January 17th, 2025

FRENCH AUTOMOTIVE INDUSTRY
TECHNICAL POSITION PAPER
CONFIDENTIALITY LEVEL: N3 (PUBLIC)

INTERPRETATION GUIDE - DATA ACT – VERSION 2

Supersedes version 1 of September 2024

Disclaimer:

This guide reflects the collective understanding of a group of automotive sector experts regarding the European Data Act. All discussions and interpretations within this document fully comply with competition law and focus exclusively on the legal and technical framework of the Data Act. No strategic plan or commercial matters are addressed in this guide.

As the Data Act is in force but not yet in application, and in the absence of specific automotive recommendations from European bodies, dedicated authorities or court rulings, this document is based on a free interpretation of the text.

The Data Act is a cross-sectoral European regulation. As such, its application contains several points open to interpretation.

The automotive sector complies with many regulations on data that are already in force. To ensure an effective deployment of the Data Act on access to vehicle and related services data, the French automotive industry has decided to prepare a guide detailing how it understands its requirements.

This action is part of those defined by the “Contrat Stratégique de Filière 2024-2027” (Strategic agreement for the automotive industry) approved by French Authorities and Automotive Industry.

The guide is consistent with the PFA position paper ACCESS TO EXTENDED VEHICLE DATA dated 09-MAR-2021, referring to the extended vehicle standards set (ISO20077 series, ISO20078 series)[1].

This paper reflects work in progress within the PFA. The paper will be evaluated and updated regularly as our understanding progresses.

The term “Refer to FAQ Data Act” indicates the chapter of the “FAQ Data Act – Version 1.1” from 13 September 2024, published by European Commission which has been used to build our position.

(1) https://pfa-auto.fr/wp-content/uploads/2021/04/PTF_Access-to-extended-vehicle-data_EN_APRIL_2021_V4.pdf

1- Data categories

This section defines our understanding of the different data categories mentioned in the text.

Raw data

Raw data can be defined as data referring to physical measurements of the real world as produced by sensors.

Are considered as "raw data":

- Information resulting from direct action by the USER: controls, screens, buttons…
- Direct physical measurement from sensors, including formatting and scaling, units,

Example of raw data:

- *Wiper on manual command,*
- *Trigger and status of component of the car: handbrake (ON/OFF), wiper, A/C usage, car/door/window locked/unlocked…*
- *Data from simple triggering (periodic, end of journey…)*
- *Wheel speed sensor signal*
- *Tension and intensity at the electric engine entrance*
- *Tyre pressure from TPMS valve*

Pre-processed / non-substantially modified raw data

These types of data can be defined as the result from elementary processing making the data usable or understandable by product or services designers.

PFA regards the obligations related to these data, in the framework of Data Act, as identical to those of raw data.

System information resulting from processing (status, variables, etc.), data from unitary arithmetic operations on raw data, or participating in processing (parameters) even if initially generated by a USER action. This kind of data is already shared by some OEMs (API store, Android Automotive, ...).

Example of pre-processed data:

- *Status of Electric vehicle or Internal Combustion Engine functioning, stop/start state, automatic wiping/lights, ...*
- *External temperature*
- *Engine speed*
- *Information displayed in the vehicle: vehicle speed (displayed on the dashboard), fuel level (displayed on the dashboard)*
- *Wheel rotation per Minute*
- *Normalized tyre pressure at reference temperature*

Inferred or derived data

There is no definition in the industry or normative literature on the concept listed (fine-tuning data, status, complex triggers).

PFA considers that derived data is all the data which is not raw nor pre-processed.

Following some examples to illustrate what might be inferred or derived data:

- *sensor misalignment, drift…*
- *offset compensation of sensor, triangulation, fusion, enhanced vehicle speed (calculate with additional data as accelerometer, yaw rate sensor, …)*
- *algorithm tuning, adjustments, calibration...*
- *extraction of objects and their physical properties, occupancy grids, straightening, blurring, quality enhancement, etc.…*

Metadata

“Metadata” is a set of data that describes and gives information about other data.

There are 2 categories of Metadata:

- Those required by the company / DATA HOLDER for internal use (cybersecurity, privacy, IT governance, …)
- Those required by law - when not explicitly specified (as in the Data Act), DATA HOLDER must list the relevant metadata needed to understand and use the shared data.

