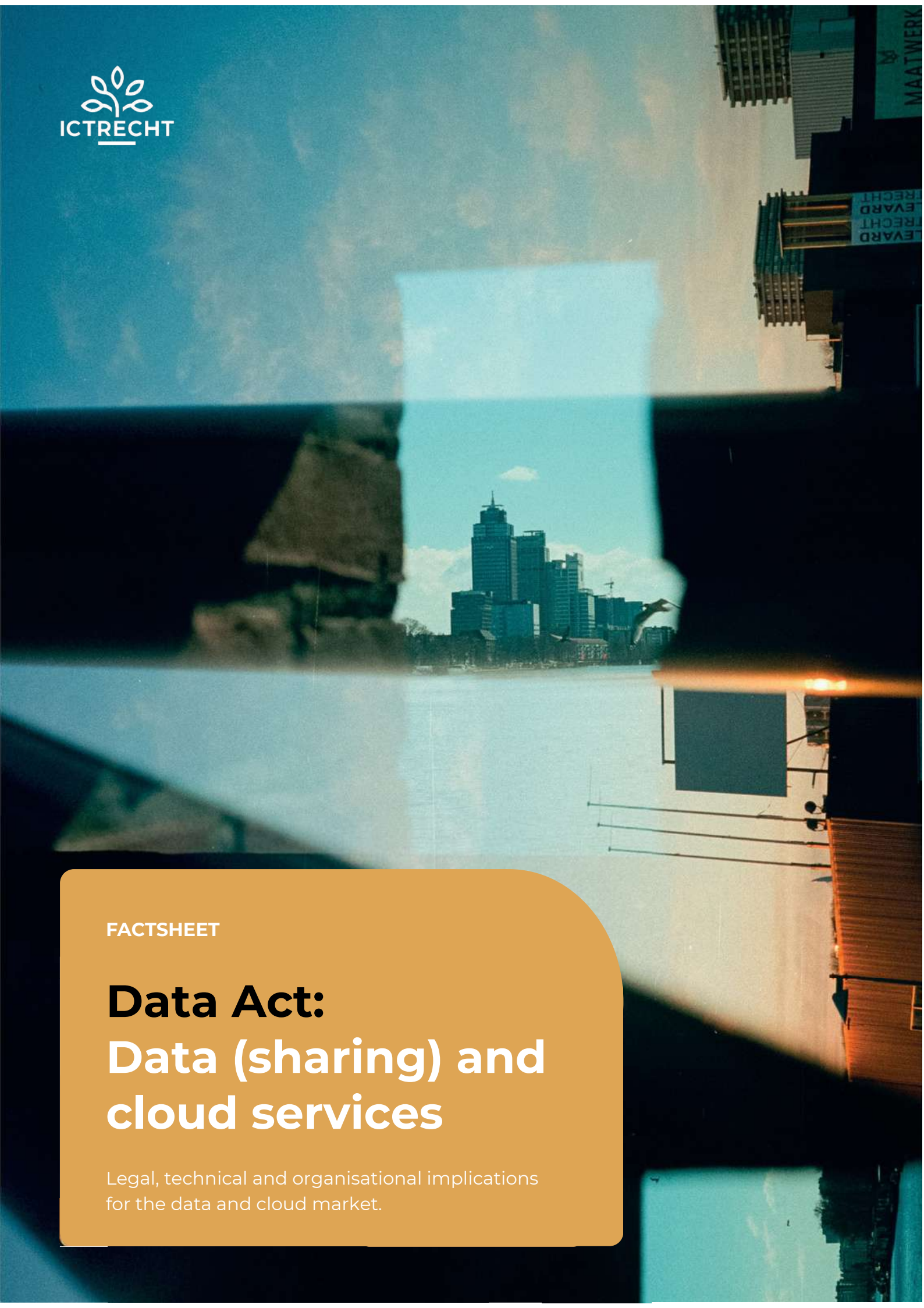


ICTRECHT

FACTSHEET

Data Act: Data (sharing) and cloud services

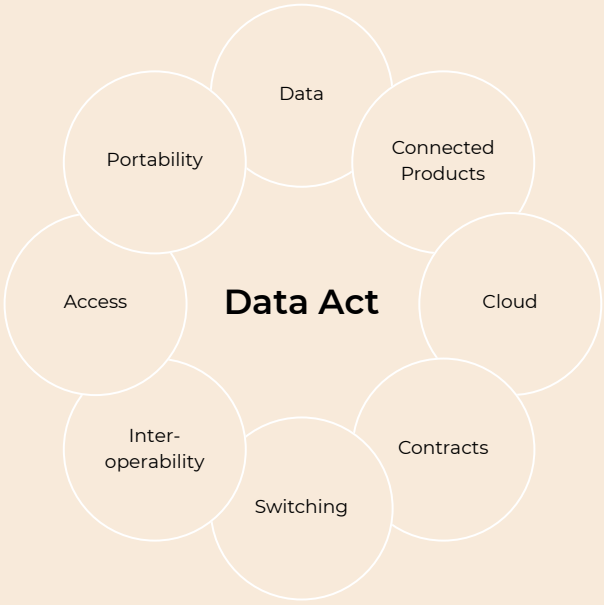
Legal, technical and organisational implications for the data and cloud market.

Unfair terms (including those agreed before 2025)
12 September 2027

Design requirements
12 September 2026

Data Act applicable
11 January 2024

Data Act in force
11 January 2024



Factsheet Data Act

Although data and the value derived from it are becoming increasingly important in and for our society, parties are often still unwilling, unable or not permitted to share data due to various obstacles. These obstacles range from disruptive market power, vendor lock-in and a lack of mutual trust, to data concentration. Customers of cloud services experience barriers when switching to another provider or when they wish to combine and integrate cloud services simultaneously. To remove these obstacles in the data and cloud market, the European Data Act Regulation introduces rules on data access, data quality and data use, switching, interoperability and contractual terms.

The Data Act (Regulation (EU) 2023/2854) contains harmonised rules that promote innovation and contribute to a fairer and more transparent market for data and cloud services, in which consumers and businesses gain greater control over their services and products, data and the use thereof. The Data Act will apply in practice from 12 September 2025 and must be enforceable in the Member States from that date.

The Data Act is framework legislation divided into chapters covering various topics and situations, with different scopes, actors, types of data and types of measures, including:

- **making product data and data from related services available to the user of the connected product or related service (Chapter II);**
- **making data available by data holders to data recipients (Chapter III);**
