Eurochambres position on the European Commission's proposal for a Data Act

Eurochambres welcomes the objectives of the European Commission to foster access to data and to encourage its further use for different purposes. For these endeavours to succeed, businesses require a clear and robust legal framework to, in particular, avoid fragmentation within the Single Market.

---

1. Why Eurochambres considers the Data Act proposal relevant

Eurochambres, through its 45 members (43 national associations of chambers of commerce and industry and two transnational chamber organisations) and a European network of 1700 regional and local chambers, represents over 20 million European businesses which in turn employ over 120 million people. More than 93% of these businesses are small and medium sized enterprises (SMEs).

Representing companies with significant investments across Europe, we share the Commission's goal of modernizing and strengthening the European digital economy, building digital skills, and preparing Europe's workforce and industrial base for a data driven future.

In a digitally connected world, the potential for innovation originating from data and data sharing is immense and will certainly play an increasingly important role for the competitive edge of European businesses. The Data Act should therefore also be an enabler for European businesses to succeed in the global data competition. A clear and balanced legal framework will allow businesses to harness the power of data for innovation and growth.

The exchanges of data need to happen in a secure and fair environment that provides businesses with legal certainty and – where appropriate – reasonable compensation. It must be ensured that the level of data protection and fair competitive conditions are maintained in practice. Most of all, with the innovation element in mind, the framework should effectively support quick, easy and secure data sharing.

Appropriate impulses and groundwork should be provided to promote and strengthen the data economy in the EU, rather than restrict it. When imposing new obligations, legislators must also beware of potential unintended consequences for the competitiveness of European businesses.

2. Summary of Eurochambres' main messages

- Legal certainty is one of the essential prerequisites for a thriving business environment and its maximisation should take centre stage when designing and/or expanding a regulatory framework. The Data Act proposal contains a number of definitions and formulations that remain too vague and/or broad: In particular, we urge further clarification on such crucial terms as "data", "product", "user" or "data holder". However, the need for clarifications goes far beyond the opening articles and extends to formulations such as "a product that competes" (Article 6(2), point (e)), "significant harm" (Article 11) or "functional equivalence" (Article 26) to name but a few.

- Businesses have a vital interest in safeguarding their trade secrets from competitors both in and outside the Single Market. While it is essential to break down barriers for data to flow as uninhibited as possible and for the European economy to be fit for the digital age, proper safeguards for trade secrets and other sensitive commercial information must be in place. In this respect, we feel that the Data Act proposal still lacks resolve: Neither is there a clear definition of what constitutes a trade secret in the context data sharing, nor do those vaguely formulated provisions that mention the issue provide sufficient safeguards or remedies for businesses to prevent the disclosure of trade secrets. When such disclosure occurs, it may cause irreversible damage.

- The interplay between a future Data Act and the General Data Protection Regulation (GDPR) is insufficiently addressed in the current proposal and thus raises many questions. When the proposal refers to GDPR provisions, it seems to ignore that the GDPR's lack of clarity has thus far been an impediment for businesses to share data. The proposal should do more to elucidate under which conditions the sharing of personal data is compliant with data privacy, including clarification over what qualifies as securely anonymised data.

- There is no doubt that SMEs are among the actors set to benefit most from the data sharing framework set out in the Data Act proposal. We welcome the exemptions for micro and small enterprises from some of the obligations put on businesses and advocate for those exemptions to also apply to medium-sized enterprises: Further overburdening SMEs would foil efforts to strengthen the data economy in the EU.

- While European businesses recognise the rationale behind improved public sector access to private sector data (B2G), the corresponding obligations for businesses must not become a bottomless pit. Conditions under which businesses have to comply with public sector requests need to be further clarified and narrowed down – ideally to public emergency situations only. Further, fair compensation for B2G data sharing must be provided in all circumstances as the associated costs may become a serious burden with stifling effects on competitiveness. Issues also remain as to compatibility with the GDPR as well as the appropriate protection for trade secrets.

- We commend the introduction of a right for users to switch between data processing services. However, besides the manifold practical difficulties this entails for service providers, the process is in fact collaborative and relies on actions taken by the original service provider *as well as* the user(s) and the designated service provider they wish to switch to. Therefore, it is worth examining whether a joint liability scheme would adequately reflect the shared responsibilities associated with a data service provider switch.