In the ISO Extended Vehicle framework, ISO/TC22/SC31 has launched a new project registered in the TC/SC working program “Data structure description” ISO/AWI TS 20077-4.
This project provides the essential characteristics (metadata) to understand the data and functions exposed via an ExVe interface.
See ISO portal: https://www.iso.org/fr/standard/84534.html

This project could be used as referential (when published) to apply Data act requirements regarding Metadata.

Other information required by Data Act

The articles 3(2) and 3(3) mandate to provide the following information to the User:

Type, format, estimated volume, frequency of collection, storage, means of access**, data holder identity, data holder contact*, request process*, contract duration.

In the ISO Extended Vehicle framework, the following standards could be used as referential to apply Data act requirements regarding “information to the User”:

(*) Request process, data holder contact:

ISO TS20077-3:2024 “Upstream process to develop services”

(**) Means of access:

ISO20077-1:2017 “Extended vehicle (ExVe) methodology – General information”
ISO20077-2:2018 “Extended vehicle (ExVe) methodology – Methodology for designing the extended vehicle”

Related Services data

Before defining “related service data”, we need to clarify what a related service is for a vehicle.

Related service

A related service is considered to be:

- A digital service or software
- Connected to the product:
  - Involving a remote connection to an off-board system
  - Allowing the product manufacturer or a third party to add, update or adapt certain vehicle functions.
  - Involving the exchange of data between the product and the service provider.
- Explicitly linked to the operation of the product's functions.
- Its absence would prevent the connected product from fulfilling one or more of its functions.
- Capable of transmitting commands to the product that may affect its action or behavior.

Refer to FAQ Data Act §8: The FAQ indicates that a related services is defined by 2 conditions:

- There must be two-way/bidirectional exchange of data between the connected product and the service provider.

AND

- The service must affect the connected product’s functions, behavior, or operation.

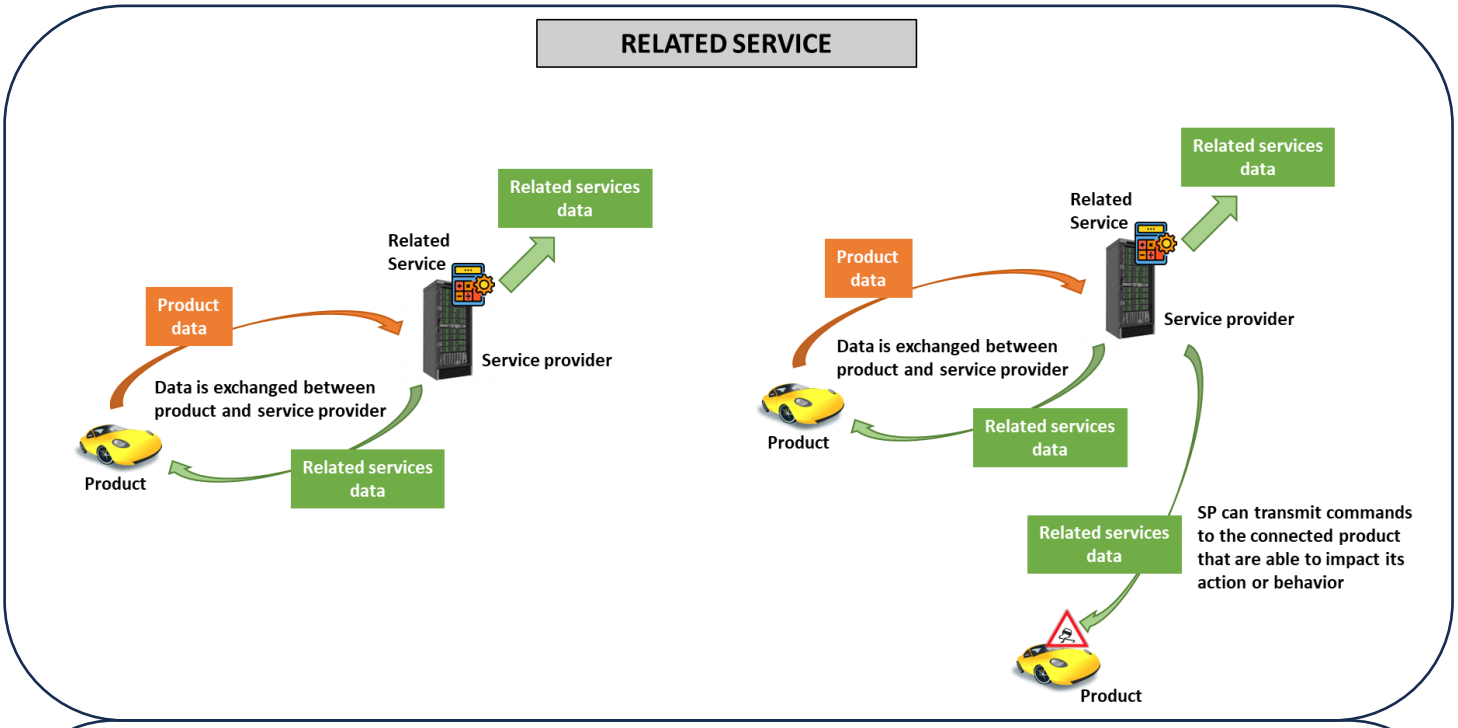
Are not considered as related services:

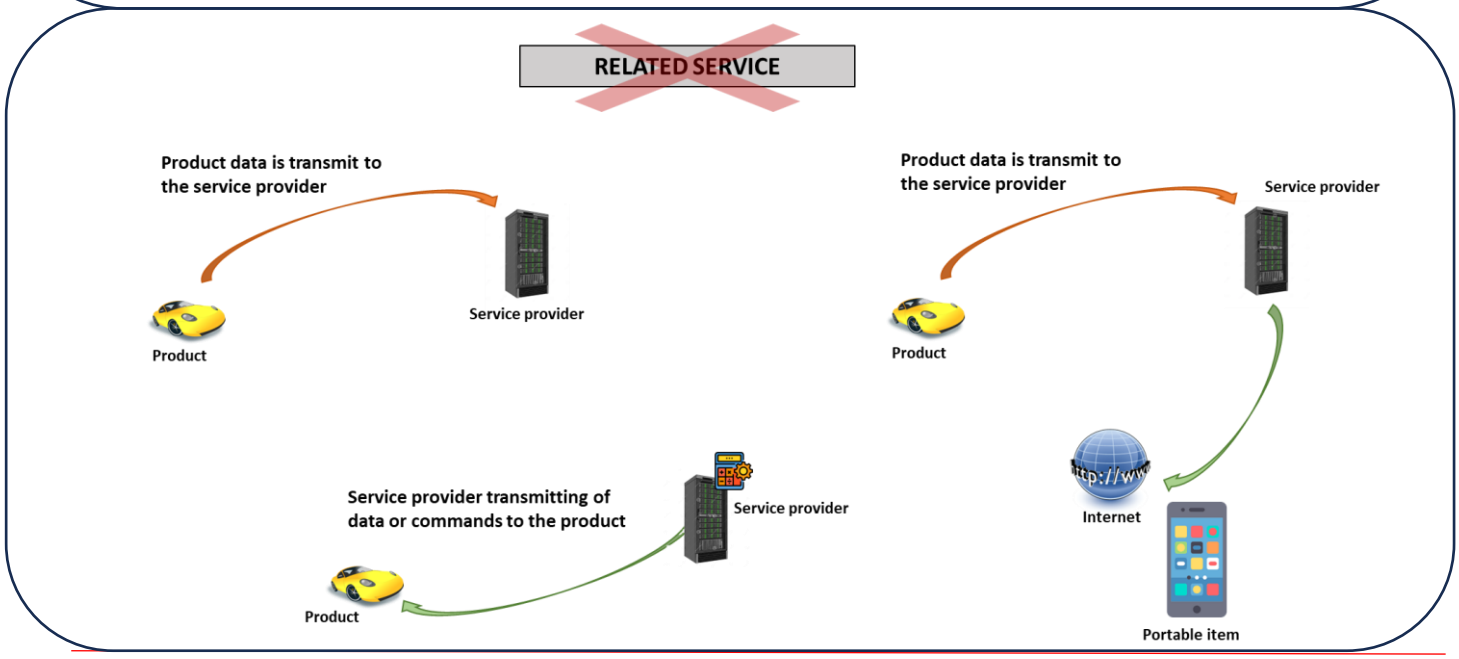
- Services that do not affect the operation of the product and do not involve the transmission of data or commands to the product by the service provider.
- Ancillary consulting, analysis, or financial services
- Regular repair and maintenance
- (Product) power supply and connectivity power supply

The following examples are not considered as related services:

- *New vehicle "function" (or update), X2V (data reception from other vehicles or infrastructure or ITS server), route calculation results with EV charging, …*
- *On-board application sending data to its servers, smartphone application using vehicle data (e.g., vehicle charging history) without feedback to vehicle, V2X broadcast mode, PAYD (insurance)*

The following two schemes illustrate our understanding of what is and what is not a related service.