- **unfair contractual terms relating to access to and use of data between undertakings (Chapter IV);**
- **making data available by data holders to public authorities, the Commission, the European Central Bank and Union bodies, where there is an exceptional need for those data for the performance of a specific task carried out in the public interest (Chapter V);**
- **facilitating switching between data processing services (Chapter VI);**
- **introducing safeguards against unauthorised access by third parties to non-personal data (Chapter VII);**
- **the development of interoperability standards for data spaces, data processing services and smart contracts (Chapter VIII).**

In this factsheet we focus primarily on the chapters of the Data Act shown in bold (rules that may be particularly relevant for access to data, data sharing and data processing services). what connected products and services are that generate and use data. This factsheet covers the following topics:

- What connected products and services are that generate and use data.
- How users of products and services obtain control over generated and recorded data.
- how the transfer of data (data portability) from one system to another is regulated;
- what the legal, technical and organisational requirements are for switching between cloud providers;
- how interoperability of data, infrastructure and applications in cloud services must be arranged;
- which contractual conditions may and must apply to data sharing, switching and interoperability.

This factsheet is structured in such a way that it can also be used as a checklist.

ICTRECHT

Data market: Connected products and related services.

Chapter II of the Data Act governs the use of data generated by (the use of) connected products or related services.

Connected products and related services

Below we explain what is meant by the most relevant terms relating to connected products and generated data.

