GIBSON DUNN

January 8, 2024

The EU Data Act, an IoT and Cloud Sector Paradigm Shift, Becomes Reality

Because of the Data Act's extensive requirements, all companies should assess if any of their products or services will be caught by the Data Act, which will start applying from the second half of 2025.

*The EU's Data Act will enter into force on 11 January 2024. With the stated goal of 'unlocking' the EU's data economy, the Data Act imposes a set of wide-ranging data sharing, product design and contractual obligations on providers of Internet of Things ('**IoT**') devices and related services, and on cloud computing providers. The obligations under the Data Act apply to all sectors of the economy, and to businesses of all sizes. Because of the Data Act's extensive requirements, all companies should assess if any of their products or services will be caught by the Data Act. The obligations under the Act will start applying from the second half of 2025 so there is little time to prepare effective compliance strategies.*

1. Executive summary

The Data Act rests on the general assumption that the vast majority of data generated by connected devices, services and cloud software is unused, or collected by a small number of large companies. Through this new legislation, the EU seeks to 'unlock' this data, facilitate moving data between one service and another, and make it accessible to users – and also to third party businesses if approved by the respective users.

The scope of the Data Act will apply to (i) manufacturers of connected products and providers of related services placed on the market in the EU; (ii) the users of such connected products or services in the EU; (iii) data holders that make data available to recipients in the EU; (iv) data recipients in the EU; (v) providers of data processing services offering services to customers in the EU; and (vi) EU institutions and public sector bodies accessing data under the regulation. The Data Act will therefore also apply to foreign companies that operate in EU markets, irrespective of their place of establishment or subsidiary presence in the EU.

The types of products and services covered by the Data Act are deliberately defined very broadly. '*Connected product*' is defined as '*an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user*'. '*Related service*' is defined as 'a *digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product*'.

The Data Act will touch companies of all sizes in almost every sector of the European economy, including manufacturers of smart consumer devices, cars, connected industrial machinery, smart fridges and other home appliances, and any related services which interact with connected products such as streaming services or data analytics software. The Data Act will equally impact on cloud computing providers.

The Data Act will require availability and portability of data generated through the use of IoT devices ('**Connected Products'**) or related services which connect to these devices. It also introduces far-reaching obligations aimed at allowing users to easily switch between cloud service providers, as well as regulating smart contracts.[1]

The Data Act has now been published in the *Official Journal of the European Union* and will enter into force on 11 January 2024. The provisions of the Data Act will begin to apply 20 months from the date of entry into force, meaning affected businesses will need to be ready to comply with the Act by 12 September 2025. Design requirements related to Connected Products will apply to products which are placed on the market in the Union after 12 September 2026.

The Data Act will also introduce a set of rules governing agreements relating to data access and use between companies and prohibiting contractual terms that are considered unfair or abusive. Where contracts are concluded after 12 September 2025, these provisions will automatically apply. For contracts concluded on or before 12 September 2025, these provisions will begin to apply from 12 September 2027.[2]

Because of the Data Act's extensive scope and range of obligations, it is imperative that businesses start preparing now by reviewing their products, practices and policies to ensure compliance. The Data Act implementation will require significant product changes and revision of contract terms. For example, companies should start auditing their data storage policies and considering the changes required to implement the Data Act's extensive data sharing requirements. Contracts governing data sharing and processing practices will also need to be reviewed and likely revised.

For some companies the Data Act will also open up novel business opportunities, and – as the rights under the Data Act are not limited to SMEs – large businesses will be empowered to benefit from this legislation and develop new business models based on third party data becoming accessible under the Data Act.

The main elements and implications of the Data Act are described further below.

2. IoT Devices and Services

The Data Act creates a legal obligation to make data generated from Connected Products available to users of such Connected Products, to third parties if requested by the user, and to public sector bodies in circumstances where there is an exceptional need to do so.

The scope of affected products and services is very broad. Connected Products include all devices and equipment which collect data concerning their use or environment and which can then communicate such data through an electronic communications service, a physical

connection or on-device access. For instance, B2B connected products might include car braking systems, elevators, factory machines capable of collecting data or smart solar panels. In the B2C sphere, examples include home appliances such as smart fridges, smart speakers and cleaning robots, fitness trackers, medical devices, and modern cars. However, products which are primarily designed to display or play content, or to record and transmit content (e.g., personal computers, servers, tablets and smart phones, cameras) are outside the scope of the Data Act.

Obligations related to Connected Products also cover related services. These are digital services which are incorporated in, or inter-connected with, the product at the time of purchase or subsequently connected to the product by a manufacturer or a third-party, and which are essential for the product to perform its primary function. Notable examples include voice assistants, music streaming services which connect to a smart speaker, lifestyle advice applications connecting to fitness trackers, command and control software for industrial machines, and software used for energy optimization in buildings.

