



17 January 2023

Joint Industry Statement: Business Community Calls for Increasing Legislative Clarity of the EU Data Act

The signatories of this statement represent a large portion of the data economy, including manufacturers of connected products, data users, software developers, service providers and cloud providers. Data is the lifeblood of the digital economy, and the sectors we represent are strongly committed to harnessing the huge benefits of data use and re-use. The breadth of this coalition shows both the widespread interest in the EU Data Act proposal, as well as its broad, systemic impact across all sectors of the European economy.

This statement highlights the shared priorities, challenges and concerns of the industries we represent. We urge policymakers working on the file to address these points as the discussion on the file progresses.

Given the significant impact and the complexity of the Data Act, we urge legislators to **prioritise clarity of the legislative text over speed in the legislative process**, to ensure key concepts are well understood, deliberately weigh the different options, and – most of all – carefully assess their full impact.

The industry supports the Commission’s ambition to stimulate a competitive data market with opportunities for data-driven innovation and to achieve fair, reasonable, and non-discriminatory access to data across all sectors of the economy. However, we share the concern that several provisions, in their current form, present significant technical and legal challenges for companies. They will also create legal uncertainty as to how data will be handled, which will likely decrease the quantity and quality of the data that businesses gather and process.

Our specific recommendations are:

- Clarify the definition of the data in scope;
- Take into account legitimate business interests;
- Ensure the protection of trade secrets;
- Ensure financial and operational viability of cloud contracts;
- Ensure cooperation between all parties to the switching process;
- Reconsider the notion of functional equivalence;
- Avoid hindering international data flows;

The following paragraphs contain a more detailed overview of our recommendations.

B2B Data Sharing – Chapters 2 and 3:

Clarify the definition of data

The definition of data is unclear, too broad and general. No distinction is made between data that could be relevant to users and data that reflect the internal functioning of the product, for instance in relation to the design, the interfaces and interactions between internal components or sub-systems. These should remain off-limits because of their intrinsic industrial sensitivity or the protection they deserve under intellectual property or trade secrets rules. If unduly disseminated, such product design data will expose core product design and technology to retro-engineering and copying, which would significantly affect the competitiveness of businesses in the EU.

There are inherent limitations to the amount of data that can be managed in any given product, and that can be transferred to an interface where it can be accessed. This is true for many products that fall under the scope of the Data Act – the primary function of which is not to generate, manage, share and receive data. From a technical point of view, transferring additional data points often requires major modifications to the physical architecture and software of a product, which in turn will require overusing its computing power. Furthermore, any modification to the physical architecture requires corresponding (cyber)security measures. Such modifications have a significant impact on the total cost, development processes and resource optimisation – not to mention on the environment. Moreover, a broad definition of data will require data holders to store and process more data (personal or non-personal) than necessary, even those that are normally deleted. This unintended consequence would be in conflict with the principle of data minimisation of the GDPR.

Data from a product can therefore only be made accessible where the design and architecture of this product allow for it. This data is readily available to the manufacturer and can be used to provide a service of which the customer avails. Therefore, this is the data that the data holder should make available to users so that they can decide whether and with whom it should be shared.

Take into account legitimate business interests

B2C and B2B data sharing and contractual frameworks differ widely. Yet the Data Act proposes to introduce an obligation on the data holder to provide access to the resulting data as soon as possible, and free of charge, to the user, be it a consumer or a professional. The cost, constraints and potential loss of trade secrets may lead manufacturers to reconsider their business model. Entering into voluntary, contractual agreements on data sharing should remain the key for regulating access to and sharing of non-personal, industrial data for professional use, in line with the rules of private law and the principle of contractual freedom. Data holders should also be adequately compensated for providing any value added data service on top of the obligations to make data available.

Ensure protection of trade secrets

The proposal provides that trade secrets should be made available to users, assuming contractual provisions are in place to protect them. The proposal also suggest that users' right to portability must prevail over contractual or technical measures seeking to protecting legitimate trade secrets. It thus entirely relies on third parties' good intentions not to use trade secrets unlawfully. This is clearly insufficient to ensure proper protection of trade secrets. Trade secrets are specifically designed to enable their holder to exclude others from accessing confidential information. The protection of trade secrets does not grant any genuine exclusive rights to the holder, but instead relies on the fact that the information is kept 'secret'. A trade secret, once lost, cannot be recovered, as third parties are free to use the information disclosed, which is now in the public domain.

