SERVITLY

Data holders' guide to implementing EU Data Act technical obligations

This document is addressed to “data holders” under the "EU Data Act" regulation and provides regulatory references, indications and useful examples for implementing the new functions required to meet the law’s technical obligations.

Specifically, it is intended for IT or R&D managers responsible for defining and developing the "IoT system" that collects and manages data from connected products.

VERSION 1.2 / 30 OCTOBER 2025

Summary

Introduction

The official documents of the regulation

Within this guide, we will often refer to the official documents of the regulation. You can find them here:

The full text of the Data Act, Regulation (EU) 2023/2854 of 13 December 2023:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302854

The FAQ document (PDF) published by the European Commission (version 1.3 of 12 September 2025):
https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act

Why the Data Act

80% of the data generated by connected products is never used.

The European Commission designed the Data Act to address the legal, economic, and technical issues that lead to this underuse of data.

The regulation aims to stimulate a competitive data market, open opportunities for data-driven innovation, and make data more accessible for all. This will lead to new and innovative services and more competitive prices for connected aftermarket services. To this end, the law clarifies who can use what data and under which conditions, ensuring fairness in the allocation of the value of data amongst the actors in the data economy.

The official portal by the European Commission about the Data Act:
https://digital-strategy.ec.europa.eu/en/policies/data-act

The press release that announces the new regulation and the rationale behind it:
https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

A comprehensive overview of the regulation, including its objectives and how it works in practice:
https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

The Data Act at a glance

In short, the Data Act consists in obligations and rights for:

Subjects who have to give access to data:			**Subjects who have access to data:**		
Manufacturers of connected products	Providers of related services	Data holders	Users	Third parties	Public bodies

These obligations and rights fall into the following areas:

1. the definition of **contractual terms** between the parties
2. the **design** of connected products
3. **information** provided to the users of connected products
4. **data sharing**:
    a. with users
    b. with third parties
    c. with public bodies
5. the collection of **compensation** for sharing data with third parties

The regulation also defines:

- obligations for providers of Cloud-based data processing services, to facilitate **switching** between providers
- the basis for setting **interoperability** standards

Technical obligations

Compliance with this regulation therefore concerns not only contractual or organizational aspects, but also technical ones.

In particular, here are the areas where obligations/rights require the implementation of new functions in data holders' IoT systems:

Area	As a data holder, do you need to implement new functions in your IoT system?
definition of contractual terms between the parties	NO
design of connected products	NO
information provided to the users of connected products	optional
data sharing with users	YES
data sharing with third parties	YES
data sharing with public bodies	optional
collection of compensation from third parties	YES

Important dates

- 12/09/2025: all rights and obligations apply, except:
  - the obligations relating to the design of connected products (Art 3.1)
  - the rules on unfair contractual terms (Art 13)
- 12/09/2026: the obligations relating to the design of connected products apply (Art 3.1)
- 12/09/2027: the rules on unfair contractual terms apply (Art 13)

Specific focus of this guide

This guide refers specifically to the areas that require implementing new functions in your IoT system, namely:

- data sharing with users
- data sharing with third parties
- collection of compensation from third parties

Before addressing the technical implications, you need to evaluate whether and how you are affected by the obligations to share data with users and third parties.

Initial assessment

To understand whether and how you are affected by the obligations to share data with users and third parties the aspects to evaluate are:

- ☐ The size of your company
- ☐ Which products fall within the scope of the regulation
- ☐ If your company is a data holder
- ☐ What data falls within the scope of the regulation
- ☐ Who are the users of your products?

Size of your company

Data sharing obligations with users and third parties depend on the size of the company.

Data holder company size	Obligations to share data with users and third parties
Micro and small enterprise (employees < 50 and turnover <10 M€)	Not applicable
Medium-sized enterprises (employees < 250 and turnover < 50 M€)	They apply 1 year after the date on which the connected product is placed on the market
Large enterprise (employees > 250 or turnover > 50 M€)	Fully applicable

REGULATORY REFERENCES

Article 7.1

The obligations of this Chapter shall not apply to data generated through the use of connected products manufactured or designed or related services provided by a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service.

The same shall apply to data generated through the use of connected products manufactured by or related services provided by an enterprise that has qualified as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise.

Which products?

The scope of the regulation extends to literally any type of connected product.

The law defines a connected product as any item capable of obtaining, generating or collecting data about its use, performance or environment through its components or operating systems, and communicating such data via an electronic communications service, physical connection or device access.