Subject	What does the Data Act regulate?	Scope
Generated data *(Article 2 (15) and (16))*	Generated data can be valuable to various actors in different ways. For example: • a product provider may, subject to conditions, use the data to improve the product itself, to provide aftermarket services such as maintenance and repair, or to offer other services. • a user of a product or service may use the data to gain insights into their own behaviour or environment.	Generated data includes both data that the user consciously records and all data that the product records as a result of its use. Examples include: • data recorded by sensors, • data registered through interaction with a user interface, • data on the use of a smartphone such as battery data and GPS data. Data generated through the use of, for example, an application, internet browser or streaming service does not qualify as generated data within the meaning of the Data Act.
Connected products *((Article 2(5))*	Connected products are products that generate or collect data about their performance, use or environment, for example by means of a sensor, and that can communicate those data via a network.	There is a wide range of products that collect data and communicate via a network, such as: • refrigerators • watches • medical equipment • industrial machines • thermostats • verhicles and agricultural equipment Products that primarily store, process or transmit data on behalf of parties other than the user, such as servers, do not fall within the definition of connected products.
Related services *(Article 2(6))*	Related services are services, such as software, that are necessary for a product to perform one or more of its functions.	Examples include: • operating system of a connected product • virtual assistants that interact with a connected product or related service.

Actors

To facilitate data sharing from connected products and related services, the Data Act defines several roles, namely: users, providers, data holders and third parties. Specific obligations, responsibilities and/or rights apply to each of these actors. Below is a description of the actors and their main characteristics.

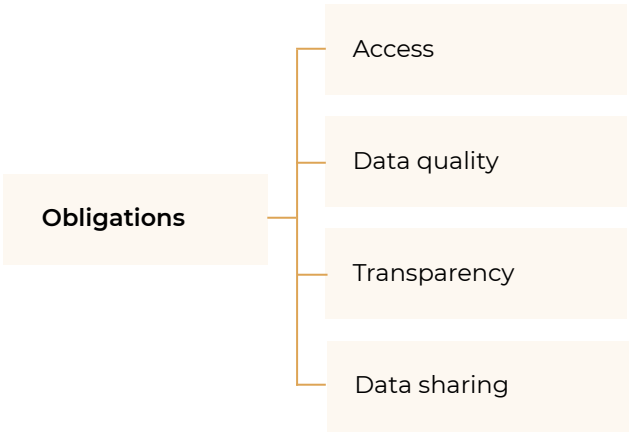
Actor	Description	Features
User *(Article 2(12))*	The user is the natural or legal person who owns, rents or leases a connected product, or who receives a related service.	• Users contribute to the creation of data through their use of products and services. • They are often dependent on the provider or data holder for access to the generated data and; • usually have only limited access to those data.
Provider *(Article 1(3)(a))*	The provider is the seller, lessor or leasing party, and where applicable also the manufacturer, of a connected product, or the supplier of a related service.	• Providers often have access to the generated data. • Providers may use or share the data within the limits of the law.
Data holder *(Article 2(13))*	The data holder is the natural or legal person who, in accordance with the Regulation or other Union or national law, has the right or the obligation to use and make data available.	The data holder may be the provider, but this is not always the case.
Third parties (data recipients) *Article 1(3)(a))*	Third parties are the natural or legal persons to whom data are made available by the data holder at the request of the user.	For example, a technician who gains access to data from a device for maintenance purposes.

Obligations relating to generated data

Data holders have obligations towards users with regard to generated data. These obligations relate to access to data, the provision of data and the quality of data.

When providing and sharing data, this must not prejudice the applicable rights and interests of data subjects and/or third parties. For example, compliance with the GDPR and other protective legislation must be ensured, and the rules on trade secrets and intellectual property rights remain fully applicable.

Below are the key principles governing data access and data sharing, as well as an overview of the main obligations.



Obligations	What needs to be done?	Scope
Access to data *(Article 4(1))*	Data generated by connected products must be easily, securely and free of charge accessible to the user, for example by: • providing direct access to the data, for instance via a display on the product. • where direct access is not possible or feasible, making the data easily and free of charge available in another way, for example via a (web) application.	Data holders are only required to make 'readily available data' available. This means data to which they themselves have access or can obtain access through a simple operation.
Quality of data *(Article 4(1))*	Access must be provided to data of the same quality as that available to the data holder.	The data concerned must be made available in their primary form and in a usable format. This means raw data, including metadata, that are automatically generated and, where necessary, pre-processed to make them understandable and usable, for example by sorting them or converting them into a unit such as kWh, weight, degrees Celsius or kilometres. Where additional investments have been made beyond pre-processing in order to attach new value or insights to the data, that information falls outside the scope of the data that must be shared. This includes, for example, information obtained through the application of complex algorithms that may be protected by intellectual property rights.

