CEMA
European Agricultural Machinery Association

CEMA Q&A on the Data Act

Version 1.1 – April 2025



Table of contents

Goals of the document **3**

Other sources of information **3**

1. General **4**

2. Data and Scope **6**

3. Data sharing **12**

4. Internal data usage **16**

5. IP protection **18**

6. Suppliers **21**

7. Dealers **22**

8. Farming **23**

9. Authorities **24**

Disclaimer: This set of technical Frequently Asked Questions {FAQs), on the Data Act, is designed to assist CEMA company members in the implementation of the legal provisions. The FAQs are the product of extensive stakeholder interactions, and this is intended to be a 'living document' that will be updated as and when necessary. The version history can be found at the top of the document. The replies to the FAQs do not replace the applicable legislation nor introduce any additional requirement. The expressed views are not authoritative and serve as assistance tools only.

Goals of the document

- Provide a useful tool for implementation managers and engineers.
- Not duplicating the work done by other organisation or the European Commission, but instead creating an added value focussing on the use cases relevant for the agricultural machinery industry.
- The tool contains answers that have been assessed and agreed upon by experts for all questions gathered within the industry related to agricultural machinery and vehicles. This will support manufacturers in the final stage (of implementation): checklists, implementation blueprint and roadmap.

Other sources of information

- Data Act regulation: *http://data.europa.eu/eli/reg/2023/2854/oj*
- Data Act explained | Shaping Europe's digital future
- European Commission Data Act FAQs: Commission publishes Frequently Asked Questions about the Data Act | Shaping Europe's digital future
- Orgalim guide on Data Act (under development)

1. General

1.1 - What are the boundaries for the connected product and the service according to the Data Act? (Vehicle, sensor, modem, telecom, app, software, data sharing platform?)

The Data Act applies to all data generated by a connected product. In general, as soon as usage data is recorded in the vehicle (for later retrieval), or usage data is stored outside the connected vehicle, it is considered to be in scope of the Data Act, and it needs to be made available to the user (or third party upon request by the user). This is detailed in Recital (14) and Article 2 with the definitions (5) and (6) of "connected product" and "related service".

The complete data flow typically involves the machine, app(s), and a data platform. Data cannot be collected and communicated without sensors, components, and in most cases modem and telecommunication, but these devices are not subject to direct requirements in the Data Act.

See also EC Data Act FAQ (v. 1.2) Q 7.

1.2 - Who are the user, the data holder, and the third party?

Definition of "user"

- Article 2 (12): *a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services;*
- **Interpretation**: a user is any person who **owns or uses** a machine. Users can therefore be owners, employees, co-owners or renters, for example.

See also EC Data Act FAQ (v. 1.2) Q 14

"Data holder"

- Article 2 (13): *a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;*
- **Interpretation**: The definition can only be understood to mean that the data holder is the person **who has actual control over the data and is in a position to grant the access** under the Data Act. This may be the manufacturer, a supplier on behalf of the manufacturer, or an after-market supplier or service provider.

See also EC Data Act FAQ (v. 1.2) Q 21.

'Data recipient'

- Article 2 (14): *a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party*

following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law.

- **Interpretation**: This is anybody that **receives the data** generated by the user. This may include a software company, app provider, agronomist, food supply chain participant, agricultural cooperative, competitive telematics provider, university or a governmental body.

1.3 - The implementation time is 20 or 32 months. What applies when?

The Data Act is in force since **12 January 2024**.
There are different implementation deadlines to give more time for manufacturers to ensure 'access by design'.

Implementation period 20 months: until **September 2025** to comply with the following essential provisions:

- Provision and transfer of data to users, third parties, public authorities
- Facilitation of interoperability between data processing services (not applicable to machinery manufacturers)
- Contractual agreement on the use of non-personal user data
- Safeguards for non-personal data in the international environment
- Transparency: pre-contractual information obligations ("package information")
- Contract design: no abusive clauses for data sharing (applies to contracts concluded after 12/09/25).

Implementation period 32 months: until **September 2026** to comply with requirements from Article 3 (1), with the obligation to make data generated by the use of products or related services accessible through "**access by design**", i.e.:

- networked products and connected services must be manufactured or provided in such a way that users can access their data easily, securely and free of charge
- if the machine is not "connected" (i.e. no access to generated data, directly to on-device data storage or remote server), it is not considered in scope (Article 2(5))
- **it applies to products that are placed on the market after 12 September 2026**.

Implementation period 44 months: until **September 2027** to address unfair terms in existing contracts concluded before 12 September 2025. (Article 50)

1.4 - What to do with historical data stored in our platform, from e.g. the past 10 years. Does the Data Act only apply to data collected after 12 September 2025, or on vehicles sold after 12 September 2025?

No, the Data Act does not apply to data collected before the application of the regulation. However, existing contracts will define what needs to be done.

- **Relevant text: Article 4 (1):** the right of users to access and use data generated by the use of products or related services.
- **Interpretation:** the right of access therefore only covers data generated from this point in time (ex nunc).

- **Argument in favour of this interpretation:** The data controller can only provide data if he is aware of the data sharing obligations; otherwise, he will handle the generated data or anonymise it in accordance with the applicable data protection laws. If the data controller was obliged to disclose (historical) data that has already been collected, it would have to be labelled to make it traceable to the user later. This cannot have been the intention of the EU legislator for two reasons: (1) the Data Act itself refers to data minimisation in several places. (2) The associated extension of the right of access to companies (currently the data subjects are entitled to this under Article 15 GDPR, i.e. natural persons).