The regulation applies to all connected products already placed on the market in the EU and to new products (when placed on the market), regardless of the place of establishment of their manufacturer.

REGULATORY REFERENCES

Article 2.5

‘connected product’ means an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user;

Recital 14

[…] Connected products that obtain, generate or collect, by means of their components or operating systems, data concerning their performance, use or environment and that are able to communicate those data via an electronic communications service, a physical connection, or on-device access, often referred to as the Internet of Things […]

FAQ 7 "What is a 'connected product'?"

Connected products are items that can generate, obtain, or collect data about their use, performance, or environment and that can communicate this data via a cable-based or wireless connection. This includes communication of data outside the product on an ad hoc basis (e.g. during maintenance operations) […]

FAQ 8 "What determines whether a connected product falls in scope of the Data Act?"

A connected product falls within the scope of the Data Act if it has been 'placed on the Union market' (Article 2(22)).[…] The concept of placing on the market refers to each individual product, not to a type of product. The requirements laid out in the Data Act are therefore applicable only to individual products […] and not to all products of that type.

FAQ 28 "Does the Data Act apply to manufacturers of connected products and providers of related services that are established outside the EU?"

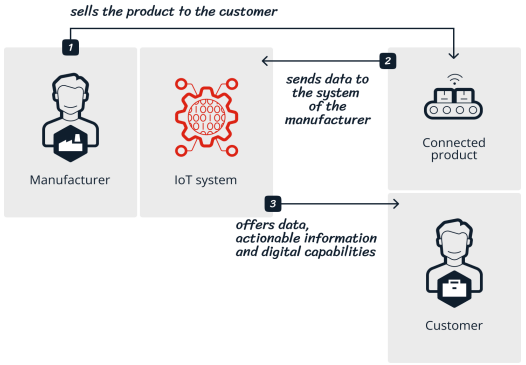
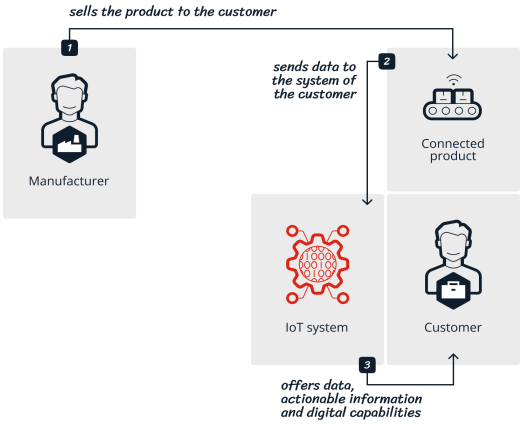
Yes. The Data Act does not require the manufacturer or related service provider to be established in the EU. […] the place of establishment of the provider of the related service is not a factor in determining whether they fall within the scope of the Data Act

Is your company a data holder?

Determining whether a data holder exists and who it is does not depend on who produced the hardware or software, but on who controls access to the data. This entity can be:

- the manufacturer
- a third party appointed by the manufacturer
- the provider of a related service

Furthermore, there are cases where no data holder exists. To find out if you are a data holder, answer this question: *What are your connected products connected to?*

If your connected products are connected to your IoT system	If your connected products are connected to your customer's IoT system
you are a data holder	you are not a data holder and in this case there is no data holder at all
	

REGULATORY REFERENCES

Article 2.13

‘data holder’ means 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;

FAQ 21 "Is a manufacturer always a data holder?"

Even though manufacturers will typically be data holders, this is not always the case. The Data Act allows an entity to 'outsource' the role of 'data holder'. […] Determining who the data holder is does not depend on who produced the hardware or software, but on who controls access to the readily available data. […] It is nevertheless possible under the Data Act for a person to be a user without there being a data holder. This situation could occur, for example, if a user acquires a connected product where the data are stored directly on the device or transferred from the device to the user's computer, and the manufacturer does not have access to any of the data. In this scenario there is no data holder, since only the user has access to the data.

FAQ 34 "Can a company be both a user and a data holder at the same time?"

[…] A company cannot simultaneously be a user and a data holder for the same data, and, a user sharing data with a third party should not be considered a data holder for that third party. […]

What data?

The regulation distinguishes between: raw data, pre-processed data, processed data.

1. Raw Data: data points that are automatically obtained, generated, or collected by the connected product without any further form of processing.
2. Preprocessed data: data accompanied by the necessary metadata to make it understandable and usable.
3. Processed data: highly enriched data, meaning inferred or derived data or data that result from additional investments (including by way of proprietary, complex algorithms).