Obligations	What needs to be done?	Scope
Transparency obligations *(Article 3(2) and (3))*	Providers of connected products and related services must comply with specific transparency obligations. They must communicate which data a product or service can generate and how users can access those data, for example via a (web) application.	The data holder, being the party that controls access to the data, must grant the user and/or third parties access to the data at the user's request. Users may also share the obtained data themselves with third parties.
Data sharing with third parties *(Article 5(1))*	Data holders must comply with a user's request to provide the data directly to a third party.	Users may also share the data they have obtained with third parties. Undertakings designated as gatekeepers under the Digital Markets Act may not receive data as third parties. Data holders and third parties may not use the available data to gain insight into the economic situation of the user or to undermine the user's commercial position.

Restrictions and prohibitions on data sharing	Data Act
a prohibition on using data to gain insight into the economic situation of the user or to undermine the user's commercial position;	*Article 4(13) and (14)* *Article 5(6)*
a prohibition on using shared data to develop a competing product or to gain insight into the economic situation of the provider or data holder;	*Art 4 (10 en 11)* *Art 5 (5)* *Art 6 (2)*
a prohibition on misusing the technical infrastructure of the data holder.	*Art 4 (11)* *Art 5 (5)*

ICTRECHT

Contractual terms for data sharing

The Data Act also imposes requirements on the information that must be provided before concluding the agreement, as well as other rights and obligations relating to the making available of data.

Contractual terms for data sharing

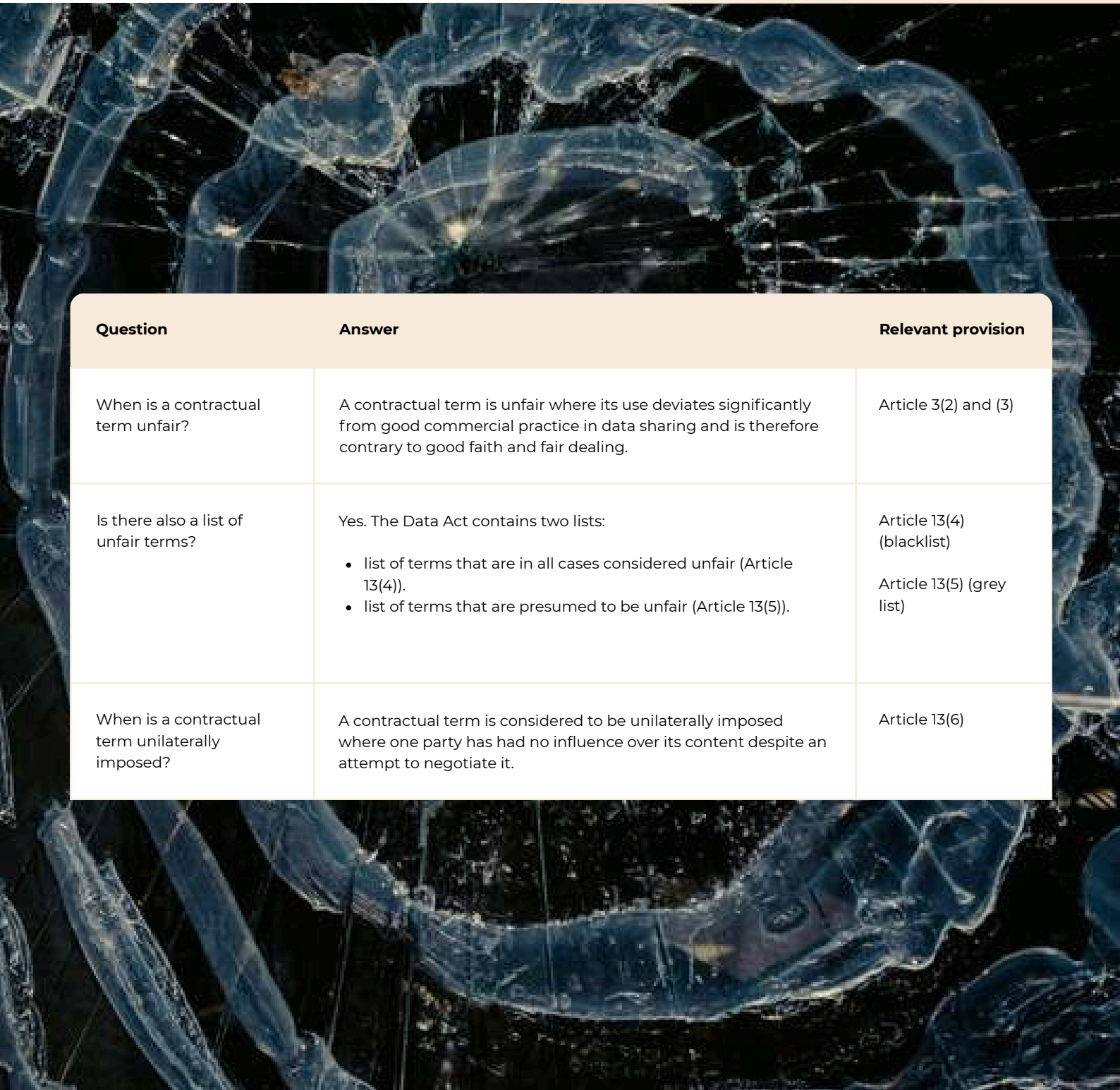
Although parties are free to negotiate the specific terms for making data available, they remain bound by the requirements imposed by the Data Act on those contractual terms. Chapter IV of the Data Act applies to all contractual relationships between undertakings relating to the sharing and use of data.