The protection of confidential business data and trade secrets is paramount to a well-functioning internal market. Therefore, the Data Act should not compromise trade secret protection by preventing the trade secret holder from taking all reasonable steps to protect its trade secrets, including the right to refuse to share the protected information. To ensure fairness in the data economy, generate trust and preserve manufacturers' incentives to innovate, it is critical to protect trade secrets and intellectual property-related data.

We therefore call on the European Parliament and the Council to clarify this legislation to ensure that the principles that it lays down are served by requirements which facilitate data sharing. The legislation should strive to preserve economic incentives to innovate and invest in connected products, and to generate and share data for all market operators, most of whom already share their data.

Cloud switching – Chapter 6:

The Data Act mandates the elimination of legal, technical and organisational barriers to cloud switching, while ensuring full service provision to customers throughout the switching process. While the industry supports the objective of improving switching between providers, some of the measures raise questions around their technical feasibility and their legal and economic viability. The following aspects should be amended or reconsidered:

Ensure financial and operational viability of cloud contracts:

The 30-day termination clause creates significant uncertainty in cloud contracts that normally rely on multi-year commitments reflecting long deployment timelines, front-loaded implementation costs and other factors. This predictability is fundamental from an operational and financial perspective. Introducing new termination rights by regulation, without allowing fixed-terms contracts, would almost certainly lead to price increases for all cloud users and would be contrary to the expectations of B2B contracting parties. This risk would be reinforced by the proposed phase-out of transfer fees. Data transfer fees reflect the cost of providing customers with network services and are not meant as a disincentive to switching. The cost and timing to switch to another provider is highly variable and depends on choices made by the customer, such as how the customer architected their solutions, what data the customer wants to move and the customer's destination solution. An alternative approach could be the clear scoping of what constitutes switching fees through transparent information on switching feasibility and pricing in contracts.

Ensure cooperation between all parties:

Business and service continuity is only guaranteed through collaboration between both service providers and the client. The obligations on the original service provider in article 24 to complete the switching process while ensuring service continuity are technically unrealistic. Normally, customers and providers agree in a contract on specific service level agreements that providers commit to meet during the termination assistance phase. The service levels agreed therein never foresee a 100% service continuity, as parties understand and agree that the service will not be the same during a termination phase as during the lifecycle of the contract.

Reconsider the notion of functional equivalence for infrastructure services:

This notion is confusing operationally, legally and technically. It is impossible to envisage how the provider of the original environment can ensure minimum functionalities without accessing a competitor's environment. The current approach to functional equivalence, both in the context of proposed portability and interoperability requirements, could damage competitive advantage due to exposure of trade secrets, sensitive information, and inevitably lead to homogenous/standardised

service offerings with a negative impact on choice and service diversity. Similarly, the notion of ‘same service type’ reduces the complexity of cloud services into discretionary ‘buckets’ which do not reflect the reality of cloud services. While services may share a similar objective (e.g. storage or computing), by categorising them as fundamentally the same service (and requiring functional equivalence between services), services will be forced to standardise in a way which is not beneficial to the customer or competition between cloud service providers.

International data transfers – Chapter 7:

Avoid hindering international data transfers:

Access to data is crucial for innovation and allows companies to reach consumers and access new markets. The flow of data across borders should thus be encouraged to support the global competitiveness of businesses in Europe. Chapter 7 of the Data Act proposal mandates providers of data processing services to take measures to prevent international transfer or governmental access to non-personal data when this would create a conflict with EU or national law. Since the proposal neither defines “conflict of law” nor it provides derogations to these data transfer restrictions similar to those set out by GDPR, such provisions could create impediments to companies’ ability to transfer non-personal data worse than those that the GDPR imposes on personal data. This is not justified by the risk posed by non-personal data, which unlike personal data, do not pose risks for fundamental rights. It is also unclear how cloud providers could comply with these provisions without directly accessing the data of their customers. Besides, clients of cloud services should retain control over the data and therefore should be able to choose under which condition their data may be transferred outside of the Union.

The signatories:

Adigital
AFNUM
Allied for Startups
CCIA, Computers & Communications Industry Association
Confederation of Danish Industry
Confederation of Industry of the Czech Republic (SPCR)
Confederation of Swedish Enterprise
Developers Alliance
Ecommerce Europe
IBEC
Infobalt Lithuania
ITI, Information Technology Industry Council
Teknikföretagen