Related services data is:

- Data representing the digitalization of user actions or events related to the connected product: controls, screens, buttons, etc.
- Data recorded intentionally by the user or as a by-product of the user's action.
- Data generated during the provision of a related service by the provider based on product data: 'The related services data will be provided by the provider of the related service (third party, manufacturer acting as provider).

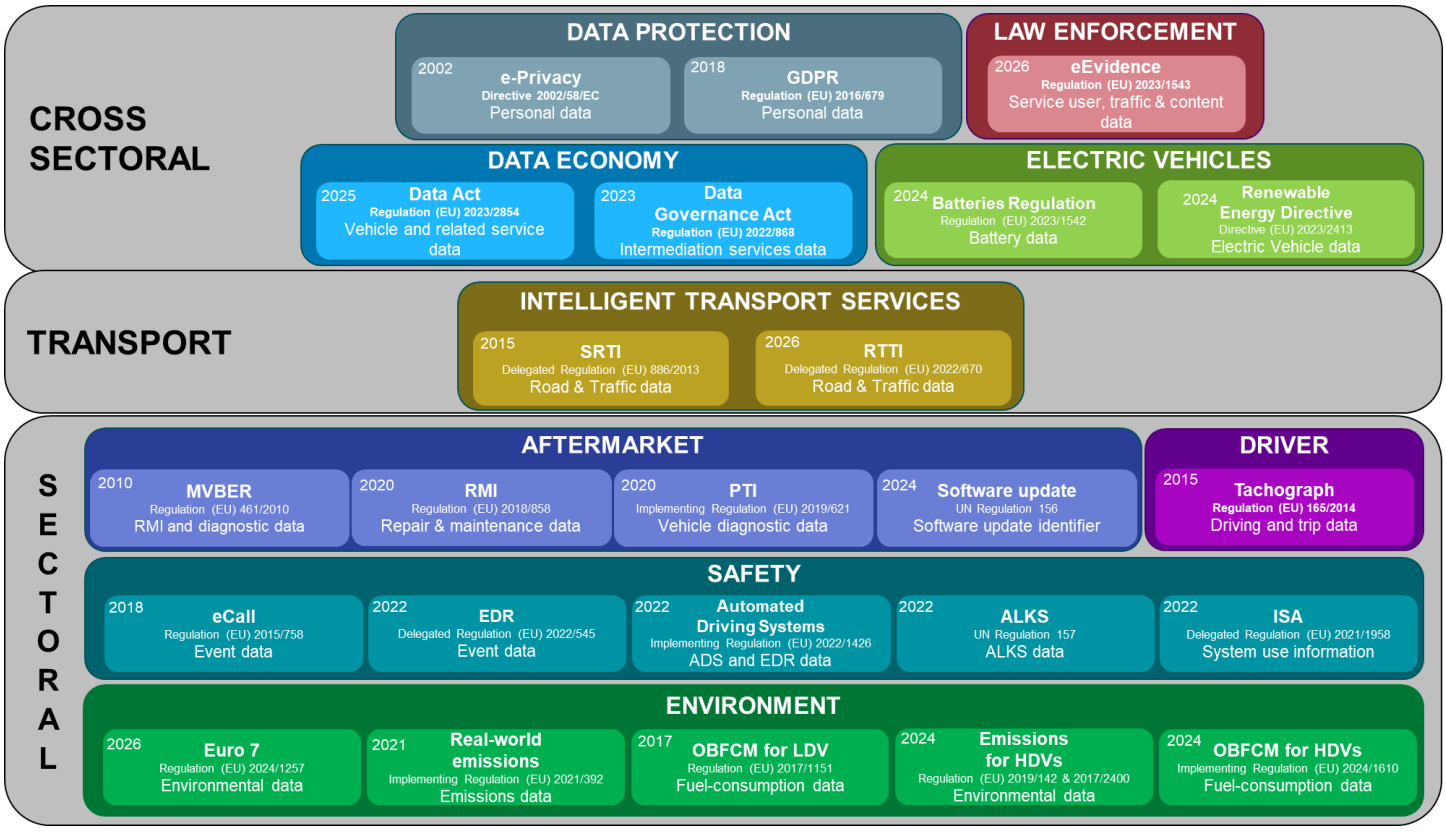
Regulatory Data

As demonstrated in the chart below, here are many regulations involving vehicle data.

There is a risk of inconsistency which represents legal uncertainty for all ecosystems. Some might consider that insofar as regulated data is accessible to the data holder, it falls within the scope of the Data Act.