This chapter determines when contractual terms between businesses relating to access to and use of data are considered unfair.

Unfair contractual terms for data sharing

Chapter IV regulates when a contractual term for data sharing between undertakings is unfair. The objective is to prevent the imposition and use of unfair contractual terms.

Unfair contractual terms relating to access to and use of data that are imposed unilaterally are not binding on the undertaking on which they are imposed. This concerns all unilaterally imposed contractual terms, meaning terms over which a party has had no influence despite attempts to negotiate.



Question	Answer	Relevant provision
When is a contractual term unfair?	A contractual term is unfair where its use deviates significantly from good commercial practice in data sharing and is therefore contrary to good faith and fair dealing.	Article 3(2) and (3)
Is there also a list of unfair terms?	Yes. The Data Act contains two lists: • list of terms that are in all cases considered unfair (Article 13(4)). • list of terms that are presumed to be unfair (Article 13(5)).	Article 13(4) (blacklist) Article 13(5) (grey list)
When is a contractual term unilaterally imposed?	A contractual term is considered to be unilaterally imposed where one party has had no influence over its content despite an attempt to negotiate it.	Article 13(6)

Model contractual terms and standard contractual clauses

The European Commission has drawn up non-binding model contractual terms (MCTs) for data sharing agreements to assist companies in drafting appropriate provisions on, for example, reasonable remuneration and the protection of trade secrets.

In addition, non-binding standard contractual clauses (SCCs) have been developed for cloud agreements (see the next chapter). The purpose of these model clauses is to create a more balanced relationship between contracting parties and to improve legal certainty. The SCCs are intended to lead to fairer, more reasonable and non-discriminatory contractual rights and obligations.

ICTRECHT

Cloud market: Cloud services as data processing services

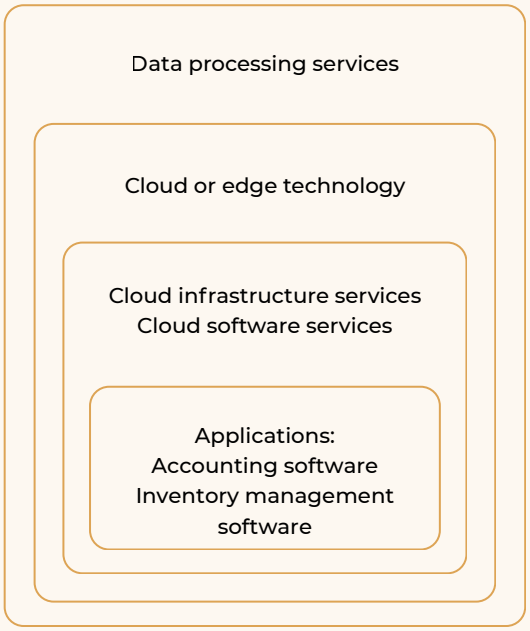
The Data Act introduces a range of measures aimed at providers of cloud services to promote competition, innovation, and the adoption of new technologies in the cloud market.