Only raw data and pre-processed data are in scope. Processed and enriched data are out of scope.

Furthermore, only data that is already stored, or transmitted, and readily available are in scope. Where, on the other hand, the design of the connected product, and/or its components, does not provide for data being stored or transmitted outside, such data are out of scope.

The regulation does not impose an obligation to store data in the central computing unit of a connected product.

Only data generated or collected after the entry into application of the regulation (12 September 2025) are in scope.

Examples of raw data

- data about the use of the product by the user, recorded intentionally or which result indirectly from the user's action
- data generated by the user interface (HMI) or via a related service (a Mobile App that allows remote control of the connected product)
- data about physical quantity or quality detected by the product, such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed

- data collected by sensors regarding the environment in which the product operates and the interactions it may have
- data collected by internal sensors or applications regarding the status of the product and its operations
- data about malfunctions of the product (eg. error codes)
- data about the components that are part of the product (eg. batteries)
- data generated or collected even when the user is not acting on the product, or while the product is in stand-by mode

Also metadata

The regulation also requires the sharing of all metadata necessary to make raw data understandable and usable, such as its structure, unit of measurement, context, meaning, and timestamp.

The Data Act emphasizes the importance of metadata in concretely helping users and third parties to harness raw data in order to drive innovation, develop digital and other services, and protect the environment and health. It also supports the circular economy and facilitates the maintenance and repair of connected products.

Examples of metadata

- information on data structures and formats,
- vocabularies,
- classification schemes,
- taxonomies and code lists, where available,
- clear and sufficient information relevant for the exercise of the user's rights on how the data may be stored, retrieved or accessed, including:
  - the terms of use and quality of service of application programming interfaces (APIs),
  - or, where applicable, the provision of software development kits.

REGULATORY REFERENCES

Recital 15

Data […] should be understood to cover data recorded intentionally or data which result indirectly from the user's action, such as data about the connected product's environment or interactions. This should include data on the use of a connected product generated by a user interface or via a related service, and should not be limited to the information that such use took place, but should include all data that the connected product generates as a result of such use, such as data generated automatically by sensors and data recorded by embedded applications, including applications indicating hardware status and malfunctions.

This should also include data generated […] 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 […] 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 include data collected from […] sensors for […] determining a physical quantity or quality or

the change in a physical quantity, such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed. […]

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. […]

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 […]

Recital 24

[…] This could include information on data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, as well as clear and sufficient information relevant for the exercise of the user's rights on how the data may be stored, retrieved or accessed, including the terms of use and quality of service of application programming interfaces or, where applicable, the provision of software development kits. […]

FAQ 4: "Which data are in scope?"

Factor	Explanation	Reference in the legal text
Product data	Data obtained, generated, or collected by a connected product and which relates to its performance, use or environment […]	Recital 15, Article 2(15)
Related service data	Data representing user action, inaction and events related to the connected product during the provision of a related service.	Recital 15 and 17, Article 2(16)
Readily available data	Product data and related service data that a data holder can obtain without disproportionate effort going beyond a simple operation […] Only data generated/collected after the entry into application of the Data Act should be considered as falling within the scope of Chapter II.	Recitals 20 and 21, Article 2(17)
Level of enrichment of the data	In scope: raw data and pre-processed data, accompanied by the necessary metadata to make it understandable and usable. For example, 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 a change in a physical quantity (e.g. temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration, or speed).	Recital 15

	Out of scope: highly enriched data, meaning inferred or derived data or data that result from additional investments (including by way of proprietary, complex algorithms). In addition, content that is often covered by intellectual property rights (e.g. textual, audio, or audiovisual content).	
Personal vs non-personal data	Users are entitled to access all data generated by the connected product or related service, whether personal or non-personal. However, personal data processing is governed by GDPR rules, so the user's rights provided by the Data Act have to be exercised in compliance with the GDPR. Users that are not data holders or data holders must have a valid legal basis under Article 6 of the GDPR for processing personal data. Question 26 examines in further detail non-personal data access, use and sharing.	Recitals 25 and 35
Trade secrets	The Data Act establishes a new mechanism to protect trade secrets. […] This mechanism is known as the 'trade secrets handbrake' and is explored further in Question 20.	Recital 31, Articles 4(6), 5(9)

FAQ 5: "What level of enrichment transforms raw and pre-processed data into inferred or derived data, excluding it from Chapter II?"