See also EC Data Act FAQ (v. 1.2) Q 32.

1.5 – What are the penalties for non-compliance?

Article 40(4): *For infringements of the obligations laid down in Chapter II, III and V of this Regulation, the supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679 may within their scope of competence impose administrative fines in accordance with Article 83 of Regulation (EU) 2016/679 and up to the amount referred to in Article 83(5) of that Regulation.*

Regulation (EU) 2016/679 Article 83.: **20 000 000 EUR or 4 % of turn-over**.

1.6 - Does the Data Act have an impact on the conformity of the vehicle?

No, the Data Act does not have specific provisions on conformity assessment. There is no direct effect of the Data Act on the conformity of the vehicle and related procedures.

However, Data Act obligations apply to all connected products, including those that are subject to specific type approval or conformity assessment regimes.

Art. 40 of the Data Act only talks about penalties **to stop an infringement of the Data Act**. Administrative fines are mentioned in Art 40 (4) and (5).

The manufacturer should assess the impact that the Data Act has on compliance with other applicable product legislation. Any lack of conformity should be remediated.

2. Data and Scope

2.1 - Do connected machines without a display need cloud access?

The presence of a display is irrelevant in determining the applicability of the Data Act, as it serves only to visualise data, not to make it available for further use. In other words, regardless of whether

a display is present, if product data is stored on the OEM cloud, there is an obligation to provide access to that data.
Considering that the definition of a connected product (Article 2(5)) applies to the machine in question, any data generated using the machine must be made readily available, either from on-device data storage or from remote storage in the cloud. In line with Article 3 (1) this data must be provided to the user.

See also EC Data Act FAQ (v1.2) Q17 and Q22.

2.2 - What if there is no connectivity (no communication to the OEM cloud), but the vehicle stores the data it generates, and that data can be retrieved by a dealer using a diagnostics tool?

Interpretation: According to the definition of connected products (Article 2(5)), the machine's primary function is not the storage of data. In this case, the manufacturer is not in control of the data and, therefore, has no obligation to share the data as he is not the data holder. The data is not considered "readily available data" for the OEM as defined in Article 2(17).

However, all raw data that is generated during the use of the equipment is in scope of the EU Data Act. If this raw data is downloaded in the course of repair or service diagnostics by the servicing dealer, independent repairer or OEM, it remains within scope. This also applies if any raw or pre-processed data is used beyond pure service and repair diagnostics, for example for product optimization or product development.

2.3 - If a product is only connected once every year (when it is in the workshop), is it a connected product?

Yes. Data is generated through the use of the machine (and it concerns the use of the machine), it is stored and communicated by the device (Recital (15)). If the data is subsequently stored in a cloud, it also falls within the scope of data-sharing requirements.

2.4 - If the data is not recorded in the cloud, and not available to the manufacturer, does it bring any obligations to us OEMs?

No, if the OEMs do not have the data, they are not considered data holders for that data.

Implicitly included in **EC Data Act FAQ (v. 1.2) Q 31.**

2.5 - What about machines that are connected only through after-market telematics kits?

We consider that the OEM does not obtain the data.

The OEM is not the data holder and has no data sharing obligations. The provider of the telematics kits is the data holder and must comply with the legal requirements set out in the Data Act.

If the user decides to share the data with the OEM, then the OEM is treated as a third party and can get the data on behalf of the customer. This requires a contractual agreement. Compensation is an option for the data holder, but not an obligation for the recipient.

If the provider of the telematics kit only supplies the hardware and the OEM is the owner of the software, then the OEM is considered the data holder.

See also EC Data Act FAQ (v. 1.2) Q21.

2.6 - Does flight recorder data (black box on the machine collecting aggregated usage data) recorded in the machine need to be shared?

The same rules as for all other discussed data applies. Following the principle of Recital (15), recorded/stored data, intended for later retrieval, is considered to be within scope. Even if it is recorded on a black box in addition, the transmitted data will be provided anyway. Data resulting from complex algorithms is not to be provided. (Recital (15))

Black boxes are mostly ring-storage systems, meaning they will regularly overwrite stored data. In such cases, sharing the data may not always be practically possible.

Interpretation: In case of legal cases (e.g. accidents, cybersecurity incidents), there could be restrictions of access, to preserve the integrity of evidence.

2.7 - Are software interventions and logs in scope of the Data Act?

Interpretation: Logs of software interventions are not generated by the use of the vehicle (connected product) by the user and are therefore considered to be out of scope.

2.8 - Do machinery manufacturers need to give customers access to CAN-bus data?

The regulation requires to give access to product data (art. 3.1) which is designed to be retrievable (Article 2(15)) and readily available (Article 2(17)). Recital (20) explains that this excludes operational data running and contained within the machine.

Interpretation: The CAN-bus is the digital artery of the machine. OEMs are not obliged to provide access to the CAN-bus, nor to the CAN-bus data, unless this data is stored in the machine or in the cloud for later retrieval through a connection.

2.9 - Can the customer ask access to the diagnostics downloads created by the dealer?

Yes, see Question 2.2

Most, if not all, of the processing and intelligence is embedded usually in the diagnostic tool itself, which is plugged to the machine. The additional investments in building smart algorithms or assigning additional values to the data should occur within the tool, and not on the machine. The depth of processing depends on the tool itself. Instead, when the tool reads and records CAN messages that are raw or pre-processed, those downloads are in scope of the EU Data Act.

Repair and maintenance itself is not considered a "related service" and the data this generates is considered out of scope.