It is critical to have European Commission clarifying the interplay between the regulatory framework and Data Act. Only such a clarification will allow legal certainty, user's right protection, and growth.

The following picture shows the main EU regulations already (or soon) in force.



The recently published FAQ Data Act, in question 24, attempts to a precision regarding the application compensation for other regulations with legal data-sharing obligation for the data recipient.

As expected, these clarifications confirm the hierarchy of rules within the European Union, especially with GDPR (FAQ Data Act §1 to 3). However, there are still interrogations about the consistency between Data Act and other sectoral regulations.

Security-related data

(see Article 4.2) Users and data holders may contractually restrict or prohibit accessing, using, or further sharing data, if such processing could undermine security requirements of the connected product, as laid down by Union or national law, resulting in a serious adverse effect on the health, safety, or security of natural persons.

The car manufacturers may use dedicated data that are key in some strategies to

- lower the tampering attempts against the environmental protections (pollution and emission control systems),
- reconfigure the behavior of the system to avoid a vehicle safety issue (functional diagnostics, safety concepts),
- detect intrusions in the vehicle (physical access or cybersecurity attacks).

We acknowledge that the Regulation frame the restriction of sharing Security-related data. This measure is valuable in preventing access to such data by potential malicious parties who may use it to compromise vehicle security.

Intellectual Property-related data

For data protected by intellectual property rights, the Data Act does not affect or call into question existing laws concerning the protection of intellectual property rights (Article 1(8) and Recital 13). This includes in particular:

- Directive 2001/29/EC (often referred to as the Directive on Copyright in the Information Society), which harmonizes certain aspects of copyright and related rights in the European Union.

- Directive 2004/48/EC (on the enforcement of intellectual property rights), which concerns the enforcement of intellectual property rights and provides legal tools to protect them.

- Regulation (EU) 2019/790 (Directive on copyright and related rights in the digital single market), which modernizes copyright rules in the digital context.

Consequently, are excluded from the scope of the right to access, use and make available data covered by the Data Act the content protected by intellectual property rights (e.g. content protected by copyright, trademark, patent or design law but not the sui generis right of databases maker).

The Data Act mentions a protection under intellectual property law for content protected by intellectual property rights, such as textual, audio, or audiovisual content. Then, the data generated when the user records, transmits, displays, or plays such content, as well as the content itself, are not subject to the sharing obligations provided for in this Regulation.

We understand the purpose of this exclusion as a protection of exclusive rights of intellectual property rights holders in their creations and maintaining the economic balance established by intellectual property law (conformed by recital 13).

Excluded from the scope of protection under intellectual property law (and therefore included in the scope of the Data Act) are source data, understood as data in raw form (data points that are generated automatically without any further processing), as well as data that has been pre-processed with the aim of making it comprehensible and usable prior to further processing and analysis.

Trade secret-related data

Definition of trade secret:

Concerning business secrecy, Article 2(18) of the Data Act refers to the definition in Directive (EU) 2016/943 Article 2 (18): “business secret: a business secret within the meaning of Article 2(1) of Directive (EU) 2016/943”.

Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against unlawful obtaining, use and disclosure - lays down the 3 conditions for information to fall within the scope of secrecy:

a) They are secret in the sense that, as a whole or in the exact configuration and assembly of their elements, they are not generally known to, or readily accessible by, persons belonging to the circles which normally deal with the kind of information in question,

b) They have commercial value because they are secret,

c) The person who lawfully controls it has taken reasonable steps, given the circumstances, to keep it secret.

The holder of a business secret is defined as “any natural or legal person who lawfully has control over a business secret”.

Principle: right to access, use and make available protected business secrets

Data holders may not refuse a request for access to data submitted under the regulation solely on the grounds that certain data are considered to be trade secrets, provided that “the data holder and the user take all necessary measures prior to disclosure to preserve their confidentiality, in particular as regards third parties”.

The data holder or, if they are not the same person, the trade secrets holder, identifies the data protected as trade secrets, including in the relevant metadata.

Security measures, particularly when sharing with third parties, can take the form of standard contractual clauses, confidentiality agreements, strict access protocols, technical standards, and the application of codes of conduct.

- These standard contractual clauses will be drawn up by the Commission before September 12, 2025.

- Codes of conduct are to be defined by economic sector or industry.

Weakening: blocking or suspension of access rights

If the user fails to implement the agreed technical and organizational measures, or compromises the confidentiality of business secrets, the data holder may block or, as appropriate, suspend the sharing of data defined as business secrets.

This decision must be justified and documented.