Data processing services: cloud services

The Data Act also regulates data processing services (also referred to as cloud services). The rules for cloud providers are intended to facilitate switching between providers, protect user data and interests, and enable the combination and integration of services from different providers. The ultimate objective is to stimulate competition in the cloud market and increase transparency and control for users.

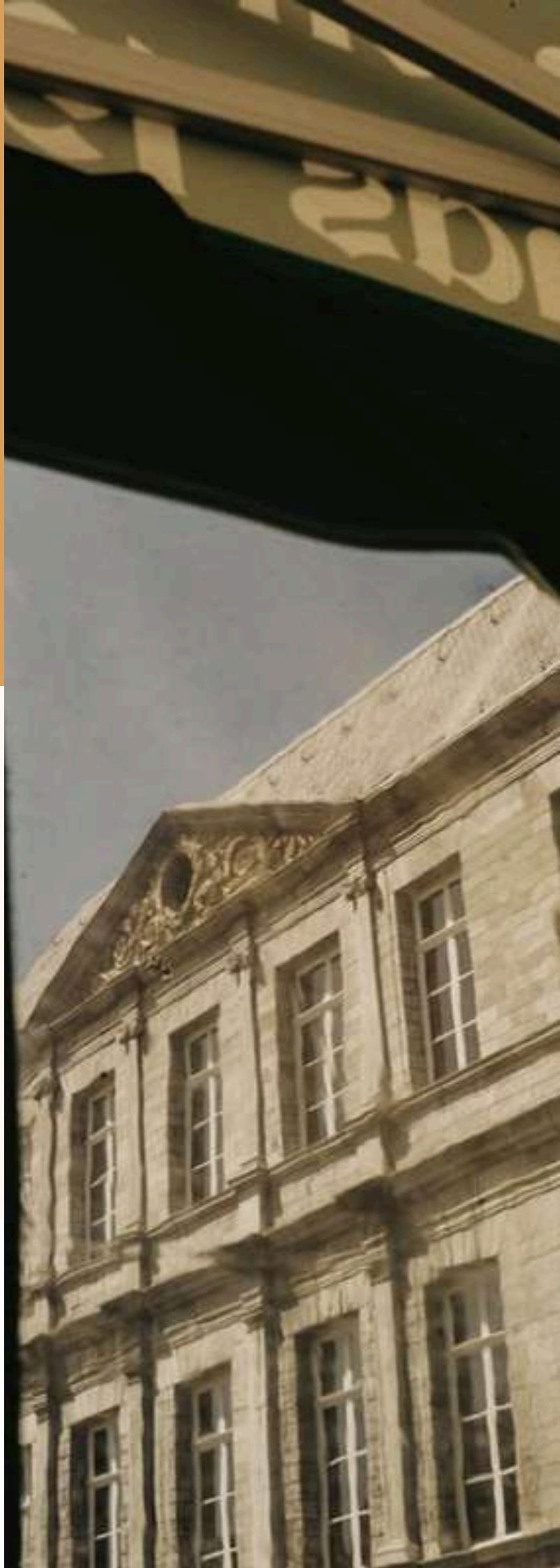
What exactly is meant by data processing services?

Data processing services cover a broad range of services offered via cloud or edge technology. This includes both cloud infrastructure services and cloud software services. The figure below provides an overview of what constitutes data processing services.



The relevant rules for cloud services are set out in:

- **Chapter VI:** facilitating switching between data processing services;
- **Chapter VIII:** development of interoperability standards for data processing services.



Rules on switching and combining cloud services

Users of cloud services often face vendor lock-in. For this reason, rules are needed to facilitate switching between data processing services and the simultaneous combination and integration of different services.

Where users wish to switch to services from other providers or to combine services from different providers, they often encounter barriers that discourage and hinder switching, combining and innovation. This section addresses the measures cloud service providers must take to make switching and combining cloud services easier.

Below is a schematic overview of the principles governing the switching process.