See also EC Data Act FAQ (v. 1.2) Q10.

2.10 - If the captured data is deleted upon arrival (e.g. security data), is the OEM still required to share it with the customer?

No. If you do not have the data, you are not the data holder, so you cannot be obliged to share it.

2.11 - Are error messages out of scope of data sharing?

Interpretation:
In most cases error messages are the result of using proprietary, **complex** algorithms, based on the OEM's know-how. Based on this principle they are out of scope of this Regulation for mandatory sharing, unless otherwise agreed between the user and the data holder. For example, a misfiring of engines depends on engine calibration and is complex to identify.

However, **simple** error messages must be made available. In most cases the driver will see these items in the cab anyway. For example, an engine overheating alert is a simple calculation (pre-processing), it is the result of the usage of the vehicle, and would be within the scope of the data sharing obligations.

2.12 - When is data "pre-processed" (subject to the sharing obligation) and when is it the output of an algorithm (not subject to sharing)? Is a histogram of events considered as an algorithm? When do you consider that it is a simple transformation (pre-processing)? Is an encryption a complex algorithm and processed data?

As explained in Recital (15), **raw data, pre-processed data and metadata** are **in the scope** of this regulation:

- *Recital (15): Data which are **not substantially modified**, meaning data in **raw form**, also known as **source** or primary data which refer to data points that are automatically generated without any further form of processing, as well as data which have been **pre-processed** for the purpose of making them **understandable and useable prior to subsequent processing and analysis** fall within the scope of this Regulation. Such data includes data collected from a single sensor or a connected group of sensors for the **purpose of making the collected data comprehensible** for wider use-cases by determining a physical quantity or quality or the change in a physical quantity [...]. The term 'pre-processed data' should not be interpreted in such a manner as to impose an obligation on the data holder to make substantial investments in cleaning and transforming the data. The data to be made available should include the relevant **metadata**, including its basic context and timestamp, **to make the data usable**, combined with other data, such as data sorted and classified with other data points relating to them, or re-formatted into a **commonly used format**. Such data are potentially valuable to the user and support innovation and the development of digital and other services to protect the environment, health and the circular economy, including through facilitating the maintenance and repair of the connected products in question.*

In the context of pre-processed data, no extra investments are demanded from the data-holder.

On the other hand, data referred as **complex algorithms** are **not in scope** of this regulation:

- *As explained in Recital (15) (following the above quote): 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, unless otherwise agreed between the user and the data holder. Such data could include, in particular, information derived by means of sensor fusion, which infers or derives data from multiple sensors, collected in the connected product, using proprietary, complex algorithms and which could be subject to the **intellectual property rights**.*
- *Only provide complex data if otherwise agreed between user and data holder (see Recital (6)).*

Interpretation: There is no need to provide histograms (insights of the data – investment to create value based on the raw / pre-processed data), but raw / pre-processed data must be provided, so that third parties can create the histogram on their own.

See also EC Data Act FAQ (v. 1.2) Questions 4, 5 and 6.

2.13 - What is "related service data", and how does it differ (or not) from "related service"?

According to Article 2(6), a **Related service** is:

- *A digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is connected to the product to add to, update or adapt the functions of the connected product.*
- *Anything that would make a connected product behave in a specific manner (European commission, Data Act explained | Shaping Europe's digital future (europa.eu)).*
- Examples are an app to adjust the brightness of lights, or applications that complement the haptic product.
- It requires bi-directional communication with the device.

According to Article 2(16), a **Related service data** is:

- *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.*
- **Interpretation:** Related service data is data that is intentionally or unintentionally generated by the user when using the related services.

Examples of related services in agricultural machinery:

- An app to verify and set settings off a planter implement.
- An app to process drone images and load them into the sprayer for selective spraying.

The following are not considered related services (EC FAQ 10): connectivity, power supply, and aftermarket services (auxiliary consulting, analytics and financial services, and regular repair and maintenance)

See also EC Data Act FAQ (v. 1.2) Q 10.

2.14 - How long should the OEM keep the data of the user?

OEMs should always respect the rights of individuals and implement data minimisation strategies (Recital (8)). If the customer's subscription is still active, we must keep the data. If there is no active subscription, the data holder may in theory keep the data in the cloud for an unlimited time-period (non-personal data), but a contractual agreement on data retention is advised. (Recital 24 "reasonable retention policy")

See also EC Data Act FAQ (v. 1.2) Q33 on the lack of "right to be forgotten".

2.15 - Does the Data Act impose requirements for audit logs?

- The Data Act has no specific requirements for audit logs. Logs must be considered like all other data and, if they exist, data logs should be minimised (Article 4(5)).
- If the audit logs are stored, the user should have to possibility to access them (as required under GDPR).

2.16 - Does the OEM need to provide data to allow the customer to chip-tune or customise features of the vehicle?

Data Act Recital (15): *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, is not considered to fall within the scope of this Regulation and consequently is not subject to the obligation of a data holder to make it available to a user or a data recipient, unless otherwise agreed between the user and the data holder.*

Engine mapping tables represent a significant (if not the main) investment from manufactures and engine suppliers, and as such could be considered out of scope of the sharing obligation.

If a data holder restricts or refuses to share data based on safety or security concerns, they must notify the competent authority, which could lead to non-compliance of the product. Modifying a vehicle holds a serious safety and security compliance risk.

Interpretation on recital 16: "improving the performance of the connected product" happens through the "aftermarket, ancillary and other services based on data", not through modification of the product itself.