[…] To distinguish between raw and pre-processed data on the one hand, and derived or inferred data on the other, Recital 15 mentions notions such as "substantial modification", "substantial investments in cleaning and transforming the data", and "proprietary and complex algorithms". As explained in Recital 15, the data in scope - raw and pre-processed data - include measurements of a "physical quantity or quality" […]

Exceptions for security reasons

It is possible to exclude certain raw data from the scope of application if sharing them could undermine security requirements of the connected product resulting in a serious adverse effect on the health, safety or security of natural persons.

We recommend seeking legal advice on this matter.

Protection of trade secrets

In general, access to raw data that may contain trade secrets cannot be prevented. However, contractual clauses can impose restrictions on the use of certain raw data.

We recommend seeking legal advice on this matter.

Who are the users?

It is important to correctly identify who the users of your connected products are. They will indeed be the ones able to exercise the right to access raw data and share it with third parties.

REGULATORY REFERENCES

Article 2.12

'user' means 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;

Recital 18

The user of a connected product should be understood to be a natural or legal person, such as a business, a consumer or a public sector body, that owns a connected product, has received certain temporary rights, for example by means of a rental or lease agreement, to access or use data obtained from the connected product, or receives related services for the connected product. […]

An owner, renter or lessee should also be considered to be a user, including where several entities can be considered to be users […]

FAQ 14: "What are 'users'?"

[…] a 'user' is 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 a related service. This implies the user has a stable right on the connected product (e.g. ownership, or a right from a rent or lease contract). […]

FAQ 15: "Does the Data Act apply to users established outside the EU?"

According to Article 1(3)(b) of the Data Act, a user must be established in the EU. A user may request access to data on the basis of the Data Act, irrespective of whether the data are stored inside or outside the EU.

FAQ 16: "Can there be multiple users for a single connected product, and how should their access be governed?"

Various actors may have a legal right based on the contractual arrangements related to the use of a connected product. It is therefore entirely possible for multiple persons to be users of the same connected product. In such a situation, data holders should have mechanisms in place to ensure that each user can access the data to which they are entitled. Users might also conclude separate agreements (e.g. a user-to-user sub-lease of a connected product). […]

Technical implications

Now, let's move on to the areas where you need to implement new functions in your IoT system. These areas are:

1. sharing data with users
2. sharing data with third parties
3. collection of compensation from third parties

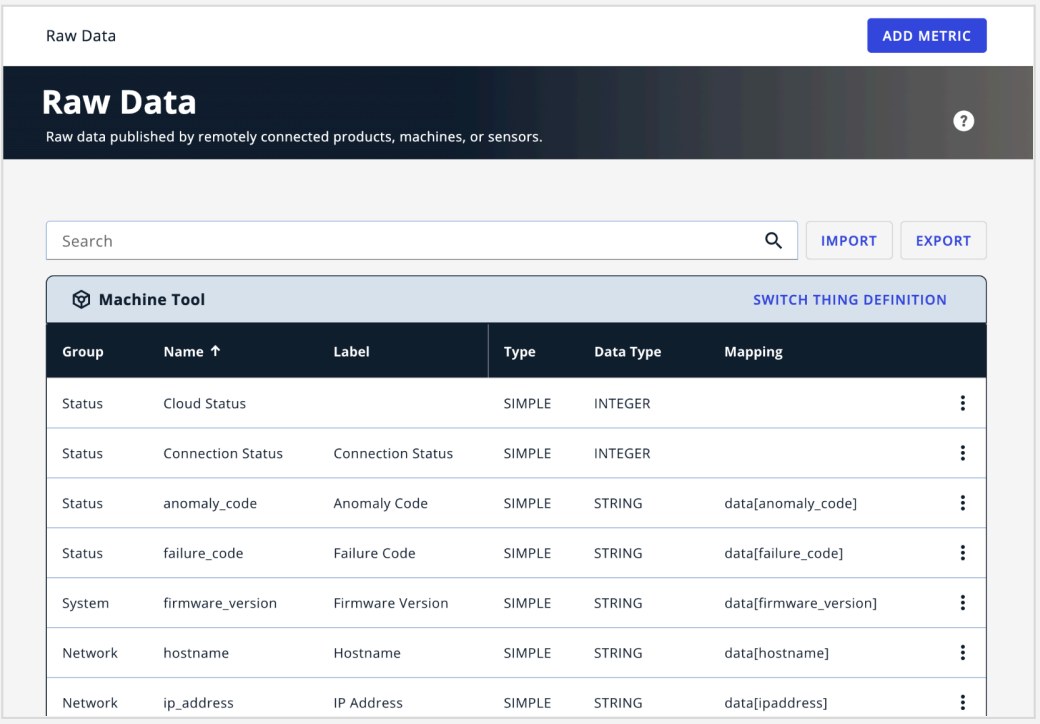
In the following paragraphs, we will address these three areas, providing all the regulatory references, useful information, and an implementation example with Servitly.