Manufacturers of Connected Products are recognised as '*data holders*' in the Data Act. As regards data in scope of the Data Act, the regulation distinguishes between '*product data*' and '*related service data'*. '*Product data'* refers to data generated by the use of a connected product which is designed by the manufacturer to be retrievable by a user, data holder or a third party via an electronic communications service, a physical connection or on-device access. '*Related service data*' covers '*data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider*'. To fall within the scope of the Data Act, '*related service data'* must be related to the use of the device in question.

Under the Data Act, data holders will be obliged to design Connected Products in a manner which provides users with simple and secure access to the data generated by their use. Access should be provided by default, or at the user's request if direct access is not possible. Upon the user's request, data holders must make data '*readily available'*, as well as the metadata that is necessary to interpret and use that data.

Further, if requested by the user, data holders must share data with third parties. Data holders must share the data under fair, reasonable and non-discriminatory terms. To incentivise the generation of valuable data, in B2B relations, data holders may request reasonable compensation when legally obliged to make data available to a data recipient.

One of the hotly debated topics during the Data Act negotiations was how to balance the protection of trade secrets against data sharing requirements. As a general rule, trade secrets must be protected and only disclosed if the data holder and user take all necessary measures prior to disclosure to protect confidentiality. The recitals to the Data Act provide that the obligation to disclose data should be interpreted in such a manner as to preserve the protections afforded under the Trade Secrets Directive (Directive (EU) 2016/943). Data holders should identify trade secrets prior to disclosure and should have the possibility to agree with users, or third parties of a user's choice, on necessary measures to preserve their confidentiality, including by the use of model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct. Where there is no agreement on the necessary measures or where a user, or third parties of the user's choice,

fail to implement agreed measures or undermine the confidentiality of the trade secrets, the data holder should be able to withhold or suspend the sharing of data identified as trade secrets. In '*exceptional circumstances*' and on a '*case-by-case basis*', it may be possible for a data holder to refuse the request for access to data where it can be demonstrated that it faces a threat of '*serious economic damage'* due to the disclosure of trade secrets. The text provides that serious economic damage '*implies serious and irreparable economic loss'*. This exception is likely to be strictly applied. Moreover, the open-ended nature of the exception does not allow affected businesses to rely on a clear legal standard and it remains to be seen how the exception will be interpreted by the CJEU.

3. **Gatekeepers**

The Data Act notes that '*start-ups, small enterprises, enterprises that qualify as a medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC and enterprises from traditional sectors with less-developed digital capabilities struggle to obtain access to relevant data*'. On that basis, the Data Act's aim is for such smaller companies to be the primary beneficiaries of the legislation. On the other hand, the Data Act prevents companies that are designated as gatekeepers under the EU's Digital Markets Act from being able to receive data (with the exception of their cloud services).

4. **Cloud Switching**

The Data Act will have a significant impact on both public and private cloud computing services by requiring providers to facilitate switching across cloud and edge offerings.

The Data Act introduces a number of contractual, commercial and technical requirements to facilitate the transfer of data from one provider to another. Affected providers will be required to remove '*obstacles to effective switching*' between their own and competing cloud services, which can be commercial, technical, contractual and organisational. They will also no longer be permitted to charge costs if a user wishes to remove its data from its current provider and switch to a new one. The Data Act, however, states that cloud services providers are not required to develop new technologies or services, disclose digital assets protected by intellectual property or take measures compromising the integrity and security of their service.

The cloud switching obligations in the Data Act leave scope for interpretation and the exact nature of their application is difficult to predict. Additionally, given the complexity of cloud switching, especially for certain types of workloads, it remains to be seen how regulators will approach the implementation of this requirement in practice given the apparently limited attention paid to the technical complexities when formulating vague and broad obligations. In order to build a defence, it likely will be important for a company that faces significant technical hurdles to comply with the requirements under the Data Act to develop strategies for the documentation of those hurdles and the efforts put into compliance.

5. **Smart Contracts**

One of the Data Act's more controversial requirements concerns the design of smart contracts. A smart contract is defined very broadly as '*a computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and*

ensuring their integrity and the accuracy of their chronological ordering'. The Data Act does not distinguish between just digital contracts and smart contracts utilizing distributed ledger technology, and may also potentially affect existing smart contracts on public blockchains.

Vendors of an application using smart contracts must ensure that smart contracts offer '*access control mechanisms*' and a '*very high degree of robustness*'. They also need to ensure that smart contracts contain a kill switch which is a mechanism that can either destroy the contract or pause its operation '*to terminate the continued execution of transactions*.'