The exception: rejection of a request for right of access

In exceptional circumstances, where the data holder who is a trade secret holder can demonstrate that it is highly likely that he will suffer serious economic harm as a result of the disclosure of trade secrets, despite the technical and organizational measures taken by the user, the data holder may refuse a request for access to the specific data in question on a case-by-case basis.

This decision must be duly substantiated based on objective factors, in particular the enforceability of trade secret protection in third countries, the nature and level of confidentiality of the data requested, and the unique and new nature of the connected product and shall be provided to the user in writing without undue delay.

Recourse to the competent authority

In the event of disagreement, the parties may refer the matter to the competent authority for resolution: supervisory authority, dispute resolution body (or competent court which cannot be set aside by the Regulations).

Database rights (Sui generis)

In order to eliminate the risk that holders of data contained in databases obtained or generated by means of physical components, such as sensors, a connected product or related service, or other types of machine-generated data, might invoke the sui generis right provided for in Article 7 of Directive 96/9/EC, and thus hinder, in particular, the effective exercise of the right of users to access and use data, as well as the right to share data with third parties provided for in this Regulation, it should be made clear that the sui generis right does not apply to such databases.

Article 43 states: “The sui generis right provided for in Article 7 of Directive 96/9/EC shall not apply where data is obtained from or generated by a connected product or related service falling within the scope of this Regulation, in particular as regards Articles 4 and 5 thereof.”

The data holder cannot therefore invoke database copyright or the right of the database producer to reject a request for a right of access to data under the Data Act.

Specific raw data: "Closed loop" data

According to regulation (EU)2023/2590 on "Advanced Driver Distraction Warning", the article 2.3.2 request that:

"The ADDW system shall be designed in such a way that it shall only continuously record and retain data necessary for the system to function and operate within a closed-loop system."

This system is based on inside camera to monitor the behavior of the driver. Moreover, the regulation (EU)2021/1341 for the same function (ADDW) can do without the camera, by using another mean (e.g. vehicle trajectory analysis).

All data which contribute of vehicle functioning, but which are not transmit outside the vehicle are "closed loop data".

Data running in a closed loop within a vehicle are not retrievable, and therefore, cannot be accessed by neither the car manufacturer either the User.

2- Data access

Art. 3.1 / 4.1 / 5.1

The vehicle is a set of complex systems and processes a large quantity of data (up to 25GB/h of data generated per vehicle / 4TB of data generated for 8 hours for a vehicle, the cameras alone generate 20 at 40 Mbps, and radar between 10 and 100 kbps).

According to our understanding, article 3.1 refers only to vehicle's "product data".. Therefore, we consider there is no obligation to design the product to provide all data generated during the use, but only data that the manufacturer designed to be retrievable.

Data readily available (Data act art. 4.1, art. 5.1) or directly accessible (Data act art. 3.1) to the user are those which are already accessible to the data holder and that the product can provide via data access interfaces (local and/or remote) compatible with the design of the product (see ISO20077-1:2017 et ISO20077-2:2018 - Extended Vehicle / ExVe methodology).

Cybersecurity

The cybersecurity regulations are without prejudice to other regulations/legislations governing the access by authorized parties to the vehicle, its data, functions and resources, and conditions of such access (art. 1.3 of UNR155, NIS2, CRA).

Taken together, these regulations demonstrate a clear division of responsibilities between:

- the manufacturer: Defines and implements the cybersecurity perimeters, rules, and solutions, in particular access management rule and solution, in Extended Vehicle to manage cyber risk.
- the user: Control and review of access rights in compliance with applicable regulations, particularly the Data Act.

3- Application scope

Article 50 – Entry into force and application

- The Data Act applies to all connected products whose characteristics correspond to the regulation's definition, regardless of whether they are new, used, reconditioned, or retrofitted.

- There is no legal or regulatory definition of a refurbished product. In the absence of clear case law on the subject, the Commission's Blue Guide provides a useful clarification, subject to any contrary interpretation of case law.

- When modifying a connected product that has already been placed on the market for the first time, the manufacturer must ask himself whether his modification or transformation results in a new product, by means of a risk assessment. If the answer is yes, the manufacturer is considered to be the manufacturer of the modified connected product and must fulfill the corresponding obligations. In particular, he must ensure that the product complies with the Data Act at the time he makes the product available, i.e. when it is supplied (for distribution or use on the EU market). In this case, making the product available again is akin to “placing it on the market”.