- Considering the constraints imposed by the Data Act from technical, organisational, processing, administrative and legal standpoints, the period of 12 months provided for its entry into force, appears to be far too short and unrealistic. Member States and stakeholders should be granted a period of at least 24 months to implement the extensive Data Act requirements. In any case, a longer implementation period should be considered for SMEs.

3. Detailed comments on the Data Act proposal

▪ Chapter I: General Provisions (Articles 1 and 2)

In order to ensure legal certainty, it must be absolutely clear which facts are covered by the Data Act. Unfortunately, the scope of the regulation is too unclear at this stage. The lack of clarity extends to some key terms.

The current definition of “data” is too broad and provides for different, sometimes conflicting interpretations. Especially the term “any compilation of such facts” is unclear and brings up the question of whether data sets that have been processed to a large extent fall within its scope or not. Businesses need to know whether raw data and/or inferred data fall under the “data” definition of the present proposal. Hence, Article 2(1) should be clarified and narrowed down so as to provide parties with certainty over which data is to be shared and which is not.

Questions further remain over who falls under the rights and obligations of the “data holder”. As things stand, the definition in Article 2(6) seems to extend to anyone with the (technical) ability to make non-personal data available. There might be circumstances, however, when the person(s) processing the data is(/are) not always the data controller(s). The identity and responsibilities of the “data holder” need to be stated with more clarity.

The “user” definition in Article 2(5) seems to extend to situations where a product might have several users at once. For a given product or service the data holder will not necessarily be always aware of the full circle of users. It remains unclear how far the access rights of each of these users should extend or how the data holder is to establish their validity and reach. As it stands, this lack of clarity will lead to high expenditures and legal uncertainty for businesses. The user will also not necessarily be the same as the data subject, which raises all sorts of questions in relation to the data minimisation principle of the GDPR.

The definition of “product” is not only very broad but also vague. The same holds true for “related service”. While Recital 15 should give more guidance on the meaning of the definition, it instead excludes a number of products (e.g., tablets) which are designed for processing data. The excluded products all feature wireless internet connections, while products that have fixed internet connections are not excluded from the scope. The economic operators that will be subject to the new law should at the very least be given an explanation as to how the Commission arrived at this distinction between physical products. Correspondingly, more clarity is needed on the definition of “a product that competes” referred to in Article 6(2), point (e).

- Chapter II: Business to Consumer and Business to Business Data Sharing (Articles 3 to 7)

Eurochambres believes that the proposed act should have the facilitation of data sharing as one of its main objectives: An increased availability of data has a great potential to spur innovation and investments in new technologies.

Article 3(1) obliges businesses to design and manufacture their products and related services in a way that "by default, [would make data] easily, securely and, where relevant and appropriate, directly accessible to the user". However, nowhere does the proposal seem to acknowledge the manifold technical difficulties that business will encounter with regards to (i) new products and related services as well as (ii) products that are already present on the market. It is a legitimate worry that the associated financial and administrative burdens will favour the market positions of bigger players.

The transparency obligations in Article 3(2) are too far-reaching: It is unclear who exactly will have to provide the information on the data collection. The terms "nature" and "volume" of the data (Article 3(2), point (a)) need reconsideration, as the former lacks precision and the latter depends on the use of the service by the end-user.

The legislators should be very sensitive with regards to the protection of intellectual property (IP) rights and trade secrets, as the sharing of data could jeopardize the competitive position of a company. A good balance needs to be struck between the sharing of data-by-data holders to users and third parties, on the one hand, and the protection of IP and trade secrets, on the other hand. As things stand there seem to be insufficient safeguards for businesses that will be under the obligation to share data. Therefore Article 4(3) should be complemented by a list of supplementary safeguards. Data holding businesses must retain knowledge about who the data is shared with and to what purposes it is used. In addition, clear liability rules must be in place for misuse of shared data. Any remedies currently included in the proposal – if at all effective – risk kicking in too late and at a point when irreversible damage has already occurred. Finally, the lack of clarity concerning the interplay of the Data Act with the GDPR could also cause considerable difficulties for preserving and protecting trade and business secrets. The Data Act proposal needs more specifics and further clarification in this regard.