See also EC Data Act FAQ (v. 1.2) Q25.

3. Data sharing

3.1 - Do we need a data sharing platform with APIs for third parties to connect? Does it need to be OEM specific (internally developed) or can we rely on data spaces, DKE Agrirouter or DataConnect?

There are no obligations regarding the technical method used to share data. We do have obligations in terms of (Article 5(1)):

- Data quality;
- Readable/usable in an easy and automatic mode;
- In a commonly used format;
- Real time (if applicable).

An OEM specific API can be used, as well as existing telematics solutions, Agrirouter, DataConnect or a standardized "method" defined by agricultural machinery manufacturers.

Is it sufficient if customers can see the data in real-time and download the data? Is an API absolutely necessary?
Article 5.1 states that data must be provided "of the **same quality** as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where **relevant** and technically feasible, continuously and in real-time"

Interpretation: The quality of the data needs to be retained (i.e. the resolution, including timing), but when it comes to timing, the data to be delivered needs to be in real-time only if relevant. This depends on the use case: for example, uploading the data in the farm management system happens only once for all data, before analysing and planning the next year farming activities.

EC Data ACt FAQ (v1.2) Q 5 suggest that if data quality improvements happen before the data is made available to the OEM internally, the improvement is also applied to the data shared externally.

3.2 - Do we need to provide data sharing for third parties, even if the customer has direct access to the data through the machine?

Sharing data with customers is not necessary if the customer has direct access (Article 3(1)). However, Article 5 on sharing data with third parties continues to apply if the OEM is the data holder (i.e., has control over the data).

Interpretation: Customers cannot set up a data sharing system to third party services without getting data from a cloud platform.

See also EC Data Act FAQ (v. 1.2) Q31.

3.3 - We as manufacturers do not know who the rental user is. How can we arrange data access?

The contract between the manufacturer and the rental company needs to clarify who assumes the role of data holder for rental users. (Data Act Article 3(3), point (d))

For machinery manufacturers (selling directly or via the dealer network), the customer is the owner of the product (rental service provider), with a contractual relationship between manufacturer and customer. In any case, manufacturers are obligated to share data with the rental service provider.

At any time, the owner of the vehicle (rental service provider) can access all the collected user data, and consequently should adhere to all applicable regulations (Article 3(2) Data Act, GDPR, etc.).

The rental service provider has a contractual relationship with the rental user and must provide guidance to its customer (Article 3(2), point (d)).

From a technical point of view, these are the options to consider (Recital (21)):

- The rental company provides the data to the rental user through its system. A potential simpler solution is to share the collected data during the rental period via email using simple file formats like for example xml.
- The manufacturer can take care of the data sharing, creating temporary users for the rental period upon request from the rental service provider. A management solution for the rental company in the OEM cloud may facilitate setting up the data flow for the rental user. In any case Recital (21) requires OEMs to allow separate user accounts for individual persons.
- The user can set up his own data-sharing flows, from within the machine through the HMI, or using QR codes through the web.

See also EC Dat Act FAQ (v. 1.2) Questions 16 and 30.

3.4 - What if there are multiple data holders (DH)?

According to Recital 21, the user should turn to each party with which he has a contract. The contracts should specify the relevant data holders and trade secret holders, and the data they control.

See EC Data Act FAQ (v. 1.2) Q 21.

3.5 - Can an OEM charge money for telematics data? How much can be charged?

For users, data access should be free of charge (Article 3(1)).

- If the OEM collects data from the machines through an active telematics subscription, then it must share the readily available data free of charge, regardless of whether the customer/OEM pays for the telematics subscription or not, and regardless of whether the customer has access to the telematics application or not.
- If the telematics is not active, the OEM may sell the telematics service. But note that the OEM will not have the telematics data without an active telematics subscription.

- The free access concerns only the data. The front-end application should not be free of charge.
- The OEM may recuperate some costs if the customer prefers to use a front-end application from another supplier (see B2B below).

For B2B (third parties), a remuneration (Article 9) is possible.

- For SMEs and non-profit: the OEM may charge for the costs of making data available + reasonable margin.
- Other: same as above + charge for additional costs for investment in data collection, volume, etc. + reasonable margin.
- The OEM needs to provide details about the calculation.

In the agricultural business, the telecommunications service, the telematics software, and the data access are sold together as a subscription package. Can we still charge for the telecommunications service and the software?
Yes, but once data is captured through the telecommunications service and the software, data access must be provided free of charge.

See EC Data Act FAQ (v. 1.2) Q 39.

3.6 - What if a competitor refuses to pay for the data, but the customer expects it to be visible on MyCompetitor.com?

The regulation ***does*** require the data holders to share the data with the customer/user and a third party on behalf of the user. The regulation ***does not*** require the third party (competitor) to accept the customer's data transfer request. So, if the third party is not interested, there will be no contract with the data holder for data transfer and the data will not be visible on Mycompetitor.com.

Note: there are obligations for third parties ***if they*** *do* use the data, and reasonable fees may be charged for data transfers.

3.7 - Can a customer escape the cost for data sharing if he shares the data directly with the third party (bypassing the OEM)?

Unless there are data restrictions (because of security or trade secrets), then nothing prevents the user to do so. To note:

- Non-trade secret related data will in any case be available to the farmer.
- Article 3(3), point (h) states that the service contract must describe the trade secrets.
- Article 11(1) states that technical protection measures shall not hinder the right of the user to share data with a third party.

Users are even allowed to monetise their data.

