

# Data Act – How manufacturers can avoid the disclosure of product data.

Ted Kroke

## Data Act (Which data does **not** have to be disclosed?)

Claim: A manufacturer who designs its connected product in such a way that the (raw) data generated by sensors in the product is processed within the product and only the result of such processing but not the (raw) data can be retrieved is neither required to disclose the results of such processing nor the (raw) data.

1. Recital 15 of the Data Act clarifies that the **results of the processing** do not have to be **disclosed**:  
*"By contrast, **information inferred or derived from such data, which is the outcome of additional investments into assigning values or insights from the data**, in particular by means of proprietary, complex algorithms, including those that are a part of proprietary software, **should not be considered to fall within the scope of this Regulation** and consequently should not be subject to the obligation of a data holder to make it available to a user or a data recipient....."*
2. The following pages explain why the **(raw) data processed for generating such results does not have to be disclosed** if the manufacturer designs the connected product in such a way that this raw data is not accessible to them either.

## Background: When to avoid data disclosure

**Previous approach:** Manufacturers designed products to make as much data as possible retrievable.

**Problem:** The Data Act requires manufacturers to extensively share data generated by connected products that can be retrieved.

**New approach:** All currently retrievable data should be classified by (a) whether the manufacturer needs it and (b) whether there is a confidentiality interest:

|            | Confidentiality Interest                                                                                                                | No Confidentiality Interest             |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Needed     | Manufacturer should consider how to protect confidentiality despite the Data Act's limited safeguards ( <b>see this presentation</b> ). | No action required by the manufacturer. |
| Not Needed | Manufacturer should redesign the product so this data can no longer be retrieved (including during maintenance).                        | No action required by the manufacturer. |

## Data Act (What data must be disclosed?)

### So-called "product data" must be disclosed

see Art. 3 (1) Data Act: *"Connected products shall be designed ... so that product data ... are directly accessible to the user ..."*).

#### ➔ What is product data?

Art. 2 (15) DA: *"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."*

#### ➔ Three CRITERIA:

1. *"Data generated by the use of a connected product ..."*
2. that is *"... retrievable, via an electronic communications service, physical connection or on-device access ..."*
3. that the *"... manufacturer designed to be retrievable ...."*

# Data Act (What data must be disclosed?)

## Criterion 1: "data generated by the use of a connected product"

**Key point: The obligation to disclose data covers**

- **merely the data generated by user actions,**
- **and not all data available in the connected product in question.**

**However, the understanding of what qualifies as "data generated by user actions" is rather broad as further clarified in Recital 15 of the Data Act. This includes:**

- *"data recorded intentionally or data which result indirectly from the user's action, such as data about the connected product's environment or interactions"*
- *".... data generated automatically by sensors and data recorded by embedded applications, including applications indicating hardware status and malfunctions"*
- *"data generated by the connected product .... during times of inaction by the user, such as when the user chooses not to use a connected product for a given period of time and instead to keep it in stand-by mode or even switched off."*

## Data Act (What data must be disclosed?)

Criterion 2: *"retrievable, via an electronic communications service, physical connection or on-device access ..."*

**Key statement:** Basically, any means of retrieval is sufficient.

- *"electronic communication service, a physical connection or on-device access"* refers to any interface, even if it is only USB access or an OPC UA interface.

**PLEASE NOTE:** The fact that USB access is sufficient is often overlooked, as *"device-internal access"* was only added during the legislative process.

- *"retrievable"* means that it is not necessary for the data to actually be retrieved; e.g., a retrieval option is sufficient in the event of maintenance, even if no maintenance contract has been concluded.

## Data Act (Which data does **not** have to be disclosed?)

Criterion 2: *"retrievable, via an electronic communications service, physical connection or on-device access ..."*

**Key reversal:** Data that cannot be retrieved does not have to be disclosed.

- ➔ If you only process the digitized user actions (i.e. the raw data) generated within the product but do not make them retrievable, you do not have to make them available to the user.

Criterion 3: that the *"... manufacturer designed to be retrievable ...."*

This clarification is important, as it means that a third party cannot subsequently coerce the manufacturer into disclosing machine-generated data by setting up a mean to retrieve that data.

However, if the manufacturer himself sets up such a mean at a later point in time, the relevant data will qualify as "product data" and must be disclosed to users.

## Data Act (Which data does **not** have to be disclosed?)

### Interim conclusion:

- If you are the manufacturer of a product that generates data during use and want to "escape" the Data Act, you must design the product so that this data is not retrievable.
- If the manufacturer still needs this data for product analysis, the processing of such data must take place within the product and only the result of the processing may be retrievable.
- This result of the processing does not fall within the scope of the Data Act.

### Wait, it's not that easy! Remember Recital 15 Data Act:

*"By contrast, information inferred or derived from such data, which is **the outcome of additional investments** into assigning values or insights from the data, in particular by means of **proprietary, complex algorithms, including those that are a part of proprietary software**, should not be considered to fall within the scope of this Regulation and consequently should not be subject to the obligation of a data holder to make it available to a user or a data recipient...."*

- .

## Data Act (Which data does **not** have to be disclosed?)

At what point does the processing of data within the product mean that the result of such processing is no longer subject to the Data Act?

**Key conclusion from Recital 15 Data Act: Not every analysis or processing is sufficient;** in the absence of case law, there is a risk that the chosen form of processing will be deemed insufficient by a court.

The EU Commission has also addressed this in questions 5 and 13 of its FAQs on the Data Act (<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>), although this does not provide for an answer (as it is rather explained which metadata must be disclosed together with the product data), one use case is identified as insufficient: *".... processing that is designed to preserve the privacy of the information such as anonymisation or pseudonymisation or processes of encryption should not be considered sufficient for the data to be excluded from scope of Chapter II..."*