Free Flow of Data

The European Commission's proposal for a Regulation on a framework for the free flow of non-personal data in the EU, published in September 2017, prohibits national governments from creating unjustified data localisation rules.

- **Key elements of the Regulation**

1. Obligations on national governments not to restrict movements of data

This Regulation enshrines the principle of the free movement of data into EU law, with clear obligations on national governments not to restrict the location, storage or processing of non-personal data in any specific territory, unless justified on grounds of public security.

2. Repeal of existing unjustified data localisation rules

EU Member States must repeal all data localisation requirements which are not justified by public security reasons within a year from the adoption of this Regulation.

3. Notification and transparency procedure

Any new data localisation requirement justified on public security grounds must be notified to the European Commission. Details of all approved data localisation rules must be made publicly available.

4. Access to data for purposes of regulatory control

Public authorities should be able to access data stored in a different Member States for regulatory purposes.

5. Portability of data between Cloud services

Industry is encouraged to draft self-regulatory codes of conduct on data portability and best practices to facilitate the switching of Cloud providers.

- **Detailed provisions and position**

Article 1 – Subject matter

Importantly, this article introduces the principle of the free movement of data within the European Union. Specifically, it lays down "rules for data localisation requirements, the availability of data to competent authorities, contractual transparency for data porting and security of data storage and processing."

Article 2 – Scope

The Regulation applies to national localisation measures that are based on reasons other than the protection of personal data (i.e. data flows that are not regulated by the

GDPR, which already prohibits restrictions on the processing of personal data if those are based on reasons of privacy protection). The complementary nature of this Regulation to the GDPR is explained in Recital 10.

Nevertheless, it must be kept in mind that if this Regulation addresses the storage and processing of non-personal data, the GDPR only addresses the processing of personal data, not its storage. As such, national governments may still be able to force the localisation or personal data in a specific territory.

Art.2.2 states that the Regulation "does not apply to an activity that falls outside the scope of Union law."

If at first this provision seems normal, it may leave Member States room for manoeuvre to adopt data localisation measures in policy areas where the European Union does not have competence. As this is unclear, we may want to ask for the deletion of this provision Art.2.2.

Article 3 – Definitions

The Regulation covers any data other than personal data as covered by the GDPR, any type of electronic storage, and any type of processing service unless merely ancillary to a different service (as explained in Recital 11). The Regulation covers all users and service providers who are using or providing such data services.

Regarding the definitions of "drafts act" in Art. 3.3 and "data localisation requirement" in Art.3.5, if these definitions seem quite exhaustive and do cover "administrative provisions", public procurement is not mentioned and it is not clear if public procurement rules are understood as "administrative provisions". Recital 4 doesn't mention public procurement either, although it describes administrative practices mandating data localisation or the use of locally certified technologies which limit the choices available to the public sector. We should ask for a clarification that public procurement rules are explicitly mentioned in the text of the Regulation.

Article 4 - Free movement of data across borders within the Union

The text in Art.5.1 prohibits measures which require that data be either stored/further processed in a specific territory or which prevent storage/further processing in a territory, unless justified on grounds of public security (this is the only exception to the rule).

The text does not include a definition of "public security". Recital 12 refers to public security as defined by Union law, in particular Art.52 of the Treaty on the Functioning of the EU, but this article does not provide a definition of public security either. Even though having an exception limited to national security echoes our asks, a definition of public security would still be helpful so that it doesn't lead to a broad interpretation of what data localisation measures could be justified on public security grounds.

According to Art.5.2 and Recital 13, Member States will have to notify the Commission of any draft act which introduces a new data localisation requirement or makes changes to an existing data localisation requirement, using the procedures from the Transparency Directive 2015/1535.

If the procedures under the Transparency Directive do include back and forth communications between Member States and the Commission on the validity of draft rules, it is not clear what powers the Commission actually has to block a draft act which it would consider to be unjustified. We need to assess the functioning of these procedures and the competences of the Commission in practice since, in the case of data localisation, a notification procedure should be extremely robust and give clear blocking powers to the Commission in order to be effective.

