ENTRY INTO FORCE OF THE EU DATA ACT: WHAT ARE THE KEY REQUIREMENTS?

The Data Act[1] was published in the Official Journal of the European Union on 22 December 2023 and entered into force on 11 January 2024. The majority of the Data Act's provisions will apply from 12 September 2025.

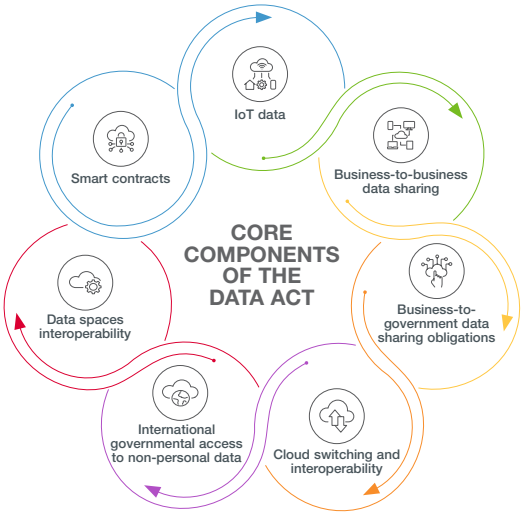
The Data Act is a major piece in the EU's data strategy and, beyond this, its broader digital strategy. It has important ramifications for a broad range of businesses.

It seeks, in particular, to foster innovation within the EU by increasing access to, and re-use of, data concerning the performance, use and environment of connected products and related services. Such data is expected to increase in volume and value, particularly as the Internet of Things continues to expand.

Another key aspect of the Data Act is the introduction of a range of provisions which aim to facilitate switching between data processing services (such as cloud services).

The Data Act also includes: (i) conditions applicable to business-to-business data sharing more broadly; (ii) rights for public sector access to privately held data in cases of exceptional need; (iii) requirements relating to data spaces interoperability; and (iv) requirements for smart contracts that execute data sharing agreements.

The Data Act has extraterritorial effect and may apply to certain entities operating in the EU market regardless of where they are based. For instance, manufacturers of connected products placed on the market in the EU and entities providing data processing services to customers in the EU will be subject to the Data Act.



Member State legislation is being enacted in anticipation of the Data Act becoming applicable. For example, in France, lawmakers are currently working on an important bill that includes cloud-related provisions such as restrictions on switching charges and requirements for interoperability, digital asset portability, functional equivalence, transparency and safeguards regarding unauthorised third-country data access. Such initiatives may raise a number of questions and challenges as already underlined by the Commission, including regarding consistency, articulation and compatibility with EU tech regulations.[2]

1 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). The Data Act text published in the EU's Official Journal can be found here.

2 This bill also addresses other digital issues linked for instance to the Data Governance Act, online content and the Digital Services Act, the Digital Markets Act and AI developments.

Data Act overview and update

Core components of the Data Act include:

1. Removing barriers to IoT data access and re-use

Redefined rules for access and re-use of data concerning the performance, use and environment of connected products and related services which are placed on the market in the EU (subject to certain exemptions based on entity size), including:

- Data access design requirements for the design, manufacture and provision of connected products and related services;
- Rights for users of connected products and related services (including companies and individuals) to require that data holders make such data available to them or to third parties (with requirements regarding, notably, the format, accessibility, security and quality of data, as well as immediacy and continuity of access) – subject to limited restrictions and exemptions (including with regard to the disclosure of trade secrets);
- User transparency obligations for providers of connected products and/or related services;
- Certain data usage and sharing restrictions for data holders; and
- Restrictions on users and third-party data recipients regarding the use, sharing and storage of the obtained data.