Basic functions

Before going into the details of the 3 areas, it is appropriate to establish a common foundation

Definition of "raw" metrics

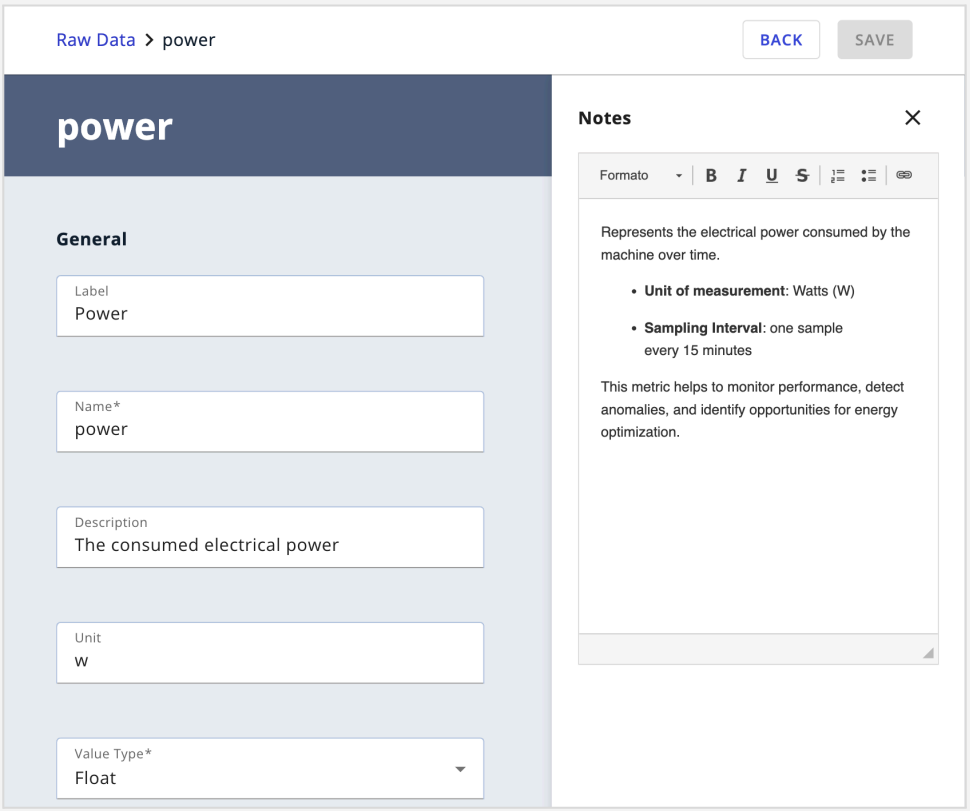
To facilitate the management of sharing functions, it is advisable to first identify and mark the metrics that generate raw data, that is, the only data that falls under the sharing obligation.



As a data holder you can define all the metrics you manage in your IoT system and mark which ones should be considered "raw" for the purposes of the Data Act. You can do this for each product model.

Metadata documentation

To fully comply with metadata publication requirements, it is advisable to add to the definition of the metrics that generate raw data all the documentation necessary to interpret the values correctly.



As a data holder, you can prepare and make available the documentation necessary for end users and third parties to interpret the data correctly.

Functions for sharing data with users

The regulation grants the user of a connected product the right to access raw data. This can be done in two ways:

1. Direct access: the user is technically able to get the raw data directly from the product
2. Indirect access: the user access data through sharing functions provided by the data holder

When direct access is unavailable, Article 4.1 requires data holders to provide indirect access by implementing data sharing functions.

REGULATORY REFERENCES

Article 4.1

Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. […]

FAQ 22a: "What technical and practical requirements must data holders meet concerning criteria such as data format, quality and latency?"

Data holders must meet several technical and practical requirements, including:

Format: […] Data holders, as the entities responsible for the design of the data at the source, must provide data in an interoperable format (e.g. XML, JSON, CSV). Formats subject to licensing constraints are not considered “commonly used”. While industry is encouraged to develop common formats for certain data, no obligation to develop those flows from the Data Act.

