N O V E

ANALYSIS:
THE EU DATA ACT

FEBRUARY 2022

OVERVIEW

On 23 February 2022, the European Commission unveiled its proposal for a "Data Act" (DA) – a Regulation of the European Parliament and of the Council on harmonised rules for fair access to and use of data. The DA complements the EU's Data Governance Act, which lays down basic conditions for data sharing and supports the creation of Common European Data Spaces, and is the last piece of the puzzle completing the European Data Strategy that was first published in February 2020.

While existing EU laws cover the use and transfer of personal data, the DA focuses on non-personal, large datasets that can be used to enable new innovative business models and ancillary aftermarket services. The draft law, divided into 11 Chapters and 42 Articles, presents a rulebook for:

- Business-to-business (B2B), business-to-consumer (B2C), and business-to-government (B2G) data sharing;
- Switching between cloud and other data processing services;
- Data transfers outside of the EU.

As a horizontal proposal, the DA is sector-agnostic. However, it leaves room for vertical legislation to address sector-specific regulatory objectives, such as access to in-vehicle data. Once in force, it will have a **major impact on producers of connected devices** – more broadly known as the Internet of Things (IoT) – and related services, clarifying who (users, manufacturers, or third parties) is entitled to use data generated by such objects or systems and on what basis.

This proposal will now be debated and amended by the EU's two co-legislators, the European Parliament and the Council. Given its far-reaching scope and initial difficulties in going through the European Commission's internal approval process, the DA may still undergo significant changes throughout the legislative process.

Our analysis of the text is structured as follows:

I. Scope
II. Data sharing
III. Switching between data processing services
IV. Interoperability
V. Data transfers outside of the EU
VI. Implementation and enforcement
VII. Initial stakeholder reactions

I. SCOPE

The Data Act aims to remove barriers to access data for both private and public sector bodies, while introducing mechanisms to compensate actors that make data available. The regulation applies to:

- **Manufacturers** of products and **suppliers** of related services placed on the EU market and the **users** of such products or services;
- **Data holders** that make data available to data recipients in the EU;
- **Data recipients** in the EU to whom data are made available;

- **Public bodies** (public sector bodies and EU institutions, agencies or bodies);
- **Providers of data processing services** offering such services to customers in the EU.

Where the proposal refers to products or related services, such reference also applies to virtual assistants, insofar as they are used to access or control a product or related service.

II. DATA SHARING

B2B and B2C data sharing

The DA introduces provisions on how businesses and consumers can access data generated by the products and related services which they own, rent or lease (*Articles 3-13*).

- **Data access by design**: the regulation would oblige manufacturers and designers to design the products in a way by which the data would be easily accessible by default. **They would also need to be transparent** with the user, informing in a clear and comprehensible format on how to access the data, the nature and volume of the data, and how to request that the data are shared with a third-party.

- **User (or third party) access right**: The DA grants users the right to access and use the data they contributed to generating. Users are also entitled to authorise the data holder to give access to the data to third party service providers (e.g. providers of aftermarket services, such as repair).

- **Obligation of the data holder to make data available upon request** for: (1) user to the user, (2) user to a third party and (3) third party authorised by the user to the third party.

- **The data holder should make the data available without undue delay, free of charge for the user** and – where applicable – **continuously and in real-time**. This should be done under fair, reasonable and non-discriminatory terms and in a transparent manner.

Safeguards for data holders

- Having received data, users would be forbidden from developing a product that competes with the product from which the data originates.

- The list of obligations on third parties notably prohibits deploying coercive means or abusing evident gaps in the technical infrastructure of the data holder, as well as deceiving or manipulating the user in any way or preventing the user from making the data it receives available to other parties. **Trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary**.

- The data holder may also apply appropriate technical protection measures, including **smart contracts**, to prevent unauthorised access to the data and to ensure compliance.

Compensation

The DA allows data holders to set **reasonable compensation** to be met by third parties, but not from the user, for any cost incurred in providing direct access to the data generated by the user's product. Any compensation set for SMEs cannot exceed the costs incurred for making the data available (unless otherwise specified in sectorial legislation).

