fieldfisher

An overview of the new EU Data Act

Table of Contents

Introduction

Introduction

The Regulation on harmonised rules on fair access to and use of data (**"Data Act"**) is a key part of the EU's strategy to make the EU a leader in a global, data driven economy.

The Data Act seeks to set out rules on the availability of data in connected products or related services; facilitating the switching between providers and protecting such data from unlawful access as well as the development of interoperability standards for the data to be accessed, transferred and used.

The Data Act applies to datasets irrespective of whether or not they contain personal data. This comes with challenges in that it overlaps with the General Data Protection Regulation ("**GDPR**") and other (EU wide or EU member state) data protection legislation. In case of conflict between the Data Act and applicable EU / member state data protection regulations, the data protection regulations will prevail.

Timescale

The timer of a 20-month transition window started on 11 January 2024. Therefore, the Data Act will be applicable from 12 September 2025. Some provisions only come into effect at later days (subject to certain conditions).

Enforcement

As a Regulation (not a Directive) the Data Act will apply automatically across EU member states. However, there will be local law variations on the way in which the Data Act is enforced as each EU member state will have to set out the penalties applicable to infringements and designate a competent authority in their local country.

Member States have until 12 September 2025 to notify the Commissioner of its rules regarding penalties for infringements. This mean that companies may have to prepare for the Data Act's implementation before - and without knowing - the scale of penal risk. That said, the Data Act does outline the approach towards penalties, it should be 'effective, proportionate and dissuasive'. The same three words that the GDPR uses in its approach to fines!

Material and Territorial scope

Material and Territorial Scope

The scope of the Data Act

The scope of the Data Act is far reaching. It will be of particular concern to the following:

- Manufacturers of connected products who offer their products to the EU market and providers of related services.
- Users (natural or legal persons) in the EU of connected products or related services.
- Public sector bodies, who may request access to data in exceptional circumstances.
- Providers of data processing services to customers in the EU (e.g. cloud service providers).
- Participants in data spaces and vendors of applications or professionals using smart contracts.

Connected products are, of course, increasingly appearing in society. The Data Act lists examples- vehicles, health and lifestyle equipment, ships, aircraft, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery – indicating the broad scope of products intended to fall within its remit.

The Data Act includes a broad definition of Data Holder meaning a natural or legal person who has the right or obligation to use and make available data, including data in connected products (product data)[1] or related service data[2] generated during the provision of a related service. In this context:

- 'product data' refers to data designed to be retrievable from the connected product by a user, data holder, manufacturer or third party; and
- 'related service data' refers to data which are related to the connected product and generated during the provision of a related service by the provider. This includes data generated by a user interface or related service including applications indicating hardware status and malfunctions.

The Data Act is clear that the data to be made available should include the relevant metadata. Data that sensor equipped connected products generate when the user records, transmit, display or play content, as well as the content itself, are not covered by this Regulation. Data obtained, generated or accessed from the connected product which was transmitted to it for the purpose of storage or other processing on behalf of other parties (not by the user) (e.g. servers or cloud infrastructure) is also out of scope of this Act.

The Regulation recognises a small number of very large enterprises have emerged with considerable economic power in the digital economy and this Regulation aims to facilitate access by smaller entities (in particular, there are proportionate obligations in relation to micro, small and medium-sized enterprises)[3].

Does it have scope outside of the EU?

In addition to having a broad material scope (as explained above), the Data Act has a broad extra-territorial scope (similar to the GDPR). A company that makes connected products available or offers services to individuals in the EU – even if the company is not established in the EU – will be in scope. This means that **a company does not need to be physically present within the EU in order to be subject to the Data Act.** For example, a US medical device manufacturer business targeting the EU market would be in scope.

By virtue of the UK leaving the EU, the Data Act is not part of the UK statute book – however, it will still apply to UK companies who fall within scope.

1 'product data' means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer.

2 'related service data' means 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.

3 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

What type of obligations does it impose?

The Data Act aims to set out a framework for sharing of "product data" and "related service data", ease the switching between providers of data processing services, introduce safeguards against unlawful data transfer and provide for the development of interoperability standards for data to be reused between sectors.

The ambition is that it will enable both individuals and businesses to have more control over their data through a reinforced portability right, allowing for copying or transferring data easily across different services, where data is generated through smart objects, machines, and devices.

Below we have set out a summary of obligations. This is not an exhaustive list but only of those provisions which seem the most generally applicable or of concern.

