POSITION PAPER

Date: 26/04/2017

Contact: sanne.goossens@ceced.eu

Building the European Data Economy

CECED Views on the European Commission's Public Consultation

The European Committee of Domestic Equipment Manufacturers (CECED) represents the domestic appliances sector in Europe.[1] CECED welcomes the opportunity to provide input to the public consultation on building the European data economy. CECED also appreciates the European Commission's approach to clarify several relevant issues before proposing possible legislation.

To take full advantage of the digital transformation and compete effectively worldwide, a timely completion of the European Digital Single Market is crucial, ensuring free movement of goods, people, services, capital and data. However, we also recommend policy makers to be cautious and to carefully assess if and where action or coordination at European level is needed to achieve a business and innovation-friendly legal framework for data use.

Legal Framework

The European legislative framework for data must allow companies to compete globally, foster the creation of new business models and ensure a level-playing field, with legal certainty and stability. It should also ensure consistent enforcement for all economic operators across Member States, while at the same time fostering consumer trust – striking the right balance between protecting consumer rights and facilitating the free flow of data in the single market.

CECED believes that it is important to cultivate an innovation-friendly approach to data, to empower the digitalisation process and offer robust solutions for data use, and smart and big data applications throughout the value chain. The ability to innovate is based on the ability to invest, which requires the possibility to make use of data generated because of upfront investment. Policy makers should therefore carefully assess if and where action is needed.

Data Ownership, Use & Access

Data ownership and data access issues are adequately addressed by existing legislation. Current rules and practices allow adapting to the needs of the relevant parties and provide the appropriate setting to share data based on contractual terms, allowing innovation. In addition, issues regarding the use of data in the digital world are not completely new: they exist also in the "traditional" market world and have been adequately addressed in regulation.

[1] Direct Members are Arçelik, Ariston Thermo Group, BSH Hausgeräte GmbH, Candy Group, Daikin Europe, De'Longhi, Dyson, AB Electrolux, Gorenje, Groupe Atlantic, LG Electronics Europe, Liebherr Hausgeräte, Miele & Cie. KG, Panasonic, Philips, Samsung, Groupe SEB, Vestel, Vorwerk and Whirlpool Europe. CECED's member Associations cover the following countries: Austria, Baltics, Belgium, Bulgaria, Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, the Netherlands, Norway, Poland, Portugal, Romania, Russia, Slovakia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Thus, CECED believes that the default approach should be to assess whether existing regulation is fit to solve any conflicts also in the digital world. It is likely that the existing legislative framework and contractual arrangements are satisfactory. Especially for personal data, regulated under the General Data Protection Regulation (GDPR), existing legislation adequately deals with the issues of data ownership, use and access.

Whereas personal data and the rights of individuals have been widely regulated by the GDPR, the rights of access and use between commercial parties are best set by contractual relations. Still, because of the wide definition of "personal data" under the GDPR, in certain cases it may be difficult to draw a line between personal and non-personal data. To take advantage of the potential of the data-driven economy, different consideration should be given to personal and non-personal data.

A balanced approach to issues of access for third parties to non-personal, machine-generated data is required. While openness is essential for the digital economy's development, it is also important to consider negative developments potentially resulting from unlimited third-party access to data. Current contract law and practices allow adapting to the different needs of the contracting parties. The private sector should remain free to share its data based on contractual terms. Due to the different parties involved and the variations in the nature and purpose behind the diverse types of data, a harmonised regulatory solution would not be preferable to the existing flexibility of contract negotiations.

Caution also applies to granting open access to research data from private sector R&D or from public sector research performed in collaboration (or (co-)financed) with industry, because this could potentially discourage industry from participating in such collaborations.

Privacy by Design

Regarding data privacy, CECED would consider the incorporation of privacy by design features to certain appliances producing data – reflecting the type of process, the needs and risks involved and avoiding a top-down, one-size fits all approach, as each business has different sets of data and applicable de-identification best-practices will vary significantly.

In addition, where possible, data can be technically anonymised or pseudonymised to facilitate and secure their usability. A consistent approach to anonymisation, pseudonymisation and de-identification may offer robust solutions for smart and big data applications. It would offer little or no privacy implications, while the data may have many economic, environmental and social benefits.

Liability

The current framework is fit to address liability issues in the field of the Internet of Things (IoT). Consequently, no new liability rules for data-related services and connected products are needed. Overall, clarity in roles and liabilities for the treatment of data is crucial. Lastly, it is important to recognise that different categories of data can be treated differently with different rules applying for their use.

Free Flow of Data

Europe must ensure free movement of data in the internal market, to take full advantage of the digital transformation of the European Single Market and compete effectively worldwide. Therefore, EU legislative action to remove restrictions to the free flow of data is needed. If not, companies are not able to deploy the best technical measures available – for example to protect security – only because they would have the obligation to store the data in a specific geographic area. Storing data in a centralised location would also offer a more attractive target for hacking or surveillance. Under a

Digital Single Market, there is little justification to say that data is safer or better accessible if stored in a specific Member State, as the physical location should not have much relevance anymore.

The ability to transfer data across borders is crucial for companies, both within the Single Market and beyond. Any forced data localisation requirements should be subject to EU scrutiny and should only be kept if proportionate and in line with EU legislation and Single Market principles. As far as personal data is concerned, data flows must be carried out in accordance with the GDPR, irrespective of the nature and location of the parties, to guarantee a fair protection of users.

Lastly, intellectual property rights, trade secrets and the right of companies to protect their know-how should be fully respected in the digital economy. Digitisation and innovation of industry requires that companies can trust that their know-how is protected.