2. Framing business-to-business data sharing

- Requirements and restrictions (e.g., with regard to the disclosure of trade secrets) regarding the modalities of making data available and the contracting terms to be entered into between data holders and data recipients, where data holders are obliged to make data available under: (i) the Data Act obligations regarding connected devices and related services data; or (ii) other EU or Member State law that enters into force after the Data Act becomes applicable.
- Requirements and restrictions regarding fairness of contractual terms unilaterally imposed by one business on another in relation to any private sector data access. Note: non-binding model contractual terms on data access and use are to be recommended by the Commission.
- Provisions to frame the compensation that may be agreed for making data available, including to ensure it is non-discriminatory and reasonable and requisite information is provided to the data recipient. The Commission will issue guidelines on the calculation of reasonable compensation under the Data Act, although the Union or national laws could provide for a lower (or no) compensation.
- Provisions framing dispute settlement between data holders and data recipients.
- Provisions permitting application of appropriate technical protection measures for ensuring data access is secure and compliant with the Data Act and any contractually agreed terms.
- Provisions addressing deceptive practice or unauthorised use or disclosure of data, including the possibility to require erasure of compromised data or to put an end to the production, offering or placing on the market of goods, services, or derivative data based thereof and destroy infringing goods under specific circumstances leading to significant harm.

3. Providing certain business-to-public bodies and institutions data sharing obligations

Provisions for access by public sector bodies and certain EU institutions to data held by private sector data holders in cases of “exceptional need” (including, for example, the need to respond to a public emergency).

- Conditions applicable to the type of data requested which must be specific, justified and proportionate to the exceptional need.
- Restrictions on public bodies regarding the obtained data include only using it for the defined purpose, implementing measures to protect it (including when it relates to trade secrets), and deleting it as soon as it is no longer needed (unless agreed otherwise with the data holder) as well as special provisions intended to protect trade secrets during data use and data disclosure to third parties.
- For mixed data sets (of personal and non-personal data) data holders’ obligation to share anonymised data if possible, otherwise pseudonymised or aggregated data (to which GDPR will apply).
- Limited grounds for refusing access (e.g. the requested data is unavailable).
- Limited (costs-focused) financial compensation rights for data holders for certain types of data access.
- Modalities of sharing of data obtained in this context with research organisations or statistical bodies.

4. Facilitating cloud switching and interoperability

Requirements aimed at facilitating switching between data processing services (such as cloud and edge services) that are offered to customers in the EU and are not custom-built or provided as a temporary testing version, including:

- Obligations for providers of data processing services to not impose (or to remove, if they exist) obstacles inhibiting termination of services, entering into new agreements with other providers, unbundling data processing services from one another and porting their exportable data (and in some cases digital assets) to other providers or an on-premise system – with some exceptions, e.g. provider data protected by IP or which constitutes a trade secret, or where the contemplated operations could create security and service integrity risks.
- Requirements and restrictions regarding (i) contractual terms relating to switching between providers (or to an on-premise system) and (ii) contractual transparency obligations regarding international access and transfer of non-personal data. Note: non-binding standard contractual clauses for cloud computing contracts are to be recommended by the Commission.
- Information obligations for providers of data processing services, including regarding providing customers with information on procedures for switching and porting to their service and a reference to an up-to-date online register hosted by the service provider, which contains details on the data structures, data formats as well as the relevant standards and open interoperability specifications.
- An obligation for all parties to collaborate in good faith to enable effective and timely switching between services.
- Requirements for providers to facilitate functional equivalence (re-establishing a minimal level of functionality for the same service type in the environment of the destination service, on the basis of the customer's exportable data and digital assets) when customers switch to a new data processing service, in relation to the features that both the source and destination service providers offer and where the destination service delivers a materially comparable outcome in response to the same input.
- Interoperability requirements for providers, including to enhance portability of digital assets, facilitate functional equivalence (see above) and facilitate in-parallel use of data processing services. There are requirements regarding compliance with open standards and interfaces in some cases. The Commission is empowered to adopt common specifications for further interoperability standards.
- Requirement for charges related to switching activities to be abolished three years after the Data Act comes into force (and gradually diminished beforehand).

5. Providing safeguards re international governmental access to and transfers of non-personal data

Providers of data processing services are required to take certain measures to prevent international governmental access to, or transfer of, non-personal data held in the EU where such access/transfer would conflict with EU or Member State law.

- Decisions of third-country courts are recognised if they are based on an international agreement with the EU or Member State.
- Some exceptions based on the third-country's judicial systems and the nature of the decision or judgment (but with requirements to consult with competent EU authorities in some cases regarding whether the conditions for exception are met).
- Requirement for data processing services providers to minimise the data shared in that context and to inform data holders of access requests by third-country administrative authorities prior to complying with such requests (with an exception for preserving the effectiveness of law enforcement activity).