See EC Data Act FAQ (v. 1.2) Q 19.

3.8 - Are OEMs still responsible/liable for the data shared with somebody else (under GDPR)? Are there requirements on the side of the third party they need to demand?

OEMs need to maintain safety, security, and protection of trade secrets. This requires specific statements in the contract. The model contracts from the Commission should provide good examples on how to handle this. GDPR and Data Act requirements both require a legal basis for transfer, i.e. consent. If there is a legal base for data transfer, the consent is embedded, and no additional consent would be required.

EC Data Act FAQ (v. 1.2) Q 1-3

3.9 - What if the customer neglects all documents, agreements, etc. Who is liable? Do machinery manufacturers still need to fulfil their obligations?

If the customer refuses to sign the data usage agreement, OEMs have no obligations. The contract must be available before the service is started (Article 3(3)).

As a data holder, OEMs must have a legal basis to transfer data to a third party in accordance with the Data Act. If the customer (user) refuses to provide the relevant documents, it is not possible to act in a legally secure manner and OEMs cannot fulfil their obligations as a data holder.

If the customer does not fulfil his obligations, OEMs have a reason to cancel the contract and stop the data transfer. This is a normal clause that needs to be added to the contract. Contracts may include clauses on liability as well.

3.10 - One of my customers asks to share data with a US-based software company. Am I legally obliged to do so, or only with EU-based software companies? (Where can I find support for this in the regulation?) What counts to define if it is an EU-based company? The legal entity or the location of the data storage?

- Article 1(3), point (d) states the regulation only applies for data recipients (including third parties on request of the user) in the EU. Third parties outside of the EU are not in scope of the regulation if the user of the connected product is from outside of the EU.
- The user from inside the EU can request data from suppliers outside of the EU to be shared with third parties inside the EU (product placed on the EU market).
- Users may ask Data Holders to share data with a recipient outside of the EU, but the Data Holder is not obliged to provide it. If data recipients in third countries offer a service to the user in the EU, then they have obligations. In any case they have no rights to claim data access.
- Users from inside the EU have rights and obligations under the Data Act (Article 1(3), point. (b)), third parties from inside the EU that would receive data fall under the Data Act (Article 1(3), point (d)),
- Sharing data outside the EU requires adequate measures to prevent governmental access. (Article 32(1))

Interpretation: Learning from the discussion around the DSA (Data Services Act), we interpret Art 1(3) as (a) OR (b) OR (c) OR (d). Regardless of where the data originates, if the user/recipient is in

the EU, then the Data Act applies. So European data recipients (app providers) need to adhere to the European Data Act rules, also if they receive data from outside of the EU (e.g. Brazil or US).

See EC Data Act FAQ (v. 1.2) Q 37.

3.11 - Can OEMs be obliged to share the DTC (error) codes in relation to product safety and market surveillance requirements?

- The diagnostics error code (DTC) could indicate a safety risk.
- OEMs may disclose information about unknown product safety risks after the product is placed on the market through the Safety Gate, the EU rapid alert system for dangerous non-food products. However, the Safety Gate only requires a high-level description of the issue, not the technical details (no DTC codes).
- For TMR products, non-compliance safety items must be reported to the type approval or market surveillance authority. This information sharing is not public, but may require technical details like DTC codes if relevant.

4. Internal data usage

4.1 - Can the OEM use the data from its own machines?

Yes, if a contract with the customer has been established before the usage of the data (Article 3(3), point (c)). The internal data usage needs to be detailed in the sales contract. OEMs, as such, can always use the data from their products.

In terms of personal data, the GDPR must also be applied. If the data originates from a supplier's component, additional agreements may also be worked out with the supplier (e.g., it may contain trade secrets).

See also EC Data Act FAQ (v. 1.2) Q 29.

4.2 - Can an OEM use the data from competitive machines as well?

Yes, with consent of the customer, but not to develop competing connected products (Recital (32)).

4.3 - Are OEMs allowed to use competitive data for reverse engineering?

Recital (32) states that reverse engineering is allowed, provided it complies with regulations like competition law. However, data must not be used to develop competing products. It is explicitly prohibited. (Recital (32)).

4.4 - How to prove that competitive data is used to train AI algorithms?

This question is not relevant, as according to the Data Act competitive data can be used for the development of new services and products. So, the real question should be "How to prove that competitive data is used to develop a competing product?".

Only the development of a competing connected product is prohibited (Recital (32)). For example, one could develop a predictive maintenance app for a competing product, even if the competing manufacturer has a similar service.

4.5 - Can we use API usage data for marketing purposes?

In general, the usage of personal data for marketing or commercial purposes, is regulated by the GDPR and not the Data Act.

For non-personal data Recital (26) provides more info: *Users should therefore have the right to share non-personal data with data recipients for commercial and non-commercial purposes. Such data sharing could be performed directly by the user, upon the request of the user via a data holder, or through data intermediation services* And *Data holders should not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user.*

Based on the Data Act, it is possible to use data received as a third party for marketing or commercial purposes, as agreed by the contract.

As a data holder, permission must also be given by the user (Article 5(6)) and trade secrets shall be handled as such (Article 5(9)).

As a third party, you shall neither use the data for profiling of the user (Article 6(2), point (b)), nor use the data to derive economic insights from the data holder [Art. 6.2 (e)]. You must also respect trade secrets of the trade secret holder (Article 6(2), point (g)). This especially applies when OEMs get data from competitive platforms.

4.6 - Do we need additional consent for GDPR, or is the Data Act contract sufficient?