Mandatory data sharing carries the risk of violating the GDPR. According to Article 32 of the GDPR, sufficient security measures must be implemented when processing personal data, including pseudonymization and encryption measures. The data are still considered personal but are and should be untraceable back to the specific data subject. It is questionable which access to which data is to be granted in this context. In general, it should be noted that access to one's own data is only possible in the context of personal reference. If data is to be considered anonymized or anonymous, they can also no longer be assigned to any specific person or user, i.e., access could only be granted broadly to "all data created by the use of the product".

Article 4(4) could give rise to different interpretations and some businesses think it should be amended to ensure that it is comprehensive enough to include "related services". The text should thus read as follows: *"…to develop a product or a related service that compete with…"*. Accordingly, the same amendment is being advocated by some businesses in relation to Article 6(2) that applies to third parties.

Article 4(6) focuses on the relationship between data holder and user but seems to omit safeguards for the manufacturer when they are not also the data holder. Safeguards for the manufacturer need to be further clarified.

The obligations will naturally incur costs for the involved enterprises, and we therefore are supportive of Article 7 which exempts micro and small enterprises from the obligations of Chapter 2. The exemption should be extended to medium-size enterprises.

- Chapter III: Obligations for Data Holders Legally Obliged to Make Data Available (Articles 8 to 12)

Article 8 establishes a reversal of the burden of proof on the data holder who will be under the obligation to demonstrate that there was no discrimination in case such a claim is raised by the data recipient. The reversed burden of proof is consistent with the GDPR approach. However, the question needs to be raised whether such a reversal makes sense in the context on non-personal data. Eurochambres does not believe so.

- Chapter V: Making Data Available to Public Sector Bodies and Union Institutions, Agencies or Bodies Based on Exceptional Need (Articles 14 to 22)

Eurochambres is very sceptical about the provisions included under Chapter 5, which set the framework for companies to deliver data to public bodies in exceptional circumstances (B2G data sharing). We note in this respect that we are equally sceptical about similar provisions that were put forward in other legislative proposals such as in the Chips Act and the Single Market Emergency Instrument.

One of the most fundamental issues with the introduction of measures that in crisis situations allow public authorities to address exceptional requests to private parties, relates to the fact that the grounds on which a request can be made are extremely loosely defined. In principle, Article 14 states that only an exceptional need can trigger the obligation for an economic operator to provide data to a public authority. The "circumstances" listed in Article 15 are so vague however, that the triggering of mechanisms in effect might depend on a purely political decision instead of being based on proportionate and well-considered criteria.

This is not to state that there cannot be situations that warrant the triggering of crisis mechanisms, but rather that the current wording leaves too much wiggle room for impertinent requests. The European Data Protection Board and Supervisor (EDPB-EDPS) joint opinion, for instance, found that access to data by public authorities should always be properly defined and limited to what is strictly necessary and proportionate. The joint opinion therefore urged "co-legislators to define much more stringently the hypotheses of emergency or 'exceptional need'".[1]

We believe that mandatory B2G data sharing is only warranted in cases of truly *exceptional* circumstances. Considering the "necessity and proportionality test", confirmed by consolidated case law of the European Court of Justice, legislators should only maintain Article 15, point (a) and limit Article 15, point (b) to "recovery" from a public emergency as

[1] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act): https://edps.europa.eu/system/files/2022-05/22-05-05_edps-edpb-jo-data-act_en.pdf

"prevention" cannot be considered exceptional due to its loose temporal boundaries. Article 15, point (c) is particularly problematic because e.g., "the lack of available data" is not specific enough for a B2G data sharing request and risks exposing companies.

Additionally, any obligation in this sense should strive for proportionality in its application as well as the reduction of costs for those it applies to. Fair compensation schemes are thus necessary as a check on potentially inflationary requests from public authorities. In public emergency situations, the data holder should at least be entitled to recover the costs associated with collecting, processing, anonymizing, aggregating, analysing and delivering the requested data. For data requests aiming at assisting the recovery from a public emergency, the data holder should have the right to commercially negotiate the economic terms.