6. Facilitating data spaces interoperability

Requirements applicable to participants of data spaces that offer data or data services to other participants. These requirements are aimed at facilitating interoperability of data, data sharing mechanisms and services, and of the common European data spaces. These include requirements relating, for instance, to dataset content, use restrictions, data collection methodology, quality and uncertainty of the data, data formats and structures, technical means to access the data and their terms of use and quality of service. These requirements can have a generic nature or concern specific sectors.

7. Defining essential requirements re smart contracts

Requirements for vendors of applications using smart contracts in the context of executing an agreement to make data available (or, in the absence of a vendor, requirements for persons whose business involves deploying such smart contracts for others). These include obligations relating to robustness and access control, safe termination, or interruption of the operation of the smart contract, and consistency with the terms of the relevant data sharing agreement. Harmonised rules are expected to be adopted either by EU standardisation bodies upon the Commission's request.

Enforcement

National competent authorities: Each Member State must designate at least one competent authority as responsible for applying and enforcing the Data Act, which must be well-provisioned with human and technical resources. They must communicate the names and respective tasks and powers of these designated competent authorities to the Commission which will maintain a public register of competent authorities. Generally, entities which fall within the scope of the Data Act will be subject to the competence of the Member State where they are established. If they are established in multiple Member States, they will be subject to the competence of the Member State in which they have their main establishment (defined further in the Data Act). A European Data Innovation Board is to be set up as a Commission expert group in which competent authorities are represented, to support consistent application of the Data Act.

Penalties: Each Member State must lay down rules for "effective, proportionate and dissuasive" penalties for violations of the Data Act (i.e. a national, rather than EU-wide, penalty regime – fines could therefore vary from country to country for the same violations.) Also, Member States must take account of the recommendations of the European Data Innovation Board, and non-comprehensive criteria described in the Data Act. For infringements of certain obligations under the Data Act, the supervisory authorities referred to in the GDPR and in the Regulation (EU) 2018/1725 on the processing of personal data by EU institutions, bodies, offices and agencies may, within their respective scope of competence, impose administrative fines in line with these Regulations.

A broader EU legislative context

The Data Act should be considered alongside other existing and emerging laws within and outside the EU. In some cases, these will interact with the Data Act's obligations or have similar practical implications. Within the EU examples of the wider legislative landscape include:

DGA: The Data Act complements the Data Governance Act (DGA) – which entered into force on 23 June 2022 – as part of the European Data Strategy. While the DGA introduced broad frameworks for data access and sharing within the EU – including setting conditions for reuse of protected public sector data and trusted mechanisms for voluntary data sharing – the Data Act notably introduces specified rights of access to privately held data as well as mandatory requirements and standards for facilitating data reuse.

GDPR: The term "data" in the Data Act comprises both personal and non-personal data, but requirements regarding personal data processing (including access and use) in the Data Act are subject to compliance with the GDPR – requiring an understanding of how these requirements will layer and interact when they apply to mixed data sets.

DMA: The Data Act also interacts with the Digital Markets Act, for example by prohibiting the transfer of connected product data to undertakings designated as "gatekeepers" under the DMA.

(See our overview of the *DGA*; our article *The EU Data Act proposal: data access*; and our paper *The EU Data Act and its interaction with Competition, Privacy and other recent regulations*.)

IP: The Data Act states that it is without prejudice to EU and Member State laws for the protection of intellectual property, with the exception that the sui generis right provided for in Directive 96/9/EC (the Database Directive) shall not apply when data is obtained from, or generated by, a connected product or related service falling within the scope of the Data Act. Given the subject matter of the Data Act, the potential for conflict with IP rights other than trade secrets and database rights (such as copyright and patents) is limited. However, to mitigate the risk of unforeseen impacts on IP protection, an initial evaluation of the effects of the Regulation on the protection of intellectual property and trade secrets is to be carried out as part of a wider impact assessment by 12 September 2028.

When will the Data Act start to apply?

The majority of the Data Act's provisions will apply from 12 September 2025, with exceptions for: (i) obligations for design, manufacture and provision of connected devices and related services, which are expected to apply from 12 September 2026; and (ii) provisions on unfair contractual terms for data access between businesses, which are expected to apply from 12 September 2027 for certain contracts of long-running or indefinite term that were concluded on or before 12 September 2025.