Yes, if personal data is involved, you need a legal base. User consent is one of the options, but there are other legal bases (see GDPR 2016/679).

See also EC Data Act FAQ (v. 1.2) Q 2 and 20.

4.7 - Can we use data collected before the Data Act (for example collected according to CoC (Code of Conduct for agricultural data sharing under contractual agreement))? Does the Data Act apply as well on historical data?

You are bound to the existing contract with the customer, also if it is based on the CoC. If there is no contractual clause preventing the use of data (according to the CoC) you can use the historical data.

See also EC Data Act (v. 1.2) Q 32.

4.8 - If we as an OEM buy a machine from a competitor, can we, as a customer, ask for data exchange into our platform?

Yes, we, as the owner of the machine, are entitled to get the data and share it with a third party. But we are prohibited to use the data to develop competing connected machines (Recital (32)).

4.9 - Can customers refuse to let us use their data (e.g. for engineering and support services) while still being able to get the data of the machine (because the contract needs to be there before the start of the service)? Is this fair/unilaterally imposed?

No, the contract needs to be available before the start of the service, which will include the terms on how the data holder will use that data. It would be unfair if one party unilaterally prevented the usage of the data provided or generated (Article 13(5), point (c)) while still demanding access to it.

See also EC Data Act FAQ (v. 1.2) Q 29.

4.10 - If a manufacturer has different legal entities, do they need "internal" contracts for sharing data between those legal entities?

Before concluding a contract with the customer, the manufacturer needs to detail all third parties that have access to the data for the reasons agreed with the customer. (Article 3(3))
The other legal entities are third parties working on behalf of the manufacturer for the reasons agreed with the customer.

Interpretation: Listing all the legal entities having access to the data in the contract is sufficient. This is different than GDPR.

5. IP protection

5.1 - Can machinery manufacturers restrict access to the telematics data?

In general, all data may have to be shared, except safety relevant data (Article 4(2)). Trade secret relevant data may be protected (a secret should remain a secret after all) (Article 4(6)). If data is refused to be shared, a competent authority must be informed (Article 4(2), 4(7), 4(8)). In B2B relations, users may agree to limit further sharing of data (Recital (25)).

OEMs should follow this process:

- Adhere to data minimization principles. (Recital (8))

- Classification of the data: security/functional safety relevant data (to be done anyway for cybersecurity), trade secrets or patents, raw or pre-processed data, processed data
- Decide where to process the data. If the data is processed on the machine and is the result of a complex algorithm, then the data does not have to be shared.
- Use legal protection: patents.
- Use technical protection measures (Article 5(9))
- Apply voluntary contractual restrictions (Recital (25))
- Only share data required for the service of the third party. (Recital (26))

Note: OEMs may carefully select what data is made available on the machine and what is available on the cloud in order to protect sensitive data.

See EC Data Act FAQ (v. 1.2) Q 22.

5.2 - How do we legally protect our IP-sensitive data?

The following measures are available:

- Patents
- Trademarks
- Copyrights
- Trade Secrets: with the Data Act the protection will be limited as it is difficult to demonstrate/provide evidence that it concerns a trade secret, and under specific conditions it needs to be shared in any case.

Arguments from the regulation:

- **Article 4(6)** -> The rights and obligations of users [...] with regard to access, use and making available product data [...]
  *prior adoption of "necessary" secret protection measures (Model contractual clauses, confidentiality agreements, strict access protocols, technical standards and codes of conduct, TOMs) before giving **user** access to the data*
  ...deny access under certain conditions
- **Article 5(9)** -> Right of the user to share data with third parties
  *Limiting data access to strictly necessary contractual purposes to fulfil the contract between user and third party prior adoption of "necessary" secret protection measures (Model contractual clauses, confidentiality agreements, strict access protocols, technical standards and codes of conduct, TOMs) before giving **third party** access to the data.*
- **Article 30(6)**
  Providers of data processing services shall not be required to develop new technologies or services, or disclose or transfer digital assets that are protected by intellectual property rights or that constitute a trade secret, to a customer or to a different provider of data processing services or compromise the customer's or provider's security and integrity of service.
- **GDPR Article 15(4), GDPR Article 20(4)**
  Rights and freedom of other people are not impaired.

See EC Data Act FAQ (v. 1.2) Q 23 and 24.

5.3 - What data can be considered trade secrets? What are examples of trade secrets? Do we have to define the trade secrets in advance? Do we have a framework for the justification?

Trade secret is information

- which is neither generally known nor readily accessible nor in the precise arrangement and composition of its components, to persons in the circles who normally deal with this type of information and is therefore **of economic value** and
- which is subject to appropriate **confidentiality measures in the circumstances** by its legitimate owner and
- where there is a **legitimate interest in confidentiality**.

Examples: designs, price calculation, manufacturing process, recipes, algorithms, list of customers and suppliers, …

In Germany: *§ 2 Abs. 1 GeschGehG*

- Sensorfusion - Data from multiple sensors can be derived or inferred, collected using complex proprietary algorithms (Recital (15))

5.4 - Can the telematics database be protected using the Database regulation?

You cannot use the database regulation to deny access to the data.

Article 43: The **sui generis right** provided for in Article 7 of (EU) Directive 96/9/EC shall not apply when data is obtained from, or generated by a connected product, or related service falling within the scope of this Regulation, in relation to Articles 4 and 5 thereof.

5.5 - What legal measures do I have to protect my expensive research into predictive maintenance? What about specific sensors feeding into complex algorithms? What can be protected and how?