At the same time, businesses should have more clarity about what data are concerned as well as for which purposes, they can be requested. Legal certainty should be provided about the interplay between the Data Act and the GDPR. It seems for instance unclear whether personal data are covered by Chapter 5 of the Data Act and, if they are, how the present provisions link to Article 14 GDPR which sets rules on information to be provided where personal data have not been obtained from the data subject. Moreover, the recitals of the Data Act proposal clearly state that the provisions of the act do not provide a legal basis for data disclosure under GDPR. However, Article 18(5) readily assumes that personal data must also be disclosed if the requirements of the Data Act are met. There is no indication in the proposal that the obligations under data protection law must be fulfilled and that there must therefore be a legal basis under data protection law for a data transfer in the sense of Article 6 GDPR.

- Chapter VI: Switching Between Data Processing Services (*Articles 23 to 26*)

More and more businesses rely on cloud and data processing services in their daily activities. As end users, they can expect to benefit from an open and dynamic market for cloud and data processing services. A majority of businesses therefore welcomes measures in the Data Act proposal that aim at strengthening their bargaining position as users, facilitating the switching process and countering lock-in effects.

Regulation must however be practicable and proportional in order not to stifle the further development of the cloud and data processing services market. Service providers have raised concerns about the implementation of the provisions in Chapter 6. While it is indeed desirable for end users to be able to switch services easily, there may be situations (e.g., tailor-made platforms and services) where technical aspects render it very challenging. As things stand, all obligations giving end users the right to have compatible services are put on the service providers. Further, the one-month period within which a switch is to be completed is in many cases impracticable and ignores technical realities.

Article 26 introduces the concept of "functional equivalence" for end users when they switch services. As for other provisions in the present chapter, doubts have been raised over the practicability of its implementation as it would lead to an erosion of service providers' freedom to contract and have disproportionate effects on the right to free design.

The co-legislators should consider that in practice, when switching cloud provider, end users do so in order to upgrade functionalities. Requiring the new provider of data processing

services to “deliver the same output at the same performance and with the same level of security, operational resilience and quality of service” may set an obligation to invest in a functionality it never offered in the first place.

Eurochambres believes that the costs associated with the aforementioned obligations on providers should be calculated and weighed up carefully, especially since there is no exemption for SMEs for whom these obligations would be disproportionately burdensome. It is important that the responsibility for implementation is not simply transferred to businesses, but that the obligation is made dependent on the existence and establishment of a corresponding set of standards.

Lastly, all obligations giving users the right to have compatible services are put on the original service provider. However, a big part of the switching process relies on the user (e.g., users may have their own requirements in terms of business continuity, migration hours, etc.). Therefore, we recommend considering a collaborative approach with a joint liability between the user demanding the switch and the service providers, both of origin and destination.

- Chapter VII: International Contexts of Non-Personal Data Safeguards (Article 27)

The creation of minimum safety standards is viewed favourably. However, flexibility should be provided with regard to SMEs depending on economic capabilities.

- Chapter VIII: Interoperability (Articles 28 to 30)

Eurochambres welcomes the objectives of Article 28, namely making data transfers easier for end users through the establishment of essential requirements regarding interoperability. Tearing down barriers in this respect is indeed essential. The Commission is making the right choice by not prescribing specific technical standards and interfaces. We do note that clarity could be enhanced by adding a definition of the term “operator of data spaces”, in Article 2.

Rather than governmentally-imposed standards we would favour industry driven standards which better reflect the daily realities businesses have to cope with, and which are therefore more conducive to innovation-friendly solutions. Hence, industry and business experts should lead these efforts together with specific standardization bodies. Public-private collaborations offer an opportunity for a more competitive and efficient environment.

It must also be assured that interoperability is extended to all levels of the administration: European, national as well as regional and local.

- Chapter X: Sui generis Right under Database Directive (Article 35)

We welcome the clarification that the *sui generis* right under the Database Directive does not apply to databases containing machine-generated data.

Eurochambres is the Association of European Chambers of Commerce and Industry. Established in 1958 as a direct response to the creation of the European Economic Community. Eurochambres represents over 20 million businesses in Europe through 45 members (43 national associations of chambers of commerce and industry and two transnational chamber organisations) 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.

More info and previous positions on: https://bit.ly/ECHPositions

Contact:
Eurochambres Policy Advisor
Mr Daniel Romanchenko, Tel. +32 2 282 08 85, romanchenko@eurochambres.eu

Eurochambres Press and Communication Manager
Ms Karen Albuquerque, Tel. +32 2 282 08 72, albuquerque@eurochambres.eu

@Eurochambres
www.eurochambres.eu

EU Transparency Register number: 0014082722