Refer to FAQ Data Act §4 (table):

Readily available data	Product data and related service data that a data holder can obtain without disproportionate effort going beyond a simple operation. The definition of 'readily available data' does not include a	Recitals 20 and 21, Article 2(17)
	reference to the time of their generation or collection. Only data generated/collected after the entry into application of the Data Act should be considered as falling within the scope of Chapter II.	

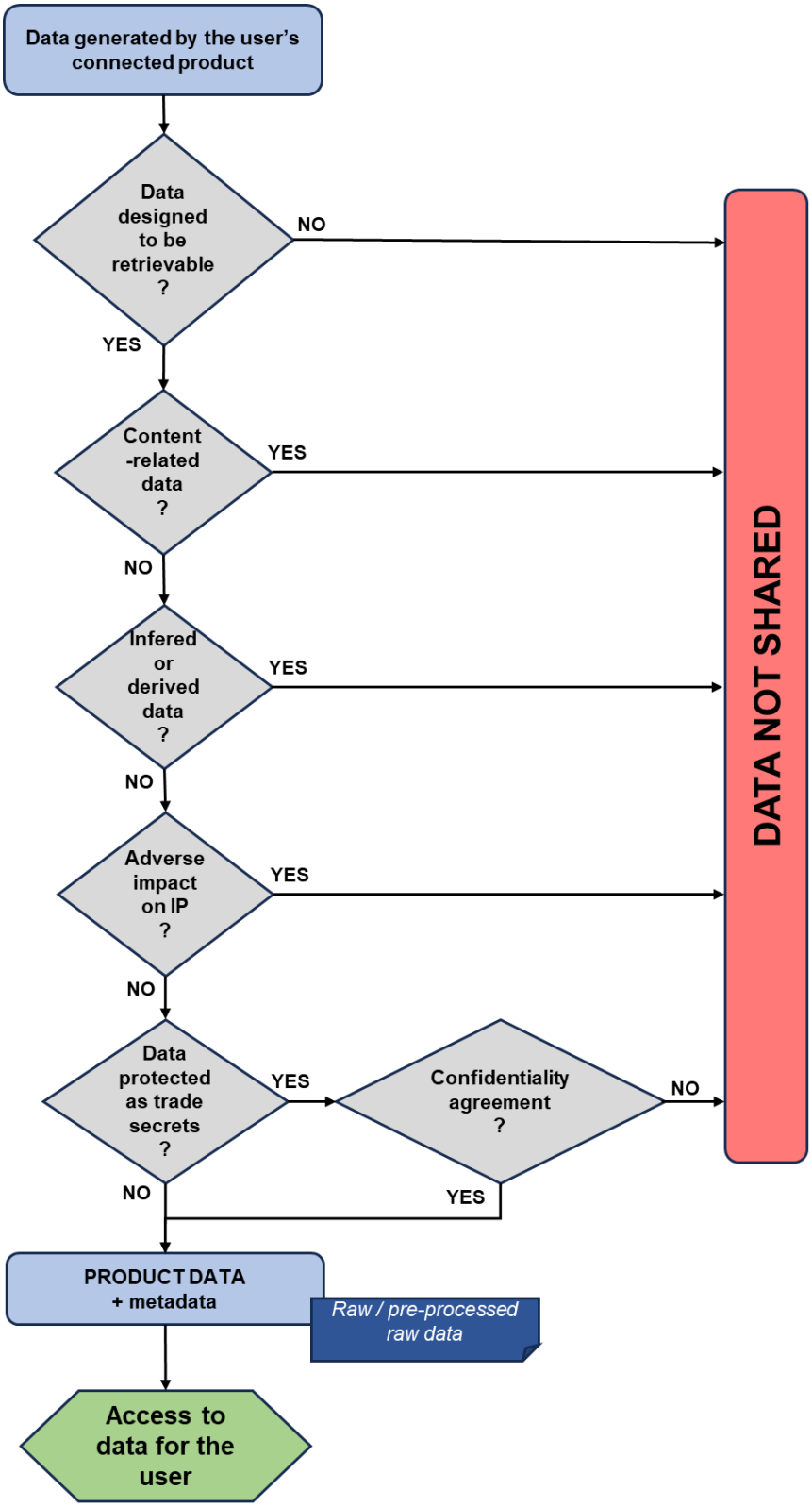
The application of the text is understood as following:

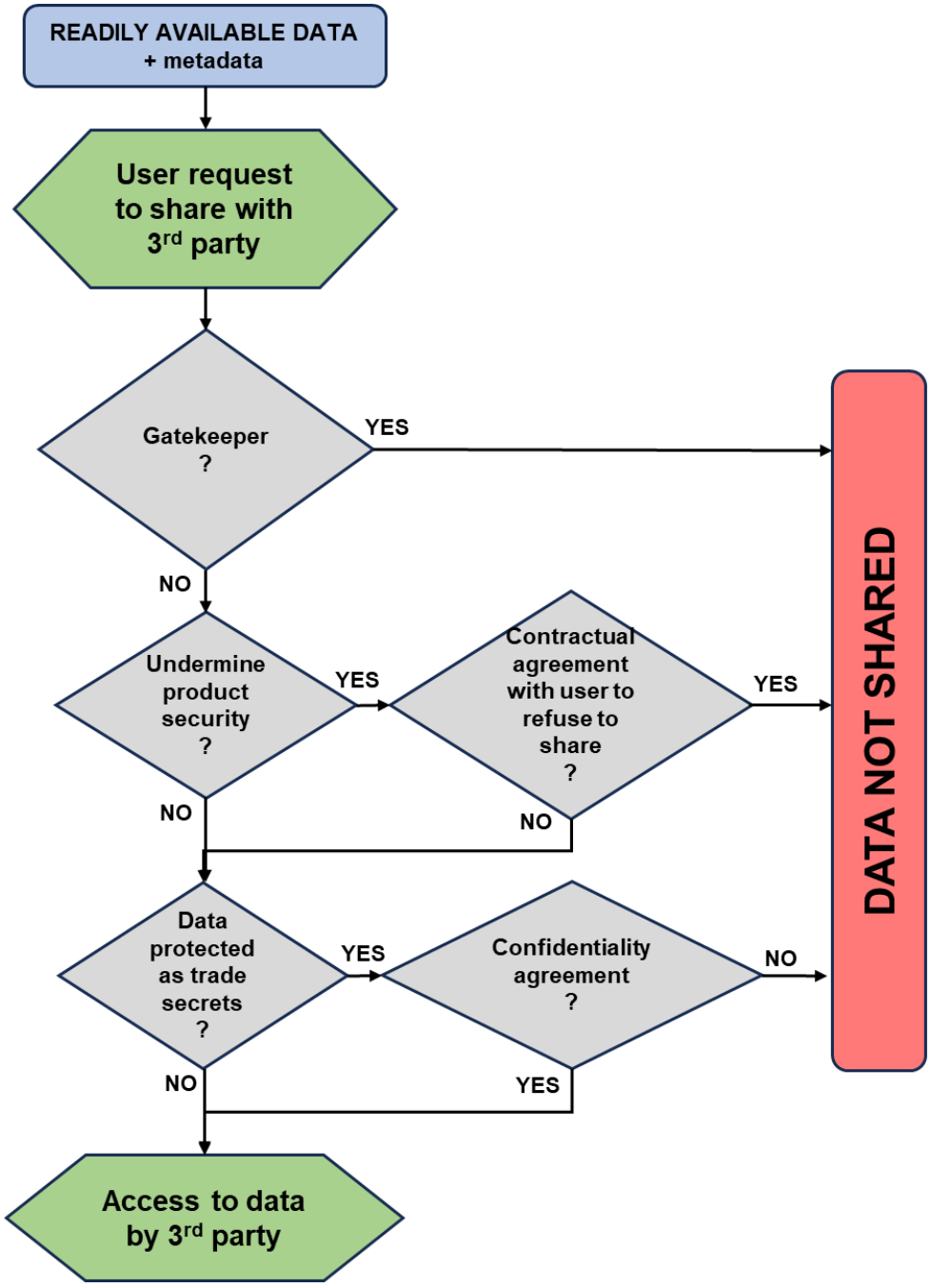
- **For connected products and related services which have been placed on the market before and after the 12 September 2025, only readily available data generated/collected after the application date fall in the scope of the Data Act (articles 4(1) and 5(1)).**

- **The article 3(1) applies to connected products and related services placed on the market from 12 September 2026.**

4- Data Act flowchart

The scheme below shows a flowchart of process to follow when analyzing data access request by the user, and by a 3rd party (under request of the user).




READILY AVAILABLE DATA
+ metadata
User request to share with 3rd party
Gatekeeper ?
YES
NO
Undermine product security ?
YES
Contractual agreement with user to refuse to share ?
YES
NO
NO
Data protected as trade secrets ?
YES
Confidentiality agreement ?
NO
NO
YES
DATA NOT SHARED
Access to data by 3rd party