19 January 2023

Joint industry statement on the Data Act: Safeguards necessary to ensure Chapter V preserves data holders' fundamental rights

As representatives of European businesses, the signatories of this joint statement want to express their deep concerns about Chapter V of the EU Data Act on how to organise mandatory Business-to-Government (B2G) data sharing. While serious concerns extend to provisions far beyond Chapter V, the present joint statement will only address those related to Articles 14 to 22. We acknowledge that exceptional situations, and in particular unforeseeable emergency events, may require public authorities to use exceptional powers to obtain specific data held by private entities, which would enable them to remedy such crisis.

However, Chapter V of the Data Act raises major concerns over its compatibility with the EU's legal order and the EU Charter of Fundamental Rights. Our assessment is confirmed by the highly critical opinion of the European Data Protection Board, which highlights the lack of "lawfulness, necessity and proportionality" and the lack of safeguards to protect data holders from arbitrary interferences with their fundamental rights.

We therefore call on the EU institutions to introduce safeguards to ensure Chapter V's compatibility with the GDPR, the EU Charter of fundamental rights and key principles organising the rule of law.

Key principles and safeguards to be introduced in Chapter V of the Data Act

1. Define precisely what is an exceptional need

Article 15 should provide a more legally precise definition of what constitutes an exceptional need, and in particular, what constitutes a public emergency.

2. Ordinary law making is not an exceptional need

Article 15(c) should make clear that it cannot be used to gather data to support the drafting of legislation. Evidence-based law making is an ordinary activity in all Member States and cannot be considered as 'exceptional'.

3. Explicit attribution of competence to the public body requesting data

The task of public interest that justifies the exceptional need under article 15(c) should be explicitly attributed (to the public body making the request) by a specific legislative act. Horizontal competences should not be considered sufficient. Moreover, the absence of data justifying the exceptional need should make it 'materially impossible' for the public body to fulfil its task of public interest.

4. EU co-legislators should not be by-passed – EU institutions should rely on sectoral legislation

EU institutions and EU agencies should not benefit from the power granted by article 15(c), as this would otherwise by-pass EU constitutional arrangements foreseen by the EU treaties. As pointed out by the opinion of the European Data Protection Board (para 92), they should "*only be able to oblige data holders to make data available in accordance with the powers provided exclusively by sectoral legislation*".

The recently proposed horizontal rules for a Single Market Emergency Instrument (SMEI) aim at establishing a framework of measures to anticipate, prepare for and respond to impacts of crises on the Single Market. Under certain conditions, this would enable the Commission to oblige economic operators to provide information. Information-sharing obligations under SMEI would be based on the so-called 'dual activation', i.e., before information/data can be requested, the Council would activate an emergency phase via a Council implementing act and the Commission has to adopt an implementing act for the specific information request. This shows that when SMEI applies Chapter V becomes obsolete and forthcoming EU legislation will be sufficient.

5. Data requests must substantiate in a detailed manner the legality of the request and provide safeguards on how to protect the data holders' legitimate interests

Article 17 should make it mandatory for data requests to contain:

a. Information about how all the requirements of article 15 are met and how the request does not interfere in an unnecessary or disproportionate manner with the data holder's fundamental rights.
b. Information on the appropriate and effective technical/organisational measures that the public body will implement to safeguard the legitimate interest and fundamental rights of the data holder, including the protection of trade secrets and the confidentiality of commercially sensitive information.

6. A clear right to refuse data requests when certain conditions are manifestly not met

Without prejudice to the obligations of the public bodies according to article 17, article 18 should provide to data holders a clear right to refuse a data request partly or in whole if:

- The conditions enacted in Articles 15 and 17 are manifestly not met partly or in whole; or
- The measures proposed by the public body to safeguard the data holders' fundamental rights and legitimate interests (including trade secrets protection and the confidentiality of sensitive information) are manifestly insufficient partly or in whole; or
- Providing (part) of the data requested would risk making the data holder infringe another legal obligation by which it is bound (e.g., competition rules in case of requirements to pool data from different parts of the company, confidentiality agreements towards third parties). Data holders should not risk civil or criminal liability when they disclose information under the Act; or
- Public authorities have not provided sufficient evidence that they have taken reasonable steps to keep data secure. For businesses, protecting the data of their customers is key.

7. Preservation of the rule of law through unconditional right of access to judicial review

Data holders should have the unconditional right to ask a court to review the legality of any data request (including any disproportionate interference to their legitimate interest/fundamental rights) or of any decision taken by the authority referred to in article 31 on a data request that they received (during which the request for data should be suspended until the decision of the Court is received). This is a key aspect to ensure the safeguard of the rule of law. For instance, this is the solution retained in the Commission proposal for a Single Market Emergency Instrument to ensure that data requests issued in this framework meet the EU standard to safeguard fundamental rights.

8. Data minimisation should apply to public bodies requesting data

Public bodies using the powers granted by Chapter V should be bound by the principle of data minimisation, and make sure they limit their request to the minimum of data absolutely required and subsequently be obliged to delete the data requested as soon as and in so far as it is no longer necessary for the exceptional need identified in the data sharing request.

9. Obligations on public bodies in case of data breaches

Just like any private operator handling data, public bodies should be obliged to inform the data holder without undue delay from the moment they become aware of any data breach and/or infringement of any fundamental right of the data holder (and/or the respective data controller) such as an infringement of intellectual property rights, trade secrets or confidentiality obligation in relation to (part of) the data that were communicated following a data request. This is all the more important as public bodies may share with other public authorities the data they receive, therefore further raising risks of data breaches, and of breaches of the confidentiality obligations. Prior to sharing the data with third parties the respective public body should ensure that such third party has implemented appropriate and effective technical/organisational measures to safeguard the legitimate interest and fundamental rights of the data holder, including the protection of trade secrets and the confidentiality of commercially sensitive information.

About Eurochambres:

Eurochambres is the Association of European Chambers of Commerce and Industry. Established in 1958, Eurochambres represents over 20 million businesses in Europe through 45 members and a European network of 1700 regional and local chambers. More than 93% of these businesses are small and medium sized enterprises (SMEs). Chambers' member businesses employ over 120 million people.

About EuroCommerce:

EuroCommerce is the principal European organisation representing the retail and wholesale sector. It embraces national associations in 27 countries and 5 million companies, including leading global players and many small businesses. Over a billion times a day, retailers and wholesalers distribute goods and provide an essential service to millions of business and individual customers. The sector generates one in seven jobs, offering a varied career to 26 million Europeans, many of them young people. It also supports millions of further jobs throughout the supply chain, from small local suppliers to international businesses. EuroCommerce is the recognised European social partner for the retail and wholesale sector.

About Independent Retail Europe:

Independent Retail Europe is the European association that acts as an umbrella organisation for groups of independent retailers in the food and non-food sectors. Our members are groups of independent retailers, associations representing them as well as wider service organizations built to support independent retailers. Independent Retail Europe represents 23 groups and their 417.800 independent retailers, who manage more than 753.000 sales outlets, with a combined retail turnover of more than 1,320 billion euros and generating a combined wholesale turnover of 513 billion euros. This represents a total employment of more than 6.500.000 persons.

Contact information:
Eurochambres
Daniel Romanchenko, Digital Policy Advisor, romanchenko@eurochambres.eu

EuroCommerce
Ilya Bruggeman, Director Digital, Single Market & Consumer Law, bruggeman@eurocommerce.eu

Independent Retail Europe
Alexis Waravka, Head Digital & Competitiveness, Alexis.Waravka@IndependentRetailEurope.eu