Dispute settlement

The proposal stipulates that parties should have access to settlement bodies certified by the Member States when they disagree on the compensation or other contractual conditions.

Stakeholders differentiation

"Gatekeepers" as defined within the **Digital Markets Act** (DMA) are **not able to benefit from the proposal** (the DA deems them as illegible third parties), whereas **SMEs receive special protection** in terms of contractual terms – fairness tests – and are largely exempt from any obligations.

B2G data sharing

The DA identifies **exceptional circumstances under which public bodies may receive data from private companies**. This would only apply in case of (*Articles 14-22*):

- **Necessity to respond to a public emergency** (e.g., pandemics or disasters);
- **Necessity to prevent a public emergency or to assist in the recovery from a public emergency** (in that case the request should be limited in time and scope);
- **Lack of available data that prevents public bodies or EU institutions from fulfilling a specific task** in the public interest that has been explicitly provided by law; and
    - public bodies were unable to obtain such data via alternative means – on the market or by relying on existing obligations – and the adoption of new legislation cannot ensure the timely availability of the data; or
    - obtaining the data in line with the procedure laid down in proposed regulation would substantively reduce the administrative burden for data holders or other businesses.

The provisions on sharing data with public bodies do not apply to small and micro-enterprises.

Compensation

- Data would be made **available for free, if needed to respond to a public emergency**.
- For other exceptional data needs, the enterprises providing the data should be entitled to **compensation which include costs related to making the relevant data available plus reasonable margin**.

Compliance with requests for data

- To ensure that the right to request data is not abused and that the public sector remains accountable for its use, the requests for data would need to be **proportionate**, **clearly indicate the purpose** to be achieved, and **respect the interests of the companies** making the data available.
- Data holders would be able to decline or seek the modification of the request within five working days following the receipt of a request for the data necessary to respond to a public emergency and within 15 working days in other cases, on either of the two following grounds:
    - the data is unavailable;
    - the request does not meet the conditions laid down in DA.
- Competent authorities would ensure the transparency and public availability of all requests. They would also handle any resulting complaints.

Obligations of public sector bodies

Having received data, public bodies would be:

- Forbidden from using the data in a manner incompatible with the purpose for which they were requested;
- Obliged to implement technical and organisational measures that safeguard the rights and freedoms of data subjects (insofar as the processing of personal data is necessary);
- Obliged to destroy the data as soon as they are no longer necessary for the stated purpose (and inform the data holder about it).

Trade secrets

Disclosure of trade secrets shall only be required to the extent that it is strictly necessary to achieve the purpose of the request. In such a case, the public bodies shall take appropriate measures to preserve the confidentiality of those trade secrets.

Contribution of research organisations or statistical bodies

The DA allows public bodies **to share received data with individuals or organisations in view of carrying out scientific research** or analytics compatible with the purpose for which the data was requested, or to national statistical bodies and Eurostat. In that case, however, such individuals or organisations should act on a not-for-profit basis or in the context of a public-interest mission in the EU or a Member State.

III. SWITCHING BETWEEN DATA PROCESSING SERVICES

The DA introduces **minimum regulatory requirements of contractual, commercial and technical nature, imposed on providers of cloud**, edge and other data processing services. The underlying idea is to facilitate switching between such services (*Articles 23-26*).

The Commission believes that businesses should be able to easily move their data and other digital assets between competing providers of cloud services. The rights of the customer and the obligations of the data processing service providers should be clearly set out in a written contract, and include:

- Clauses **allowing the customer to switch to a data processing service offered by another provider** or to port all data, applications and digital assets generated directly or indirectly by the customer, with a mandatory maximum transition period of 30 calendar days.

- An **exhaustive specification of all data and application categories exportable during the switching process**, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service;

- A **minimum period for data retrieval of at least 30 calendar days**.

- It should be **ensured** that customers maintain **functional equivalence** (a minimum level of functionality) of the service after they have switched to another service provider.

- Most importantly, the proposal contains an **exception for technical unfeasibility**, putting the burden of proof in this regard on the service provider. The draft law does not mandate specific technical standards or interfaces but requires that services are compatible with open standards or interfaces where these exist.

