AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

European Commission's Consultation on the Data Act

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.4 trillion in 2021, directly supports more than 4.9 million jobs in Europe and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

The American Chamber of Commerce to the EU (AmCham EU) shares the objectives of the European Commission to increase access to and further the (re-)use of data through the proposed 'Data Act'. The Data Act should focus on promoting greater voluntary data sharing in order to boost economic growth, research and innovation, competitiveness, job creation and to achieve Europe's digital transformation objectives. It should also ensure that international data flows are protected and encouraged, as they are not only vital to the European and global economy but also to the enhanced data sharing and re-use scenarios the Commission has identified.

However, the mandatory nature of certain requirements could have unintended consequences and even risk disrupting current and successful data sharing initiatives in Europe. In particular, many existing business-to-business (B2B) and business-to-government (B2G) data collaborations, based on contractual freedom and the use of various data sharing technologies, are already providing important examples of the benefits that more open approaches to data can achieve. Potential restrictions on international data transfers and mandatory requirements on particular subsets of data, along with prescriptive portability requirements and lack of clarity on the data which falls in scope, could make collaboration more difficult, particularly with international partners that are vital to tackle shared societal challenges and for companies operating and digitally transforming globally. Research indicates that the EU could gain around €2 trillion in growth and create two million jobs by the end of the Digital Decade if the current negative trends on data flows are reversed and the power of international data transfers is harnessed[1].

The Commission should clarify the primary scope of the proposal (eg non-personal data) by distinguishing between data that is generated by a device or system and that which is collected and stored. The technical advancements in today's products utilise a tremendous amount of data that is generated and used only within the confines of the product. Mandating all data generated to be collected and shared goes well beyond the technical capability of most manufactured products. Acknowledging this distinction in the Data Act enables sector specific legislation to define the appropriate types of data for each of them, which could be revised over time.

To ensure the Commission's data economy ambitions become a reality, several aspects of the proposed Regulation require additional clarification. The new obligations should be clear, realistic and balance the technical complexity of implementing new requirements with the need to foster user trust, serve customers' interests and encourage the development of new innovative technologies and ways of leveraging data. The proposal should also recognise successful industry-led initiatives already underway which meet similar objectives, as many B2B and B2G data collaborations are already demonstrating the benefits that more open approaches to data can yield.

AmCham EU aims to ensure the Data Act meets its stated objectives. For that, it is working on an extensive position paper as well as suggested amendments and solutions seeking to support the co-legislators in their work on the proposal. In the meantime, and for the purpose of this consultation, the Commission should pay attention to the following selected overarching issues that should have priority in the analysis of the proposal and that are in particular need of clarification:

[1] DigitalEurope, Data flows and the Digital Decade https://www.digitaleurope.org/resources/data-flows-and-the-digital-decade/

International data flows

The Data Act should contribute to removing - not instituting - conflicts of laws, and enabling - not restricting - the free flow of data. International data flows are indispensable for European companies' competitiveness, as they operate in a connected environment that goes beyond the EU's borders. Article 27 of the draft Regulation places additional restrictions on the ability to transfer non-personal data outside the EU, including in response to a third-country government demand, where such a transfer (or access by third-country authorities) may give rise to a conflict with EU or Member State law. Given the overly broad notion of 'conflict' set out in recital 77, and the lack of guidance on jurisprudence, these provisions could create additional legal uncertainty and impediments to companies' ability to transfer generally lower-risk non-personal data similar to (or potentially even greater than) those that the General Data Protection Regulation (GDPR) imposes on personal data. Although cloud service providers may receive mandatory data transfer orders from third-country governments, non-personal data is far less likely to be subject to access requests and does not raise the same kind of risks as personal data. In this regard, the Commission should solve issues around foreign authorities' access to data through multilateral governmental discussions rather than by imposing regulatory requirements on a specific sector.

Data sharing obligations

B2G

B2G data sharing should remain voluntary. However, if mandatory obligations are adopted as proposed, 'exceptional need' should be precisely defined through use cases and with proper safeguards in place for the sharing of personal and sensitive data. In their current standing, the provisions of the draft Regulation lack clarity, notably on what conditions and which thresholds must be met to grant public authorities access to data, as well as the cost implications of the sharing process.

B2C

While the proposal's scope varies from chapter to chapter, the application to manufacturers of 'products' and providers of 'related services' for corresponding data sharing provisions remains broad. However, in a consumer IoT context, it is difficult to distinguish which 'generated data' would not be personal data, and therefore already fall under GDPR rules. In addition, while 'publicly available electronic communication service' is the medium through which such data is transmitted, it should be clarified that it is not covered under any of these categories. Data Act sharing requirements go well beyond GDPR portability requirements. Requirements to share 'non-personal' data leads to an infinite scope, impossible to engineer, while bringing no or very limited added value to consumers.

Cloud portability and switching

The importance of data portability is well established and increasingly expected by customers. However, data portability is different from switchability; while the porting out of data from a data processing provider to a user is under the control of the existing cloud or data processing provider and can be handled by that provider solely, this is not the case for switching. Developing on this evidence, several concepts of the proposal pertaining to cloud portability and switching would be in need of substantial clarification, notably:

- The definition of 'obstacle'.
- The notion of 'functional equivalence'.
- Distinctions between infrastructure level services and software and platform services.

Moreover, certain provisions would need extensive redefinition, as they appear unrealistic in their demands. Notably, the proposed 30-day deadline (extendable to a maximum of six months) for switching appears disproportionate both in the timing and cost implications without further considering the complexities that could be involved in a switching process.

Protection of trade secrets

The protection of trade secrets is not given sufficient attention and importance across the different provisions of the proposal. The Data Act imposes that trade secrets shall only be disclosed to the user provided that all specific necessary measures are taken to preserve its confidentiality. However, it is difficult to see how data holders would be able to enforce this restriction in practice. Therefore, rather than focusing on confidentiality, the proposal should clearly exempt trade secrets from its scope with an applicable reference to the Trade Secrets Directive, which should take precedence.

Review of database directive

The text as proposed in the draft Data Act is appropriately balanced, as it aims to ensure IP protection for certain types of datasets while clarifying the scope and applicability of the *sui generis* right to align with the objectives of the overall proposal. In order to ensure clarity on the IP protection and to avoid confusion in implementing the Regulation, article 35 should be further aligned with recital 84 by specifying that the Database Directive does not apply unless the databases qualify for the *sui generis* right.

Interaction with existing legislation and enforcement

The draft proposal references several pieces of EU legislation, both current and upcoming, which are in various stages of adoption, implementation and review. Consistency between the Data Act and other horizontal legislation will be essential for the legal certainty necessary to create greater confidence in data sharing between businesses and across sectors. The proposal would also benefit from clarifying its scope of application to ensure legal certainty for businesses in terms of what products, type of data and players would be covered.

When it comes to enforcement, the Data Act leaves significant discretion to Member States to designate competent authorities responsible for enforcement of different chapters and provisions. Policymakers should strive for harmonisation and provide clarity on harmonised enforcement and competent authorities insofar as possible in order to provide businesses and customers with greater certainty on the resources available for relevant guidance and regulatory feedback.