Quality: The data holder is required to share data “of the same quality” as it makes available to itself. This implies that the data should be shared in a format and quality consistent with how it would be shared with another subsidiary within the same corporate group or in a manner that aligns with industry standards or practices within a specific industry.

Timeliness: Articles 4(1) and 5(1) require data holders to provide data “without undue delay” upon user or third-party request. This means data should be made available in a prompt, timely and responsive manner. Data holders must proactively implement solutions such as automation, streamlined and structured request procedures, self-service portals, and clear organisation policies to minimise administrative bottlenecks and reduce reliance on manual intervention (c.f. Recital 21). Delays can be justified based on security, technical, or legal constraints, and must remain proportionate to the request.

Latency: The requirement to provide data “where relevant and technically feasible, continuously and in real-time” applies to scenarios where low latency is beneficial, such as IoT systems, connected mobility, and industrial monitoring. Unlike Article 20 GDPR, the Data Act ensures that access is not hindered by technical obstacles (c.f. Recital 35). Feasibility must therefore be assessed objectively, based on industry standards and best practices. Data holders should proactively implement solutions such as APIs (automated data retrieval) and event architectures (software design that trigger data updates) to ensure real-time or near instantaneous access wherever feasible.

```
Convenience: Data holders must grant access to data “easily”. This requires implementing
mechanisms that streamline and simplify data sharing and avoid unnecessary complexities or
barriers. Where access is limited to on-site or specific tools are required, it must not
involve unreasonable complications for users or third parties, such as restrictive locations,
time slots, or disproportionate costs.

Security: Data must be made available “securely”, ensuring protection against unauthorised
access or use. Such mechanisms should align with industry standards and relevant legal
frameworks, such as those related to cybersecurity.
```

Let's recap:

- raw data sharing with the user must be **free of charge**
- raw data must be provided to the user according to the following criteria:
  - **format**: in a comprehensive, structured, commonly used and machine-readable format, e.g. XML, JSON, CSV
  - **quality**: of the same quality as is available to the data holder; data should be shared in a format and quality consistent with how it would be shared with another subsidiary within the same corporate group or in a manner that aligns with industry standards or practices within a specific industry
  - **timeliness**: without undue delay; data should be made available in a prompt, timely and responsive manner; data holders must proactively implement solutions such as automation, streamlined and structured request procedures, self-service portals, and clear organisation policies to minimise administrative bottlenecks and reduce reliance on manual intervention
  - **latency:** continuously and in real-time, where relevant and technically feasible; this applies to scenarios where low latency is beneficial, such as IoT systems, connected mobility, and industrial monitoring; in such case data holders should proactively implement solutions such as APIs (automated data retrieval) and event architectures (software design that trigger data updates) to ensure real-time or near instantaneous access wherever feasible
  - **convenience**: data holders must grant access to data “easily”; this requires implementing mechanisms that streamline and simplify data sharing and avoid unnecessary complexities or barriers
  - **security**: data must be made available “securely”, ensuring protection against unauthorised access or use; such mechanisms should align with industry standards and relevant legal frameworks, such as those related to cybersecurity.
- the obligation also includes the relevant **metadata** necessary to interpret and use those data

Functions to be implemented

So, you need to implement the following functions:

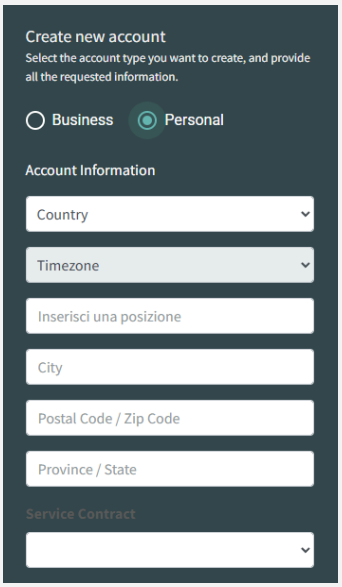
- user identification and management
- sharing data with users
- metadata publication

Let's see an implementation example.

User identification and management

As a data holder, you have probably already set up user management for your IoT system. However, the regulation may expand your user base to include previously unconsidered subjects.

This means that new user identification and management functions may be needed.



To access the raw data, the user must first self-register.

