November 2017

ETNOs Views on the Proposed Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union

The European Commission proposed on 13 September 2017 a draft regulation with the aim of facilitating the cross-border provision of data storage and processing services such as cloud computing, big data analytics and the Internet of Things (IoT) within the European Union. The Commission considers this policy initiative a central pillar of its Digital Single Market Strategy.

As a matter of fact, **companies need efficient mechanisms to transfer both personal and non-personal data across borders**, in order to respond to customers' needs in a data-driven economy. Data location restrictions for non-personal data should only be allowed if they are supported by objective, proportionate and justified reasons of public security. In addition, the protection of the fundamental rights of the individual must be guaranteed in the context of promoting free data flows outside the European Union.

Key Messages

- ETNO **welcomes the Commission's goal** of speeding up the removal of national barriers to the circulation of non-personal data within the EU borders.
- ETNO welcomes the proposal's **general consistency with other relevant legislation** in this field, but cautions against **possible conflicts with the scope of application of the General Data Protection Regulation (GDPR)**.
- ETNO asks for an improved wording of the obligation regarding **data availability for competent authorities (Article 5)**. In particular, it should be made clear that cloud service providers should not be directly addressed by competent authorities from all the EU Member States.
- In regard to the **porting of data (Article 6)**, ETNO considers that the Commission has **not provided the required evidence to sufficiently demonstrate a market failure** due to lock-in effects affecting non-personal data in the business-to-business (B2B) market. The promotion of **self-regulatory measures** should be developed without imposing additional burdens in the European market and taking into account that the provision of portability represents for some undertakings a differentiator in competitive markets.

Consistency with Existing Regulation

ETNO appreciates that the proposed regulation ensures **consistency with existing legal instruments** such as the eCommerce Directive, the Services Directive, and the Transparency Directive. This will allow Commission's and Member States' to scrutinise any draft national measure that would have a negative impact in the well-functioning of the Internal Market.

Moreover, we welcome that **the scope of the proposal is clearly limited to non-personal data**, since the regulation should not override or interfere with the provisions of the General Data Protection Regulation related to the principle of the free flow of personal data, which is treated separately.

Data Availability for Competent Authorities

Article 5 describes the coordination mechanisms for Member States to ensure that competent authorities maintain access to data even if data are stored in another Member State. This is based on the procedure laid down in **Article 7**, which establishes **"single points of contacts"** that should be used for this purpose by the authorities that are in charge of assisting the request of the issuing Member State. In case a competent authority of one Member State requires access to data stored in another Member State, the former will require the assistance of the latter through the single point of contact.

The mechanism to ensure data availability for competent authorities is of outmost importance for ensuring the success of the future Regulation and a well-working free flow of data, as Member States need to be sure that their public authorities will be allowed to access data regardless of the location of this data in the EU. This equally applies to service providers, which need clear rules on how to handle data access requests by public authorities.

In this regard, it is unclear if, in parallel with the initial procedure, **Article 5(3)** describes another mechanism whereby a cloud provider could receive data access requests directly from authorities of another EU Member State, possibly according to their own national law. This would introduce a level of complexity and legal uncertainty, in terms of assessment of the legitimacy of a given request, that the industry cannot cope with. Therefore, an improved wording is necessary to clarify that **under no circumstances cloud service providers should be compelled to directly answer requests coming from competent authorities of all the EU Member States**.

Porting of Data for B2B

Article 6 of the proposal introduces a **self-regulatory approach to non-personal data portability in the B2B context**, meaning that the Commission's role would be to facilitate and monitor industry-led initiatives such as EU-wide **Codes of Conduct (CoC)** in order to define guidelines on best practices to facilitate switching between providers and to ensure that

relevant and transparent information is provided regarding processes, technical and operational requirements or timeframes for the porting of data.

ETNO welcomes that the proposal avoids the introduction of mandatory regulation and thus new rules for B2B contracts, as **no serious switching and lock-in effects leading to market failure and justifying strict regulation have been identified**. It should also be noted that, even in cases of market failure, mandatory (*ex ante*) regulation would not represent the only and unavoidable instrument. Instruments offered by competition policy on a case-by-case basis should rather be considered to address potential anti-competitive behaviours.

In addition, ETNO reminds that B2B contracts are negotiated between well-informed organisations that suffer from fewer information asymmetries than consumers in the business-to-consumer (B2C) market. Contrary to the right to data portability introduced by the GDPR or the rules on data retrieval included in the draft Digital Content Directive, this regulation covers business customers; therefore, **contractual freedom is a key principle that should be preserved**. Commercial agreements must not be unduly constrained and should remain flexible to favour innovation and foster the European economy.

Data portability needs to be understood as a right for the individual (data subject) to allow an easy switching of the subject's personal data from one service to another. Therefore, data portability is an enhanced right to access personal data, as clearly recognised by the GDPR. However, for the above-mentioned reasons, it is not appropriate to translate a personal data portability right into an equivalent right for the individual when non-personal data are concerned.

A general portability right for non-personal data would be detrimental to the data economy, as it would unnecessarily tighten the market, depriving the competitive dynamics from the flexibility needed to flourish. Portability of non-personal data should be the result of voluntary agreements and a free, competitive process. The underlying principle of freedom of contract needs to be guaranteed.

Accordingly, CoCs developed by industry players may be a flexible tool that allows for the identification of solutions to facilitate non-personal data portability for businesses, avoiding additional burdens in the EU markets. However, any binding or self-regulatory measures for the porting of non-personal data in the B2B context could also result in a **problematic interplay with the right to portability of personal data under Article 20 GDPR** (e.g. regarding business customers that are not considered legal entities). Whereas data controllers should be encouraged to develop interoperable formats that enable data portability under the GDPR, this should not create any far-reaching obligation for the controllers to adopt or maintain processing systems which are technically compatible (as per recital 68 GDPR). It is therefore **crucial that the obligations under the GDPR and any self-regulatory approach under this proposal follow separate tracks, to avoid overlaps or a *de facto* extension of obligations for cloud providers that would run counter to the GDPR.**

In addition, it should also be clarified what the resulting obligations for providers stemming from Article 6 of the proposed regulation actually are. Most notably, it remains unclear whether **Article 6(1)(b)** only sets out the mere information obligations regarding operational requirements for switching and porting that should feature in a CoC, or whether in fact it implies that providers should develop guidelines on the actual implementation of said operational requirements.

Finally, the proposal encourages stakeholders to effectively **implement CoCs within one year** after the start of application of the regulation. This seems a **very ambitious timeline**, in light of the past experience in developing CoCs in very different areas (enhanced data protection in specific sectors, cooperation between industry and law enforcement authorities, etc.). It is important to devote the necessary time to the development of high-quality CoCs. Once CoCs are adopted, it will also be important to ensure their effective implementation.

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this paper, please contact Paolo Grassia, grassia@etno.eu