- In a maximum period of three years after the DA's approval, **providers of data processing services shall not impose any charges on the customer for the switching process**. Until then, they are allowed to impose reduced charges, but it shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process.

IV. INTEROPERABILITY

According to the Commission, data sharing was often impossible for technical reasons, such as a lack of standardised data structures or a lack of relevant core vocabularies. The proposal introduces mechanisms to identify and address these technical obstacles, and provides for essential requirements to be complied with regarding interoperability for (*Articles 28-30*):

- **Operators of data spaces** (e.g., provision of sufficient, consistent and publicly available descriptions of data and technical means);

- **Data processing service providers** (e.g., performance orientation, enhanced portability, functional equivalence guarantee),

- **Smart contracts for data sharing** (e.g. robustness, safe termination and interruption, data archiving and continuity and access control).

The DA enables open interoperability specifications and European standards for the interoperability of data processing services to promote a multi-vendor cloud environment. The European Commission has also

reserved the right to adopt implementing acts and guidelines to further specify these requirements, as well as to request European standardisation organisations to draft harmonised standards.

V. DATA TRANSFERS OUTSIDE OF THE EU

The proposal addresses concerns about potentially unlawful third-party access to data processing services offered in the EU, by **requiring cloud service providers to take measures against unlawful data transfers to governments outside the bloc** (*Article 27*).

Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to **prevent the international transfer or governmental access to non-personal data held in the EU** where such transfer would create a conflict with EU law or respective national laws in Member States. Exceptions can apply in the presence of an administrative decision or judgement of a third country.

VI. IMPLEMENTATION AND ENFORCEMENT

- Competent bodies in each Member State should designate one or more authorities or rely on existing ones, without prejudice to the General Data Protection Regulation (GDPR). National authorities are expected to, among others, conduct investigations into matters that concern the DA's application, impose **dissuasive financial penalties** or initiate legal proceedings for the imposition of fines and monitor technological developments of relevance for making available and use of data (*Article 31).*

- Member States shall also lay down the rules on penalties applicable to infringements and ensure that they are implemented. The DA proposes **fines up to EUR 20 million or 4% of annual group turnover** (*Article 33).*

- **Database Directive**: The DA reviews certain aspects of Directive 96/9/EC, essentially excluding databases containing data obtained from or generated by the use of a product or a related service from the protection of sui generis right established therein. This is to ensure that data can be accessed and used (*Article 35*).

VII. INITIAL STAKEHOLDER REACTIONS

- **Margrethe Vestager**, Executive Vice President for Europe Fit for the Digital Age, European Commission: "The European Commission wants to give consumers and companies even more control over what can be done with their data, clarifying who can access data and on what terms. This is a key digital principle that will contribute to creating a solid and fair data-driven economy and guide the Digital transformation by 2030."

- **Thierry Breton**, Commissioner for Internal Market, European Commission: "The Data Act is an important step in unlocking a wealth of industrial data in Europe, benefiting businesses, consumers, public services and society as a whole. So far, only a small part of industrial data is used and the potential for growth and innovation is enormous. DA will ensure that industrial data is shared, stored and processed in full respect of European rules. It will form the cornerstone of a strong, innovative and sovereign European digital economy".

- **CCIA** Public Policy Director Alexandre Roure: "The proposal is well intentioned, but in need of improvements. In order to serve the EU's digital ambitions, it needs to protect confidential business information, treat all companies equally, and avoid creating new data flow restrictions".

- **DIGITAL EUROPE** Director-General Cecilia Bonefeld-Dahl: "When it comes to data sharing, many companies – especially smaller ones – are still finding their feet: they need incentives and support, and this is not the time to impose strict measures across the board that are designed to fix problems that simply do not exist. They estimate that presently two-thirds of European SMEs transfer data over international borders, but they are afraid the current proposal will restrict international data flows, which will seriously hamper their growth and competitiveness. 90% of future growth will come from outside Europe. This is a fact we need to face and work hard to make Europe a better place to do business instead of constantly imposing new regulation".