- According to **Recital *(15),*** information inferred or derived from data, by means of proprietary, complex algorithms is protected. Such data does not have to be provided to customers.
- Only the raw data / pre-processed data needs to be provided (others will be able to develop predictive maintenance as well, but your own predictive maintenance results are protected). So, specific sensor information feeding into complex algorithms needs to be provided (this is raw / pre-processed data).

- If complex calculations are performed within the vehicle, and only the results of these complex algorithms are stored in the cloud, the output of these algorithms does not need to be shared. Raw sensor data that is not stored and not extractable, also does not need to be shared.

See EC Data Act FAQ (v. 1.2) Q 27.

6. Suppliers

6.1 - Can a component supplier (acting as third party) use the data from my vehicles (e.g. voltage and (un)charging current) to sell spare parts (such as batteries) to vehicle owners? (What about liability?)

- If the generated data is personal data, the GDPR applies. The purpose of data processing must therefore be stated in advance in the data protection information and, if necessary, consent of the data subject/user must be obtained (GDPR Article 6). The purpose may not be changed or extended retrospectively.
- The sale of spare parts based on generated data is a marketing activity. To implement a marketing measure based on the generated data, competition law regulations must be complied with. Marketing consent must be obtained, unless it is not required (*Directive 2005/29/EC – Directive on unfair commercial practices).*

- **What kind of liability are we talking about?**
  - Warranty claims/functional promise for the regular replacement of spare parts, comparable to warranty extensions.
  - Does requiring maintenance by specialist companies create an unreasonable disadvantage?
    Example: *Linking the manufacturer's warranty to maintenance by an authorized dealer* ("mobilo-life" warranty) – BGH of 12.12.2007 – Ref. VIII ZR 187/06 (Mercedes-Benz).
  - Is the breach of the maintenance agreement or the obligation to use original spare parts the cause of the damage incurred?
    Example: *Unreasonable discrimination against the guarantee-holder due to standard workshop commitment in the case of a paid used car guarantee (Saab)* - BGH of 25.09.2013 - File number VIII ZR 206/12.

See also EC Data Act FAQ (v. 1.2) Q 26.

6.2 - Who is the "data holder" in cases of complex supply chain interactions? E.g. a customer is using a competitor telematics system to track a vehicle my company produced. Does my competitor now become the data holder? Can the competitor ask money for the data from a vehicle that my company produced and for the telematics?

Definition of 'data holder' according to Article 2:

"a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service";

The data holder is the person **who has actual control over the data and can grant access** under the Data Act. It depends on the origin of the data, i.e., if it comes from competitors' hardware or if it comes from the machine.

Identified cases (see for details Q3.5):

- **For users, data access should be free of charge** according to Article 3(1).

- The OEM may sell the telematics services.
- The competitor acting as data holder may charge money for data transferred to other third parties against a reasonable fee.

6.3 - Is the data from our component suppliers running on our CAN-bus owned by the supplier, or owned by the OEM?

If the data is stored in the cloud, the data holder needs to adhere to the regulation. Therefore, ownership is irrelevant if the data is running on the CAN-bus but it is not stored on-device or in the cloud. However, the IP rights must be respected, and contracts shall specify trade secrets and sharing conditions.

6.4 - Can the OEM request access to the data generated by the components in its products?

This is regulated by the contract between the OEM and the supplier and it is normally out of the scope of the Data Act as the data is volatile and not recorded, and not generated by the OEM as a user.

Furthermore, the Data Act entitles *connected product users* to get access to the data they generate. OEMs are not users that generate data through the usage of the product. However, the OEM may bring the data under the scope of the Data Act by transferring it to the cloud. In all cases, a contract with the supplier is necessary.

7. Dealers

7.1 - What is the role (user, data holder, third party) of the dealer or independent repairer in the Data Act? E.g. the dealer collects the data from the gearbox during a maintenance routine.

Dealers:

- Have a contract with the OEM, that specifies rules to access diagnostics data on behalf of the OEM to provide a service to the customer. It requires specific tools and knowledge (including on safety) to be able to perform the activity.
- Conformity of the vehicle needs to be maintained at all times (e.g.: ensuring that there is no tampering with emissions chip-tuning, and ensuring that speed limitations are not removed).
- Could be considered data holders if they download usage information from the vehicle which is otherwise not accessible (e.g. black box data from the electronics systems).

Independent repairers:

- Are third parties if they get the data from the OEM cloud (they follow the contract for third parties).

- Should not perform interventions related to engineering data, except for specific maintenance agreed with the OEM and with specific diagnostic tool access, managed through the RMI (repair and maintenance information) website adhering to dedicated legislation.
- Are not data holders in case the data is machine-generated and stored in the OEM cloud without their involvement (of the repairers).
- Are data holders when they access CAN messages (using the standardized OBD access) and raw or pre-processed data which was generated during the use of the product.
- Are not product users unless they make a test drive.

7.2 - How does the Data Act affect my dealers?

Contractual agreements are important. In most cases the dealers will not be data holders. Data is stored on the systems of the OEM (or a on a supplier's system on behalf of the OEM).

See EC Data Act FAQ (v. 1.2) Q 35.

8. Farming

8.1 - What if agricultural contractors collect data from a farmer's field? How can we arrange data access for the farmer?

In this case, the data is generated by the contractor. The manufacturer must share the data with the contractor as the user of the vehicle. There is no legal obligation towards the field owner or the farmer using the field. However, as a good practice, contractors should follow the "EU Code of conduct for agricultural data sharing by contractual agreement".