While the full extent of businesses affected by these requirements is difficult to ascertain, any provider of a smart contract application should carefully consider how to comply with the Data Act.

6. **Interplay with the GDPR**

Unlike Regulation (EU) 2016/679 (the "**GDPR**"), which applies to personal data only, the Data Act has a broader scope since it applies to both personal and non-personal data. As a consequence, and as clearly stated in Article 1(5) of the Data Act, this regulation is without prejudice to EU and national law on the protection of personal data and privacy, in particular the GDPR and the Directive 2002/58/EC (the "**e-Privacy Directive**"). This means that insofar as users are data subjects, all of the rights granted under the Data Act complement the rights granted under the GDPR such as the right of access and the right to data portability. However, in order to limit the risk of an interpretation or implementation of the Data Act that could be inconsistent with the existing data protection legal framework, the Data Act clearly provides that in the event of a conflict between the Data Act and EU law on the protection of personal data and privacy, or national law adopted in accordance with such EU law, such EU or national law should prevail.

7. **Enforcement**

While the Data Act introduces harmonized rules across the EU, it will be enforced by national authorities and it is left to the individual Member States to determine which authority (or indeed, authorities) they wish to designate for this purpose. The Data Act also leaves the determination of applicable penalties in the hands of Member States, subject to some minimum requirements set out in the text. Penalties must be '*effective, proportionate and dissuasive'*, and Member States must notify the Commission of the substance of these penalties by 20 months from the date of entry into force, i.e. by 12 September 2025.

The Commission will nevertheless support Member States in their enforcement by adopting guidelines and implementing legislation on, e.g., reasonable compensation for shared data, interoperability specifications, model contractual terms or harmonized smart contract standards. For those reasons, companies should put in place a coordinated and centralized EU-wide compliance strategy.

8. **Why should you care?**

The Data Act is an extensive and highly complex piece of legislation which will have wide-ranging implications across industries and enterprises of all sizes. Given the numerous

exceptions, to an extent open-ended provisions and seemingly unclear definitions, a lot of uncertainty remains about how the Data Act will be enforced in practice. One thing is clear, however: affected businesses should begin preparing their compliance strategies and review product designs and relevant contractual frameworks right away. Such preparation will also require a closer analysis of the legal and technical issues relevant for each particular business and product as well as the interfaces to other relevant legal frameworks that may apply to, or limit, data flows under the Data Act, including the GDPR and, with respect to gatekeepers, the Digital Markets Act.

---

[1] I.e., computer programs used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering.

[2] Provided they are of indefinite duration or due to expire at least 10 years from 11 January 2024.

The following Gibson Dunn attorneys prepared this update: Ahmed Baladi, Nicholas Banasevic*, Stéphane Frank, Kai Gesing, Joel Harrison, Christian Riis-Madsen, Robert Spano, Ciara O'Gara, and Jan Przerwa.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the issues discussed in this update. Please contact the Gibson Dunn lawyer with whom you usually work, any leader or member of the firm's Antitrust and Competition or Privacy, Cybersecurity & Data Innovation practice groups, or the authors:

Antitrust and Competition:
Nicholas Banasevic* – Managing Director, Brussels (+32 2 554 72 40, banasevic@gibsondunn.com)
Rachel S. Brass – Co-Chair, San Francisco (+1 415.393.8293, rbrass@gibsondunn.com)
Stéphane Frank – Brussels (+32 2 554 72 07, sfrank@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33 180, kgesing@gibsondunn.com)
Ali Nikpay – Co-Chair, London (+44 20 7071 4273, anikpay@gibsondunn.com)
Cynthia Richman – Co-Chair, Washington, D.C. (+1 202.955.8234, crichman@gibsondunn.com)
Christian Riis-Madsen – Co-Chair, Brussels (+32 2 554 72 05, criis@gibsondunn.com)
Stephen Weissman – Co-Chair, Washington, D.C. (+1 202.955.8678, sweissman@gibsondunn.com)

Privacy, Cybersecurity and Data Innovation:
Ahmed Baladi – Co-Chair, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, Palo Alto (+1 650.849.5327, aberinger@gibsondunn.com)
Joel Harrison – London (+44 20 7071 4289, jharrison@gibsondunn.com)
Jane C. Horvath – Co-Chair, Washington, D.C. (+1 202.955.8505, jhorvath@gibsondunn.com)

Alexander H. Southwell – Co-Chair, New York (+1 212.351.3981, asouthwell@gibsondunn.com)
Robert Spano – London/Paris (+44 20 7071 4902, rspano@gibsondunn.com)