;
- Professional secrecy rules (e.g. in the health sector) requiring local data storage or processing;
- Broad regulations requiring local storage of information generated by the public sector, whatever the sensitivity of the information.

While data localisation restrictions may be justified and proportionate in particular contexts (e.g. public security) there is a trend of unjustified data localisation requirements both in Europe and globally. This is often based on the misconception that localised services are 'by default' more secure than cross-border services.

Are data flows with non-EU countries also covered?

No, the Regulation covers data mobility within the EU only.

In what cases will competent authorities get access to data stored in another EU Member State?

The Regulation ensures that **competent authorities have access to data** stored or processed in another Member State in order to be able to perform their tasks in line with their regulatory mandate, just as they do when the data is stored in their own territory. As a matter of principle, the storage or other processing of data abroad may not be used as a ground to refuse access to data to national regulators. Such access will have to be allowed in cases **where a national regulator is legally empowered** to request it from a particular holder of the data, and where it is necessary for the performance of official duties of the regulator.

If a regulator does not obtain access to data directly from the holder of the data, it could rely on an existing specific cooperation mechanism to ask for assistance from another Member State. If no specific cooperation mechanism applies or exists, the new Regulation provides for a default cooperation mechanism between competent authorities. When strictly necessary, interim measures may also be imposed on users that abuse the free flow of data and do not provide the data to the regulatory authority. If such interim measures require re-localising the data for longer than 180 days, its compatibility with Union law will have to be accessed by the Commission.

The Regulation also establishes a **single point of contact** per Member State to liaise with other Member States' contact points and the Commission to ensure the effective application of these new rules on the free flow of non-personal data.

How will the Regulation make it easier to switch data service providers and what are the benefits of easier switching?

The Commission will encourage and facilitate the development of self-regulatory codes of conduct to facilitate the switching of providers. The Regulation sets out specific requirements for the codes. For example, users will have to be informed about the terms and conditions under which they can port data outside their IT environments. The Codes should also reflect best practices regarding the processes, technical requirements, timeframes and charges that may apply in the event of switching providers.

Stakeholders engaged in the self-regulatory process will have to present plans on awareness raising of the codes of conduct. In four years' time, the Commission will review the implementation of the codes of conduct. If the Commission deems that there has been insufficient progress, it may propose additional measures.

The ability to port data without hindrance and the transparency of applicable terms and conditions are key facilitators of an informed user choice of cloud services and effective competition on markets for data processing. They are expected to boost the confidence of professional users in taking up cross-border offers and hence their confidence in the internal market.

How will this Regulation affect EU citizens?

The Regulation on free flow of non-personal data covers data other than personal data. For that reason, it primarily affects businesses and business and public sector users of data storage and processing services, and individuals acting in a professional capacity. The Regulation on the free flow of non-personal data is one of a series of proposals in the Digital Single Market strategy. Other proposals may affect citizens more directly. For example, digital contract rules enhance the rights of consumers to terminate contracts with digital content suppliers, such as cloud service providers, or to retrieve personal data that is processed by digital content suppliers. To avoid overlap with this and other EU instruments, the Regulation on the free flow of non-personal data does not cover citizens directly. However, citizens are expected to benefit indirectly from this Regulation through a more competitive

and open single market for data storage and processing services in the EU.

How will the Regulation affect the public sector?

This Regulation is about freedom of choice, for businesses, but also for the public sector. It explicitly states that public authorities, just like businesses or other professional users, are not forced to outsource data to cloud service providers. Also it is made clear that the Regulation does not apply to the internal organisation of data processing among public authorities and bodies without contractual remuneration of private parties.

Conversely, the Regulation prohibits administrative provisions (such as regulatory guidelines) imposing data localisation requirements in the field of public procurement. This means that, when framing cloud procurement policies and practices, public authorities should refrain from requiring the localisation of data processing on their own territory, except when clearly justified for reasons of public security.

What will be the impact on the security of data?

The new Regulation clarifies that all security requirements that currently apply to businesses and public administrations will continue to apply when these bodies choose to store or process data in another Member State or to use cloud services. Accordingly, the Regulation makes businesses more aware of their responsibilities regarding the security of data storage and processing in cross-border contexts.

The new measures rely on the implementation mechanisms provided in the Directive on security of network and information systems (NIS Directive) to enhance the cyber resilience of cross-border data storage and processing. Along with this Regulation, the Commission has proposed to scale up the EU's response to cyberattacks by presenting a new cybersecurity framework to better anticipate, respond, and counter cyber threats. This includes the proposal for a new European cybersecurity certification framework. The future development of certification schemes for the cloud under such a framework will eventually support cross-border supply and demand of cloud and other data services, and make the system much more trustworthy, thus stimulating the take-up of cloud services by European businesses.

What has the Commission done to support the EU data economy?

In 2014, in the Communication on "Towards a thriving data-driven economy", the Commission proposed measures to accelerate the transition towards a data-driven economy, in particular to develop an EU-wide data ecosystem and promote data-driven innovation. Tackling obstacles to the free flow of non-personal data is also one of the key actions announced in the mid-term review of the Digital Single Market strategy.

This Regulation complements the measures for building a European Data Economy launched in January 2017, in which the Commission aimed to foster the best possible use of the potential of digital data to benefit the economy and society; it assessed the barriers to the free movement of data and other emerging challenges to the European data economy.

Furthermore, the Regulation builds upon the Digitising European Industry package of April 2016, which included the European Cloud Initiative for a high-capacity cloud solution for storing, sharing and re-using scientific data. It also draws upon the revision of the European Interoperability Framework for a better digital collaboration between public administrations in Europe.

To further complement the common European data space, the Commission published additional proposals to boost the European data economy on 25 April 2018, comprising the review of the Public Sector Information Directive, guidance on business-to-business data sharing, Artificial Intelligence, liability of data-based services, and the dissemination of scientific information.

For More Information

Press release: political agreement on free flow of non-personal data

Joint Statement after the European Parliament vote on 4 October 2018

(*) : This Q&A is an updated version of MEMO/17/3191 published on 19/09/2017 and MEMO/18/4249 published on 21/6/2018.

[1] IDC 2017, European Data Market Study, Final Report.

[2] ECIPE 2016, Policy Brief "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States".

MEMO/18/4249

Press contacts:

Nathalie VANDYSTADT (+32 2 296 70 83)
Joseph WALDSTEIN (+ 32 2 29 56184)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email