Switching

A process in which a customer moves data and applications from one data processing service to another:

- to a different type of data processing service; or
- a different type of service;
- to a service from a different provider.

Shared responsibility

In the switching process, the original provider of the data processing service, the customer and, where applicable, a destination provider of a data processing service are involved.

Acting in good faith

The parties involved are required to cooperate in good faith to enable the switching process.

Timely

Parties must make efforts to ensure a timely switch.

Continuity

Safeguarding the continuity of the data processing service.

Figure: Schematic overview of the process, responsibilities, and obligations involved in switching

Switching refers to the process whereby a customer moves data and digital assets from one data processing service to another, whether to a different type of data processing service, a service from another provider, or an on-premises ICT environment.

The principles governing the switching process include:

- shared responsibilities between the original provider, the customer and the destination provider;
- cooperation in good faith during the switching process;
- timely execution of the switch;
- safeguarding the continuity of the data processing service.

But what if I developed the data processing service specifically for the customer?

If a data processing service has been developed specifically for an individual user, or where most of the key components have been developed specifically for an individual user, and the data processing service is not offered on a large commercial scale, the following obligations do not apply:

- achieving functional equivalence (Article 23(d));
- the gradual removal of switching costs (Article 29);
- certain technical aspects of switching (Article 30(1) and (3)).

In these cases, the provider must inform a prospective customer that these obligations do not apply.

The rules in Chapter VI also do not apply to temporary test and evaluation versions.

ICTRECHT

Obligations of cloud service providers

Obligations on cloud service providers to enable users to switch more easily and to use services from different providers simultaneously and in an interconnected manner.

Obligations of cloud service providers

The Data Act imposes a general obligation on cloud providers to remove switching barriers. In addition, there are more specific obligations relating to contractual terms, switching charges and technical requirements.

The core principle is that users of cloud services must be able to switch easily, transfer data and applications, and decouple services. Functional equivalence must be preserved when switching. A user switching software or applications should not experience disruption, either during the switch or when using the new service.

Functional equivalence means, for example, that an equivalent function in an old and new system should produce comparable output based on the transferred input.

Users must also be able to combine and use services from different providers simultaneously, which requires interoperability.

1. Switching between data processing services

Below, we discuss the technical, legal, and organizational measures that a cloud service provider must implement and adhere to in order to make it easier for customers to switch providers.

Switching aspects	Obligation	What must the cloud provider arrange?
Barriers	Removing barriers (Article 23 (opening words)	Remove all pre-commercial, commercial, technical, contractual and organisational barriers that prevent users from switching to other providers. Remove barriers that prevent functional equivalence after switching.
	Maintaining functional equivalence *Article 23(b) and (d)*	When switching to a new data processing service of the same type, the new service must be able to operate on the basis of the transferred data and applications and, where functions overlap, produce comparable output based on the same input.
	Maintaining interoperability *Article 23*	With a view to simultaneous use, providers must remove barriers to interoperability.

Switching aspects	Obligation	What must the cloud provider arrange?
Contractual requirements	Written agreement *Article 25(1)*	Set out the rights and obligations of the customer and the provider relating to switching in a written agreement. At a minimum, the contractual requirements referred to in this factsheet must be included.
	Transition period *Article 25(2)(a)*	Allow the customer to switch at the customer's request without undue delay and within a mandatory transition period of a maximum of 30 days.
	Risks *Article 25(2)(a)*	Inform the customer in advance of any risks associated with switching.
	Support *Article 25(2)(b)*	Make arrangements for support during termination and exit.
	Termination *Article 25(2)(c))*	Make arrangements for (automatic) early termination of the agreement following a switch.
	Maximum notice period *Article 25(2)(d)*	Agree a notice period of a maximum of two months for initiating the switching process.
	Minimum period for requesting data and data specification *Article 25(2)(e), (f) and (g)*	Determine a minimum period for requesting data and specify transferable and non-transferable categories of data.
	Facilitating the switch *Article 25(2)*	Specify how the provider facilitates the switching process.
	(Business) continuity *Article 25(2)(a)*	Ensure security and (business) continuity during the switching process or simultaneous use.
	Switching costs *Article 25(2)(i)*	Make arrangements regarding relevant switching costs.