To make data accessible to users and third parties (Chapter II)

Obligation to make product data and related service data accessible to the user (Chapter II, Article 3)

Connected products and related services need to be **designed and manufactured** so that the data is - where relevant - directly accessible to the user. There are conditions to what this means e.g. by default, easily, securely, free of charge and in a comprehensive, structured, commonly used and machine readable format. A user should be able to directly access the product and service related data.

The **seller / rentor or lessor of a connected product needs to provide certain information to a user** before concluding a contract. This includes the type, format and estimated volume of product data, whether generated continuously or in real time, if data is stored on device or on a remote server, retention duration and how the user may access data, etc.

The **provider of a related service needs to provide certain information to a user** before concluding a contract. This includes the nature, estimated volume and collection frequency of product data / related service data (as appropriate), arrangements for the user to access the data, storage arrangements, retention duration, identity of the data holder, means of communication and sharing, etc.

Rights and obligations of users and data holders with regard to access, use and making available product and related service data (Chapter II, Article 4)

Where data cannot be directly accessed by the user, **data holders need to make the data readily available** without undue delay and, of the same quality as is available to the data holder. There are other conditions too, including that this shall be done on the basis of a simple request through electronic means.

Further provisions include **contractual restrictions, how the data holder provides choices to users, how a data holder can verify the identity of a user, and protections regarding trade secrets**. There are also restrictions on how the user can use the data obtained (i.e. not to abuse gaps in technical infrastructure) and conditions on the use of non-personal data by data holders.

If the requested data is personal data of an individual that is not the user, the data holder must not make that data available to the user unless there is **a valid legal basis** under Art 6 and a condition under Art 9 GDPR. Conditions of Art 5 (3) ePrivacy Directive[4] also need to be fulfilled.

4 Article 5(3) of the ePrivacy Directive (2002/58) is the restriction on accessing information stored on a user's device, or storing information on that device, sometimes known (colloquially) as the "cookie rule". See our blog on new guidance on this provision.

What type of obligations does it impose?

Right of the user to share data with third parties (Chapter II, Article 5)

Obligations on the data holders to **make data readily available to a third party upon request of a user**. There are conditions on the format in which this data should be provided.

In essence, this is somewhat like the portability right in the GDPR.

There are also provisions which will be relevant including: (i) making it clear that this does not apply to products not yet placed on the market; (ii) stating how a data holder can verify a third party; (iii) providing protections regarding trade secrets; and (iv) setting out the interrelationship with the GDPR.

Obligations of third parties receiving data at the request of the user (Chapter II, Article 6)

Provides **obligations on a third party in relation to data received pursuant to Article 5**. A third party is obliged to process the data made available to it only for the purposes and under the conditions agreed with the user and national law. Specific restrictions on third party use are also specified.

Obligations for data holders obliged to make data available pursuant to Union law (Chapter III, Articles 8-12)

This Chapter sets out **statutory sharing obligations**.

This includes a framework to apply to a data holder when it is required to make data available to a data recipient (under Article 5 above) or under union and national law. It provides that the data holder should enter into an agreement with the data recipient, which should be fair and reasonable non-discriminatory terms and conditions and in a transparent manner.

The data holder can charge for making the data available. However, compensation for making data available in B2B relations is to be non-discriminatory and reasonable and can be more than covering costs; they can include a margin. The Commission is obliged to **adopt guidelines on the calculation of reasonable compensation**.

Obligations are placed on the data holder to apply **appropriate technical protection measures** on the unauthorised use or disclosure of data. This includes smart contracts and encryption. While there is little detail on the technical measures to be applied, we note the reference to ‘as appropriate'.

Unfair contractual terms related to data access (Chapter IV)

These requirements seek to address any potential imbalance in the position between different organisations who share data under the Data Act.

Any unfair terms (those grossly deviating from good commercial practice in data access and use, contrary to good fair and fair dealing) which are unilaterally imposed will not be binding. For instance, the Data Act sets out that terms excluding or limiting the liability of the party for intentional acts or gross negligence are unfair. Other terms that are presumed unfair include allowing the party who imposed the terms to access and use the data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other party, in particular when the data contains commercially sensitive data or is protected by trade secrets or other IP rights.

The requirement that a term must be "unilaterally imposed" suggests that these provisions will not apply to negotiated contracts. The contracting party that supplied the contractual terms bears the burden of proving that that term has not been unilaterally imposed.

What type of obligations does it impose?

Obligation to make data available to public sector bodies (Chapter V)

Data holders may be required by the Commission, the European Central Bank or a Union body to make data available to the body if it requires the use of the data (or any metadata needed to interpret or use that data) to carry out its statutory duties in the public interest.