8.2 - What about the rights of the farmer on the farming data?

Farming data can be personal or non-personal, depending on whether the data can be linked to a person (e.g. vehicle with a driver vs. weather station).
Farmers have:

1) Rights on farming data according to GDPR Articles 15 to 21 concerning **personal data** (right of access, to erase, data portability, etc.)
2) Rights on farming data according to the Data Act concerning **user-generated machine data** (if they were the user of the vehicle):
    (I) the right to free access to the data (Article 3).
    (II) the right to share the data with third parties (Article 5).

For other data (e.g. the farmer did not generate the data himself through the usage of a machine because he used a contractor) we rely on value chain participants to adhere to the "Code of Conduct for agricultural data sharing by contractual agreement".

8.3 - Is field data personal if we can identify the owner of the field? Is a field protected by GDPR better protected against "Exceptional Need" (B2G)?

- (Field) Information is personal if it says something about a person. Otherwise it is just non-personal data, which is most often the case.
- Only if non-personal data is insufficient to respond to the exceptional need to use data (Article 17(2), point (e)), personal data shall be requested. Supervisory bodies shall be informed (Article 17(2), point (i)). Where personal data is necessary, protection measures will be specified (Article 17(1), point (g)).
- The data holder must anonymise the data before sharing it, unless the request specifically requires personal data. (Article 18(4))

8.4 - Can I (as a data holder) make voluntary agreements with my users to respect the "EU Code of Conduct on agricultural data sharing"? In that case, could the customer decide not to share the data from his machine with the manufacturer, while the manufacturer is also not be obliged to share IP-sensitive data?

- While good agreements make good friends, contracts which counteract a legal requirement are not enforceable. Adherence to the Code of conduct will remain voluntary (a gentlemen's agreement). However, in B2B relations, voluntary agreements are possible (Article 25).
- Only a new regulation (e.g. a specific legislation for data exchange in agriculture) could convert the Code of conduct into a legal requirement.
- Note that standards for data spaces in agriculture may guide (not enforce) the way that data will be exchanged within the eco-system. The development of generic (cross-domain) standards by CEN/CENELEC is mandated in the Data Act. Vertical standards are being developed by e.g. AEF (AgIN). Standards also need to address ethical considerations (i.e. balance of power).

9. Authorities

9.1 - Do equipment manufacturers share liability due to potential knowledge of legal infringement, e.g. when handling data about chemical application in the field?

Example: A contractor is spraying the field of a farmer. He exceeds the legal amount of product. The contractor and the OEM (may) know about this legal infringement through data. Does the data create any liability for the OEM? Does the ownership of data (and liability) need to be transferred to the farmer?

Answer: This falls outside the scope of the Data Act; however, it remains a concern for the OEM. It is more of a fear than a risk that also exists in other businesses. E.g. a car owner can drive 200 kph where 100 kph is allowed. The car manufacturer knows this based on combined data from GPS and car. However, OEMs are not law enforcement and cannot intervene. (Article 1(6))

9.2 - What if a cybersecurity incident/accident happens? Is there a specific process for criminal investigation?

Sharing data in the frame of a criminal investigation will require a court order. For cybersecurity incidents, the relevant regulations and standards must be followed. Data handling procedures and forensics should be part of the OEM's cybersecurity incident response plan.

9.3 - If the government launches a data request, should it go to all competitors at once, or can specific companies be selected?

Governmental data requests should only occur if there are no other means to get the data (e.g. through purchasing) (Article 15). Requests must be limited to data relevant for the specific need. This may cause a differentiation, depending on which data holders possess relevant information (e.g. on. a forest fire, only certain data sources may be useful). The selection of data holders will be justified (Article 17 (1), point (e)) but should not consider whether data holders are competitors or not.

For statistical purposes, the European Commission needs to ensure the sample is big enough and random (i.e., not blue or red or green, but a mix).

9.4 - How long can the government keep the data?

The Data Act articles that should be considered are **Articles 19** (Obligations of public sector bodies, the Commission, the European Central Bank and Union bodies) **and Article 21.**

Article 19 (1), point (c) states that public authorities must erase the data after use.
Article 21(4) states: *Notwithstanding Article 19(1), point (c), individuals or organisations receiving the data pursuant to paragraph 1 of this Article may keep the data received for the purpose for which the data was requested for* ***up to six months following erasure*** *of the data by the public sector bodies, the Commission, the European Central Bank and Union bodies.*

9.5 - A farmer is supposedly performing non-compliant farming operations. Can the Data Act be used by the government to request the farmer's data from the OEM? Can the government use the data to monitor CAP (Common Agricultural Policy) compliance?

Requests related to criminal infringement require a court order. Governments (or related bodies) may only request data under "exceptional need", and if that data cannot be acquired through any other means.

ABOUT CEMA

CEMA aisbl (www.cema-agri.org) is the association representing the European agricultural machinery industry. With 11 national member associations, the CEMA network represents both large multinational companies and numerous European SMEs active in the sector.

CEMA represents about 1,300 manufacturers, producing more than 450 different types of machines with an annual turnover of about €40 billion and 150,000 direct employees. CEMA companies produce a large range of machines that cover any activity in the field from seeding to harvesting, as well as equipment for livestock management.

For more information, please contact:

CEMA aisbl

European Agricultural Machinery Industry Association

Avenue de Tervueren 168

1150 Brussels

Tel. +32 2 706 81 73

secretariat@cema-agri.org