Switching aspects	Obligation	What must the cloud provider arrange?
Switching costs	Early termination costs *Article 29(4)*	Make arrangements regarding early termination costs of the contract.
	Transfer methods and formats *Article 26*	Provide information on available transfer methods and formats for switching.
	Online register of data structures and formats *Article 30(4)*	Maintain an online register of all data structures, data formats, relevant standards and interoperability specifications in which exportable data and software will be available.
	Deletion of data and digital assets *Article 25(2)(h)*	Ensure that data and digital assets are deleted after successful completion of the switching process.
	No switching costs *Article 29(1)*	From 12 January 2027, providers may no longer charge switching costs. This does not affect agreements on early termination costs.
	Gradual removal of switching costs *Article 29(2)*	Until 12 January 2027, providers may charge reduced switching costs.
	Actual costs *Article 29(3)*	Switching costs may not exceed the actual costs incurred by the provider in the relevant switching process.
	Information on cost structure *Article 29(4)*	Provide clear information on which aspects of the service the switching costs apply to, so that users can verify that no excessive charges are imposed.
Technical requirements	Functional equivalence IaaS *Article 30(1)*	Providers of cloud infrastructure services (IaaS) must take all reasonable and feasible measures necessary to enable users to achieve functional equivalence after switching to a comparable service from another provider.

Switching aspects	Obligation	What must the cloud provider arrange?
Technical requirements	Interfaces Paas en SaaS *Article 30(2)*	Providers of other data processing services, such as cloud platform services (PaaS) and cloud software applications (SaaS), must make interfaces available free of charge to users and other providers to facilitate switching and enable simultaneous use.
	Interoperability and open standards *Article 30(3)*	Providers must ensure that their services are compatible with relevant open interoperability standards for data processing services published by the European Commission.

2. Protecting user data and interests

Granting governments from third countries access to data and digital assets is incompatible with Union and national obligations to protect them. Providers must therefore take measures to protect the data and must inform customers about the protective measures that have been implemented.

Aspect	Obligation	What must the cloud provider arrange?
Applicable law	Article 28(1)(a)	Publish information on the website about the law governing the infrastructure of their data processing services.
Protection of data against government access	Article 28(1)(b) and Articles 32 and 33	Inform customers about the measures taken to prevent governments from gaining access to non-personal data stored in the European Union where such transfer would conflict with EU or national law. This concerns the protection of fundamental rights of individuals, essential national security interests, or commercially sensitive data, including trade secrets and intellectual property rights.
Measures to protect data	Article 32(1)	Take all possible technical, legal and organisational measures to prevent the transfer of non-personal data to a third-country government where this would conflict with EU law or the law of a Member State. Examples include encryption and appropriate organisational access control policies.

3. Interoperability

Many organisations use multiple types of data processing services simultaneously. However, they experience difficulties when combining and using different data processing services at the same time. Interoperability is important to ensure that data are findable, accessible and user-friendly for the recipient.

Through rules on interoperability, the Data Act aims to ensure that simultaneous use becomes increasingly possible and effective. The overview below sets out the measures that cloud providers must take to achieve interoperability.

Aspect	Obligation	What must the cloud provider arrange?
Removing interoperability barriers	Article 34(1)	Remove barriers that hinder interoperability, similar to barriers to switching, including restrictions on entering into new agreements with other providers, ensuring business continuity and data security, specifying transferable and non-transferable categories of data, offering open interfaces, and ensuring compatibility with common specifications.
Access and machine readability	Article 35	Ensure machine readability of data, data structures and data formats, and provide the technical means to access data so that automated access to and transfer of data between parties is possible.
Standardisation	Article 35(1) and (2)	Follow open specifications and harmonised standards for the interoperability of data processing services. These specifications must enable technological development, new functionalities and innovation, and must address interoperability at the infrastructure, data and application layers.

Support with interpretation and implementation

Do you need support or guidance in interpreting and implementing the Data Act? Our ICT lawyers are happy to assist. Together, we assess the Data Act and support its correct interpretation, application and implementation within your organisation. We review your contracts, organisation and services and assess them against the Data Act and related legislation.

Our practical advice addresses the legal, technical and organisational elements of the Data Act.

ICTRECHT