According to Art.5.3 and Recital 14, Member States must carry out a review of existing data localisation requirements and notify the Commission those that they consider being justified and compliant with this Regulation, within a year of the proposed Regulation coming into force. Finally, Member States will have to create "Single Information Points" where the public can access all the information about lawful data localisation requirements. The Commission will also make this information public on its websites.

We fully support transparency obligations on Member States regarding justified data localisation measures.

Article 5 - Data availability for regulatory control by competent authorities

The Regulation does not affect the powers of competent authorities to request and receive data from providers of data storage / processing services. Such users cannot refuse to provide access to data to competent authorities on the basis that data is stored and/or further processed in another Member State. Recital 18 provides more details on existing cooperation mechanisms Member States can use in order to obtain access to data for purposes of regulatory control, but in case data cannot be obtained through these mechanisms Member States should cooperate through the points of contact and the related procedures created by this Regulation's Art. 7.

If the philosophy behind this article is to make sure that national authorities can carry out their duties as if the data was stored on their territory (so that, for example, tax authorities from Country A can have access to documents stored in country B for an audit), we should still have to make sure that the scope of this provision is not broadened beyond access for regulatory control, and include unreasonable measures on government access to data for example.

Article 6 - Porting of data

It is positive that the Commission has abandoned the idea of a mandatory right to portability following its impact assessment, judging it to be too burdensome for service

providers. The draft Regulation instead states that the Commission should facilitate the development of self-regulatory codes of conduct with industry, in order to define guidelines on best practises in facilitating switching of providers (and providing information to customers on the processes, technical requirements, timeframes and charges, and operational requirements to port data).

We support the view that portability would be best ensured via industry-led initiatives and discussions and not via mandatory rules, thus codes of conduct at least seem like a more suitable approach. Discussions in Council and Parliament will be key on this issue, as there is a risk to see this potentially turned into more binding provisions such as standard contractual terms. It should also be noted that, according to Recital 21, the Commission can adopt implementing measures if it feels that the proposed codes are not sufficient.

Articles 7 and 8 – Single points of contacts and the EU Free Flow of Data Policy Group

Linked to Articles 4 (transparency) and 5 (access by public authorities), Member States must establish Single points of contact which will act as online information points on data localisation requirements. These will also be responsible for coordinating the application of the Regulation in the Member State (in particular regarding access to data stored in another Member State, for regulatory purposes), and coordinate with contact points of other Member States and the Commission. The proposal also establishes the EU Free Flow of Data Policy Group, composed of the single points of contact. The group will advise and assist the Commission on the application of the Regulation.

Other aspects

- The legal instrument is a Regulation, directly applicable in the Member States six months after publication.

- The text does not include any rules on the other "data emerging issues" such as data ownership, access and transfer.

- On the security of data transfers and storage, the recitals refer to the continued applicability of existing national rules to data transfer and storage to another country and to the implementation of the NIS Directive and the rules for digital service providers in particular.

We support these three key elements:
- the instrument should remain a Regulation,
- the text should keep its focus on data localisation and not include issues such as data ownership or access to data,
- there is no need for new security requirements, which would overlap with existing rules and NIS provisions on digital service providers.

- **High Level Messages**

- We have actively supported the European Commission's objective to put forward binding rules preventing national governments from creating localisation rules for non-personal data. Data localisation measures are an obstacle to free trade, and are contrary to the EU Single Market principles. Eliminating data localisation is beneficial to all companies trying to scale up and do cross-border trade. Also, this is a necessary complement to the movement of personal data allowed by the General Data Protection Regulation.
- We welcome the European Commission's proposal, which echoes our request for a ban on unjustified data localisation measures in Europe.
- As the proposal is now in the hands of co-legislators (European Parliament and national governments), we hope that the scope of exceptions will not be broadened beyond public security.
- The Regulation needs strong monitoring and enforcement mechanisms to ensure it effectively abolishes unjustified data localisation measures in the EU.
- We welcome the encouragement to industry to develop codes of conduct on portability conditions.