BarentsKrans

The Data Act
Controlling and access to product data in the EU

The Data Act contains new, uniform rights and obligations on data access and usage. Although the emphasis lies on industrial, non-personal data, the Data Act applies to all types of data processed in the EU, including personal data.

This Data Governance Update provides an overview of the main obligations and provisions from the Data Act regarding data from connected products and related services.

Data categories

Data category	Definition
Product Data	Usage, environment and performance data processed by connected products, such as "Smart devices" (e.g., smart watches and lights), medical devices; vehicle sensors, and industrial machinery.
Related Services Data	Users or event data processed by digital services that are either essential to the operation of a connected product, or are subsequently connected to add, update or adapt a connected products' functions. Examples of related services are firmware, operating systems and performance management software of industrial machinery or smart devices. Telecommunication services (such as call or chat services) do not qualify as related services.
Metadata	Data as to by whom, what, where or when product data and/or data from related services was generated or accessed.

Obligations for manufacuters and data holders

Access by design: Product data, related service data, and metadata should be accessible in a direct, easily, free of charge, securely and in a structured, commonly used, machine-readable format. This access must ideally be granted continuously and in real-time, but at the very least be granted upon request of the user.

Precontractual information: Prior to the purchase, rental or provision of connected products or related services, users must be informed about the following elements:

a) The nature, frequency, manner, purposes, type, volume of the processing and retention periods of product data and related services data;
b) The contact information of the data holder and the means for submitting data access and sharing requests;
c) The right to issue a complaint with the supervisory authority; and
d) The duration of the agreement and termination protocols.

Data sharing with user-designated third parties: Upon the user's request, data holders must share readily available data with a third party designated by the user in a convenient, free, secure manner in a structured, commonly used, machine-readable format. The received data may neither be used in a

manner that compromises the security of the connected product or related service, nor to develop a competing product by the user and/or third party. Subsequent sharing of data is not allowed without approval from the data holder.

Data requests from public sector bodies

National or EU law public sector bodies may request data holders to disclose product data, related service data or metadata under the following circumstances:

a) To respond to public emergencies e.g., natural disasters and/or major cyber security incidents); or
b) To perform a specific public interest with fair compensation for the data holder. For this purpose, only non-personal data may be requested by the public sector body.

Prohibited B2B contractual terms

Unilaterally imposed contractual terms governing access to product data or related services data in business-to-business (**B2B**) relationships may not be unfair. This principle is comparable to the requirements for FRAND (*fair, reasonable and non-discriminatory*) provisions in license agreements commonly used for standard-essential patents in patent law.

Contractual terms are unfair if they grossly deviate from good commercial practices, good faith and/or fair dealing. The Data Act contains two lists akin to the grey and black lists regarding unfair terms and conditions in business-to-consumer contracts: terms that are per se unfair, and terms that are presumably unfair.

Examples of per se unfair B2B provisions are: (i) exclusions or limitations for intentional acts or gross negligence in relation to breaches of data related obligations; (ii) exclusions of liability or available remedies in the case of non-performance of contractual data related obligations; and (iii) unilateral interpretation rights of contractual terms and/or whether conformity the data is supplied in conformance with the contract.

Examples of presumably unfair B2B provisions are: (i) inappropriate liability extensions limitations of available remedies for the counterparty in case of breaches or non-performance of data related obligations; (ii) unilateral rights to impose substantial price changes and/or materially amend the terms and conditions regarding the nature, quality, quantity or format of the data; and (iii) unreasonably short termination rights.

Enforcement

Supervisory authorities

The Dutch Data Protection Authority (**DDPA**) is responsible for monitoring and enforcing compliance with the Data Act by public sector bodies. As GDPR supervisory authority, the DDPA also enforces obligations relating to product data and/or data from related services insofar it classifies as personal data.

The Dutch Consumer and Markets Authority (**DCMA**) is the supervisory authority responsible for monitoring and enforcing compliance with the Data Act by private companies. Additionally, the DCMA is designated as data coordinator to facilitate cooperation with the DDPA and assist entities with the application and enforcement of the Data Act.

Fines

The DCMA and DDPA can impose fines for infringements of the Data Act with a maximum of **€ 1,030,000** or 10 % of the offending entity's annual global turnover, whichever is higher.

Additionally, the DDPA can impose fines in line with the margins flowing from the GDPR for infringements of data sharing provisions in the Data Act. These fines therefore go up to **€ 20,000,000** or 4 % of the offending entity entity's annual global turnover.

Important dates

The Data Act has been applicable as of 12 September 2025 with respect to connected products and related services.

The following provisions have deviating application deadlines:

- *Access by design:* Applies to connected products and related services put on the EU market after **12 September 2026**.
- *Prohibition of unfair contractual B2B-terms:* Applies as of **12 September 2027** for contracts entered into on or before 12 September 2025, which are concluded either (i) for an indefinite term; or (ii) are at least effective until 12 January 2034.

Cloud and edge computing services

In addition to obligations for sharing product data and related service data, the Data Act contains specific obligations for providers of cloud and edge computing services in case users wants to switch to different providers.

See our Digital Governance Update for Data Processing Services for more information.

What can we do?

We assist organizations in assessing their compliance, reviewing contracts (including unfair terms checks), and setting up processes in line with the Data Act. Please contact Marc Elshof for more information.

Marc Elshof
attorney-at-law | partner

T: +31 70 376 06 87
M: +31 6 46 376 108
marc.elshof@barentskrans.nl