FEDIL

Position

POSITION OF FEDIL – FREE FLOW OF DATA

This position paper constitutes FEDIL's contribution to 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 ("Free Flow of Data"), published on 19th September 2017.

The Commission's work on free flow of data is part of the intended actions listed in the Digital Single Market strategy of May 2015 and was announced in January 2017, with the adoption of the Communication on "Building a European Data Economy".

CONTEXT

In the digital age, data has become a vital resource and represents a serious potential for Europe's future growth, jobs and competitiveness at a global level. Building a strong data economy enables the development of key technologies (Internet of Things, Artificial Intelligence, Industrial Internet) and helps our economy and society face the challenges of a fast-changing world.

According to a study[1] supported by the European Union, appropriate conditions for data mobility could generate up to 4% of GDP growth. Data economy could be worth around EUR 106 billion by 2020. These findings demonstrate how cross-border data mobility will become decisive for businesses of all sizes, sectors and origins.

In Luxembourg, given the significant investments in data centres (Tier IV) and high-performance computing, but also in start-ups and new business models (e.g. FinTech, smart mobility and BioHealth), restrictions to the free flow of non-personal data are particularly harmful. Disproportionate requirements for data localisation and restrictions on data access are introduced by Member States for regulatory scrutiny purposes or by lack of trust and legal certainty when storing or processing data. Such national measures are substantial barriers to innovation and the development of applications for big data, connected devices or cloud computing.

These elements illustrate the importance of the Commission's initiative to remove the major artificial barrier in the European Single Market not only for Luxembourg, but for all Members States.

General comments

Whether offline or online, Luxembourg's industry has always been in favour of

an integrated, borderless internal market. It represents the best way to enhance the competitiveness of the European economy.

In this context, FEDIL strongly welcomes the Commission's ambitious proposal and notably the introduction of the **principle of free movement of non-personal data**, which will constitute an important step towards completing the internal market.

Only a regulatory framework will ensure a harmonised, coherent application of the new freedom throughout the Union and increase trust processing and storing services by offering legal certainty.

Specific comments

The definition of non-personal data

The proposed regulation defines non-personal data as "*data other than personal data*"[2], providing a reverse definition with respect to the General Data Protection Regulation's definition which describes it as "*any information relating to an identified or identifiable natural person* "[3].

Indeed, an exclusive definition allows a clear distinction between personal and non-personal data and helps avoiding any confusion regarding the applicable rules to the respective data. In this respect, recital (9) perfectly affirms that the GDPR won't be affected by the proposed regulation on the free flow of data.

However, **a more comprehensive definition of non-personal data** would be appropriate in order to know how far pseudonymised or anonymised data will fit into one or the other interpretation.

Mixed data sets

Even though the scope of the proposal is distinctly limited to *"the storage or other processing of electronic data other than personal data in the Union"*[4], the European Commission missed an opportunity to clarify how mixed data sets, combining both personal and non-personal data, should be analysed.

Since unbundling mixed data sets is a complex and costly process, our members would prefer **an open and flexible approach**, where businesses are free to choose whether they perform such an operation or not. Likewise, the proposed regulation should not impose a separate storage for different types of data. SMEs and start-ups in particular should be able to decide if they can deploy considerable efforts and invest in the identification of non-personal data within the mixed set and if it is rentable to apply both sets of rules accordingly.

In any case, if data is inextricably linked, the proposal on free flow of data should not prejudice the application of the GDPR. It would therefore be reasonable to apply the GDPR to the whole data set. All the more so as the industry will already have adapted to the implementation of the GDPR.

The public security Exception

With the principle of free movement of non-personal data enshrined in a regulation, data localisation measures and restrictions to access data will have to be justified by public security needs[5]. This exception should remain **isolated**. Allowing further exceptions would prevent the proposal to be effective and coherent.

When invoking the public security exception, Member States have to duly

prove that the measures taken are proportional to the aim pursued. More precisely, they will have to demonstrate that the restriction of the free flow of non-personal data is necessary and that no less restrictive measure is available to ensure national security. In this context, the Parliament's Committee on the Internal Market and Consumer Protection (IMCO) confirms that *"data localisation requirements shall be prohibited unless, on an exceptional basis, they are justified on imperative grounds of public security, in compliance with the principle of proportionality*".

Member States, estimating that many scenarios fall under public security, may overuse or use the exception wrongly. **A more explicit definition** of public security is of great interest to our businesses in order to avoid a broad interpretation of the exception, which would deprive the proposal of its full effect.

In line with the GDPR, a potential definition could limit public security to a restriction that *"respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"*[6].

Furthermore, the proposal should state that Member States can put forward this justification only where restrictive security requirements apply on data which is processed or stored within their respective national territory. Opening the possibility for Member States to invoke public security when data has originally been sourced within their borders would increase administrative burdens and legal uncertainty.

Notification and publication requirements

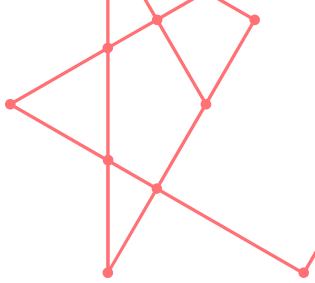
We welcome the proposal's demand for transparency on two levels and the obligation to abolish every existing, unjustified requirement for locating data within 12 months of its application.

First, the notification procedure will oblige Member States to notify all existing and newly introduced data localisation requirements. The Commission will be able to verify if the principle of proportionality is respected.

Nevertheless, to be truly effective, its competence to decide whether national measures are compliant with the fundamental right of free movement of data, should be set out the proposal. For instance, by adding recital (14) to the article 4, laying out that *"these notifications should enable the Commission to assess the compliance of any remaining data localisation requirements".* In this respect, we also support IMCO's proposed procedure, ensuring that *"without prejudice to Article 258 TFEU, the Commission shall, within a period of three months from the date of receipt of such communication, examine the compliance of that measure with paragraph 1 and shall, where appropriate, adopt a decision requesting the Member State in question to amend or repeal the measure".*

Second, Member States will have to publish details of any data localisation requirements applicable in their territory, online and via a single information point. Yet, along with a Union level publication, adapted to the future Single Digital Gateway, great efficiency could be reached. As noted in the IMCO draft report, *"a consolidated list of all data localisation requirements in force in every Member State would make the information more accessible, especially for SMEs".*

These provisions will usefully deter Member States from imposing unjustified



or disproportionate requirements and provide an accurate picture of the Digital Single Market.

Data portability

FEDIL encourages the development of self-regulatory codes of conduct providing information portability conditions at Union level. It is paramount for service providers to have guidelines, gathering best practices on transmission of data and switching of providers.

We also believe that such information, if sufficiently detailed, clear, transparent and provided prior to the signing of a data storage and processing contract, will make it easier for professional users to transfer their data.

However, the **principle of interoperability** should be the key concept of data portability and the industry is best placed to decide how interoperability is achieved as well as how the self-regulation should be formulated.

Furthermore, these codes of conduct have to be drawn as quickly as possible in order to be set up as soon as the text enters into force and be based on existing, non-binding but commonly accepted international standards and benchmarks (e.g. ISO27001), which already guarantee a high level of quality and reliability of products and services to users.

FOOTNOTES

1. Deloitte in {https://ec.europa.eu/digital-single-market/en/news/measuring-economic-impact-cloud-computing-europe}
2. Article 3.1 of the proposed regulation
3. Article 4.1 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)
4. Article 2.1 of the proposed regulation
5. Article 4.1 of the proposed regulation
6. Article 23.1 d) of the GDPR