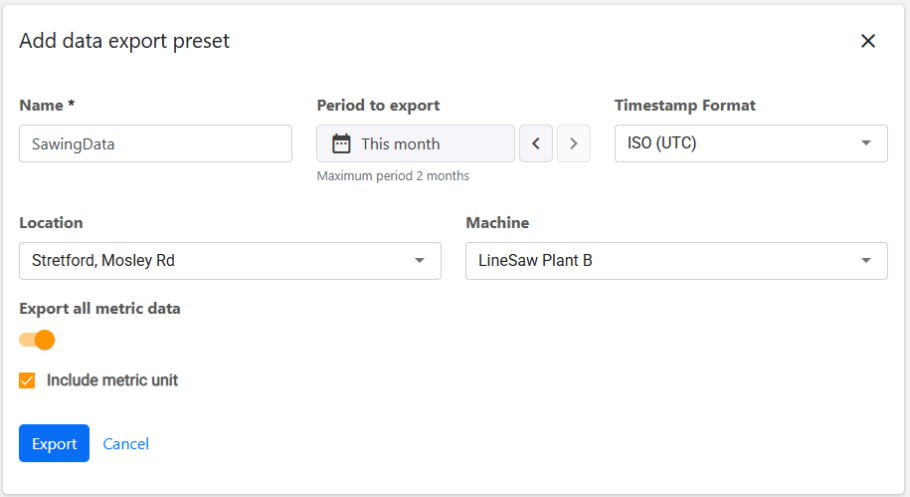
To share with users only the data relating to their products, it is necessary to identify the product for which they are requesting access. This can be done through a product identification code, such as the serial number.

The user must enter the serial number of the product from which they wish to obtain the raw data. Matching with the actual serial number is done by preloading available serial numbers or calling a provisioning API. The product model can be inferred from the serial number or entered by the user.

Sharing data with users

There are several ways to share data with users. One option is to provide a customizable data export function that returns a machine-readable file in a format such as CSV, XML or JSON.

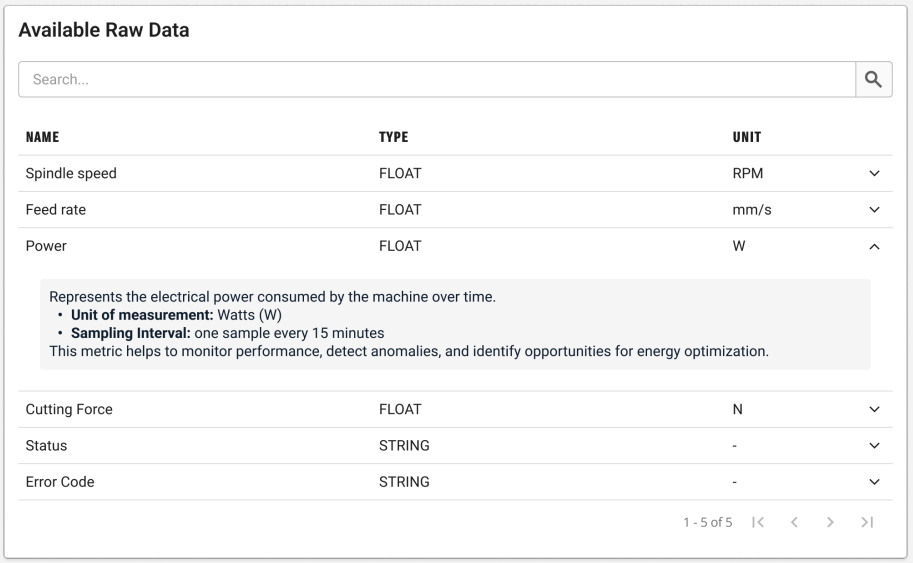
The maximum data retention period is established on the basis of the contract between the data holder and the user.



The user downloads the raw data in machine-readable format.

Metadata publication

Access to metadata can be done through online documentation available into your IoT system.



The user accesses the metadata documentation.

Functions for sharing data with third parties

The regulation requires the data holder to provide access to raw data to a third party, upon request by a user, or by a party acting on behalf of a user. This obligation applies even if the user can technically access the raw data directly.

This obligation involves the implementation of third-party management, request management and data sharing functions.

REGULATORY REFERENCES

Article 5.1

Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, 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. […]

FAQ 22a: "What technical and practical requirements must data holders meet concerning criteria such as data format, quality and latency?"

See page 16

FAQ 31: "Does a data holder still need to share data with a third party upon request of the user where it has granted direct access to the user?"

Yes. Users also have a right under Article 5 of the Data Act to request the data holder to transfer data to a third party when the user has direct access to the data in the sense of Article 3(1). This pre-supposes that there is a data holder with data readily available to them. Article 5 is not conditional upon the type of access that the user has.

FAQ 37: "Can someone established in a third country receive data on the basis of the data-sharing obligations under Chapter II?"