This is not a blanket requirement as the need to use the data will be limited in time and scope and may only apply in certain circumstances which in summary are where exceptional circumstances apply and the body cannot obtain the data elsewhere. Micro and small enterprises are exempt of some requests.

The Data Act sets out conditions for the request of such information (e.g. the information that the request should include and that the request should be specific and proportionate) and limitation to the re-use of the data by the requesting body. The data holder may decline or seek to modify the request without undue delay and no later than 5 working days (in the event of a public emergency) or 30 working days in other cases on grounds such as that it has no control of the data requested or that the request does not meet the requirements of the Act.

If the dataset contains personal data, the data holder will have to anonymise it unless the body requires the disclosure of personal data. Compensation may be available for data holders sharing data.

Obligations in relation to switching between data processing services (Chapter VI)

The Data Act sets out requirements for **cloud providers to facilitate their switching to another** (or many) provider of data processing services (of the "same service type"[5]) or to its own ICT infrastructure. All parties (including the new service provider) must **cooperate in good faith** in order to make the switching process effective.

Cloud providers cannot set out obstacles to stop customers from: (i) terminating the contract; (ii) engaging another provider; (iii) porting the customers exportable data and digital assets to the new provider or on-premises ICT infrastructure; (iv) achieving functional equivalence in the use of the new services; or (v) unbundling data processing services from other processing services, where technically feasible.

The contract for the cloud services should set out the rights of the customers and be made available to the customer in a way that it may be stored and reproduced by the customer. The Data Act sets out a list of minimum sets of terms that the contract should cover, including:

- to allow for the customer to give a maximum two months notice to initiate switching services to another provider (or inhouse);
- to allow the switching within a maximum of a further 30 days;
- the agreement will terminate on either two months' notice – if no switching services are needed because the customer only requests to erase the data – or, at the end of the switching process;
- to provide reasonable assistance to the customer and third parties in the switching process;
- to provide clear information and act with due care in order to maintain business continuity;
- to ensure a high level of security throughout the switching process;
- to provide a detailed description of the data and digital assets that can be ported during the switching process;
- an agreed transitional period and a minimum retrieval period of 30 days; timeframes may be negotiated by the parties if the provider can technically justify the need for a longer period; and
- full erasure of the data after the retrieval period.

5 The Data Act defines 'same service type' as "a set of data processing services that share the same primary objective, data processing service model and main functionalities". There is much uncertainty as to what types of service are in fact covered by this. Recital 81 recognises a distinction between services with the same "type" and those which – although the primary objective is the same –fall at a more granular level into different "subcategories" of similar services.

What type of obligations does it impose?

The cloud provider has **transparency obligations** which require it to make information on the procedures for switching available and reference to an on-line register hosted by the provider with information about the data structures and formats as well as relevant standards for interoperability specifications.

Cloud services websites will have to provide certain information, including the technical, organisational and contractual measures adopted to **prevent international governmental access** to or transfer of non-personal data held in the EU.

Switching charges may be not applied after 12 January 2027. Any charges before that must be communicated to the customer in the contract terms.

Unlawful international governmental access and transfer of data (Chapter VII)

Obligations on the providers of data processing services to take all adequate technical, organisation and legal measures, including contracts, in order to prevent international and third country governmental access and transfer of non-personal data in conflict with Union or member state law.

What next?

What next?

Given the broad scope of the Data Act, all companies should consider whether they are in scope of the Data Act and if so prepare and budget accordingly for its implementation.

If you are caught, there will be many legal and technical aspects to consider including:

- reviewing contractual terms in light of new user rights and data sharing obligations. (The EU Commission is due to issue non-binding standard terms by 12 Sept 2025; however, preparations for complying with these requirements should take place before that);
- ensuring that your services have the ability to facilitate access and transfer of the information, including meeting the interoperability measures;
- putting procedures in place in order to consider data access requests from users and from other parties, including government bodies; and
- for cloud providers, consider whether the switching obligations may apply to them, and in what circumstances, and if so, their ability to grant this right to its customer; consider new transparency requirements, technical issues and amends to standard terms.

If you have any questions or would like our assistance in considering the scope of the Data Act to your organisation, please contact us using the details provided below.

Renzo Marchini
Partner, Data
+44 330 460 7069
renzo.marchini@fieldfisher.com

Nuria Pastor
Director, Data
+44 330 460 7066
nuria.pastor@fieldfisher.com

Chloe Abbott
Associate, Data
+44 330 460 7349
chloe.abbott@fieldfisher.com