Next steps for businesses

A broad range of business across the world will need to understand whether they are in-scope of the Data Act and, if so, analyse and plan how to implement changes to adhere to the obligations it imposes, as well as strategise for any potential opportunities it may bring. This includes, in particular:

Businesses that manufacture, design or provide connected products or related services which are placed on the market in the EU – in particular, these businesses should analyse and plan for relevant data access design requirements and user transparency requirements.

Businesses that have the right to use and make available connected products and related services data, where such products or services are placed on the market in the EU – in particular, these businesses will need to implement changes to address the practical aspects of providing access to data and their obligations regarding restricting certain data use, as well as review the contracting terms they use in relation to data access and their transparency statements for connected products and related services.

Businesses that would benefit from access to connected products and related services data (e.g. in relation to device repair or provision of connected services) – in particular, these businesses will be seeking to understand what opportunities the Data Act may afford, for example in relation to receipt of data from a data holder upon an EU user's request and understand the related obligations.

Businesses that make data available to businesses in the EU on unilaterally imposed terms – they should be aware of, and plan to make changes to comply with, the requirements and restrictions for such terms.

Providers of data processing services, including cloud and edge services, providing such services in the EU – they will need to analyse and plan for a range of obligations relating to facilitating switching between data processing services.

Data holders that make data available to data recipients in the EU – they should be aware of public sector access rights, and consider steps that they would take in relation to data protection compliance and protection of intellectual property and trade secrets.

Participants of European data spaces that offer data or data services to other participants – these businesses should be aware of requirements relating to facilitating interoperability.

Vendors of applications using smart contracts and those who deploy smart contracts for others as part of their business in the context of executing an agreement – these businesses should be aware of obligations relating to such smart contracts.

AUTHORS:

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Rita Flakoll
Global Head of Tech Group Knowledge
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

Alexander Kennedy
Counsel
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Alexandre Manasterski
Counsel
Paris
T: +33 1 4405 5971
E: alexandre.manasterski@cliffordchance.com

Herbert Swaniker
Senior Associate
London
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

Ketevan Zukakishvili
Lawyer
Brussels
T: +32 2 533 5918
E: ketevan.zukakishvili@cliffordchance.com

CONTACTS:

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Devika Kornbacher
Partner
Houston
T: +1 713 821 2818
E: devika.kornbacher@cliffordchance.com

Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com

Claudia Milbradt
Partner
Dusseldorf
T: +49 211 4355 5962
E: claudia.milbradt@cliffordchance.com

Holger Lutz
Partner
Frankfurt
T: +49 69 7199 1670
E: holger.lutz@cliffordchance.com

Dieter Paemen
Partner
Brussels
T: +32 2 533 5012
E: dieter.paemen@cliffordchance.com

Gunnar Sachs
Partner
Dusseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Josep Montefusco
Partner
Barcelona
T: +34 93 344 2225
E: josep.montefusco@cliffordchance.com

Thomas Voland
Partner
Dusseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Michael Dietrich
Partner
Dusseldorf
T: +49 211 4355 5542
E: michael.dietrich@cliffordchance.com

Don McCombie
Partner
London
T: +44 207006 2010
E: don.mccombie@cliffordchance.com

Stavroula Vryna
Partner
London
T: +44 207006 4106
E: stavroula.vryna@cliffordchance.com

Nelson Jung
Partner
London
T: +44 207006 6675
E:nelson.jung@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 306
E: simon.persoff@cliffordchance.com

Jennifer Chimanga
Partner
London
T: +44 207006 2932
E: jennifer.chimanga@cliffordchance.com

André Duminy
Partner
London
T: +44 207006 8121
E: andre.duminy@cliffordchance.com

Zayed Al Jamil
Partner
London
T: +44 207006 3005
E: zayed.aljamil@cliffordchance.com

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Phillip Souta
Global Director of Tech Policy
London
T: +44 207006 1097
E: phillip.souta@cliffordchance.com

Jaap Tempelman
Senior Counsel, Amsterdam Tech Group Co-Head
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Andrei Mikes
Counsel
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Manel Santilari
Abogado
Barcelona
T: +34 93 344 2284
E: manel.santilari@cliffordchance.com

Shruti Hiremath
Senior Associate
London
T: +44 207006 3075
E: shruti.hiremath@cliffordchance.com

Ella Ditri contributed to the drafting of this overview