No. The scope of the Chapter II data-sharing obligation on data holders is limited to entities and persons, including consumers, in the Union (cf. Articles 1(3)(b), 1(3)(d) and 2(14) of the Data Act).

Giving data access to operators that do not have a presence in the EU cannot be justified based on the Data Act […] A user may ask a data holder to share data with an entity or person that is not established in the EU, but the data holder is not obliged to grant that access.

Let's recap:

- upon request by a user (or by a party acting on behalf of a user) the data holder must make the raw data available to a third party
- raw data sharing with the third party must be **free of charge for the user**

- raw data must be made available to the third party according to the same criteria of **format**, **quality**, **timeliness**, **latency**, **convenience** and **security** defined for users (see page 17)
- the obligation also includes the relevant **metadata** necessary to interpret and use those data
- the obligation applies even if the user can technically access the raw data directly
- the obligation only exists if the third party is based in the EU

Functions to be implemented

So, you need to implement the following functions:

- third-party registration and approval workflow management
- management of user requests to share raw data with a third party
- sharing data with third parties

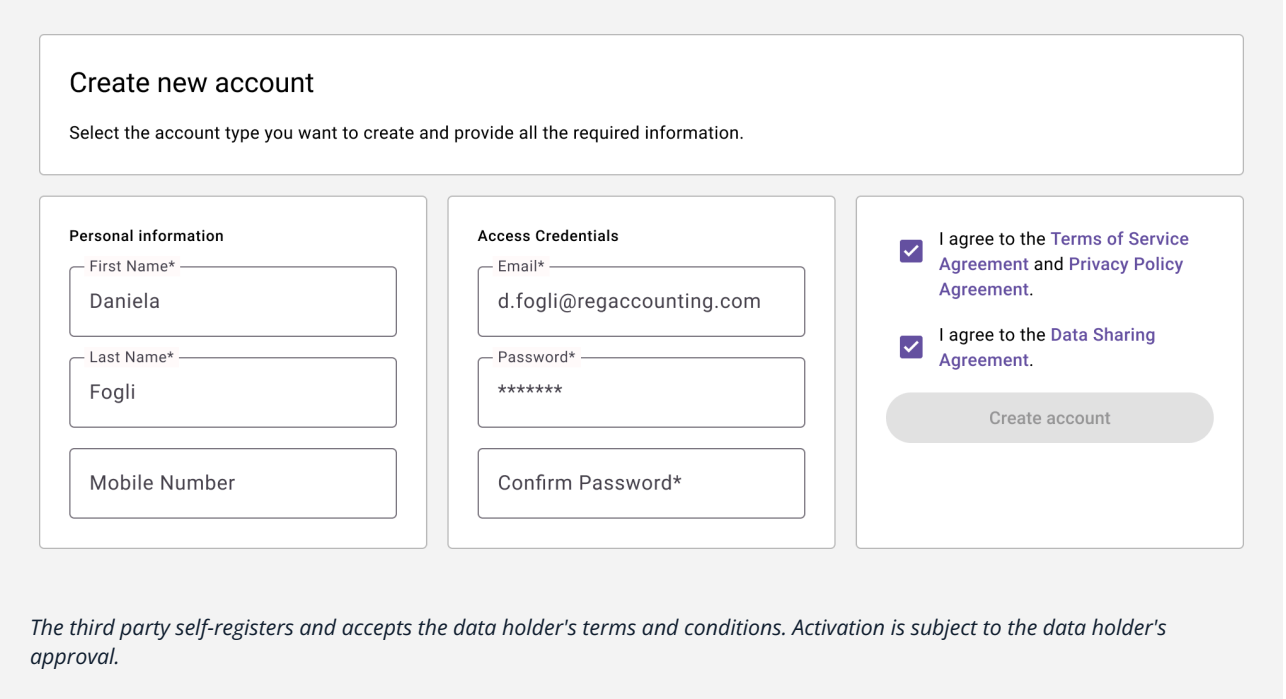
Let's see an implementation example.

Third-party registration and approval workflow management

'Third parties' are probably a new type of entity that is not currently managed by your corporate information system. You should therefore first implement basic third-party data management functions.

To streamline the registration process and given that you won't know who the third parties are in advance, it would be helpful to provide a self-registration function that requires acceptance of your terms and conditions.

Finally, you may find a third-party final approval function useful. This will be carried out by your staff, who will verify the data entered and ensure the third party's legal status (for example, whether it is based in the EU).

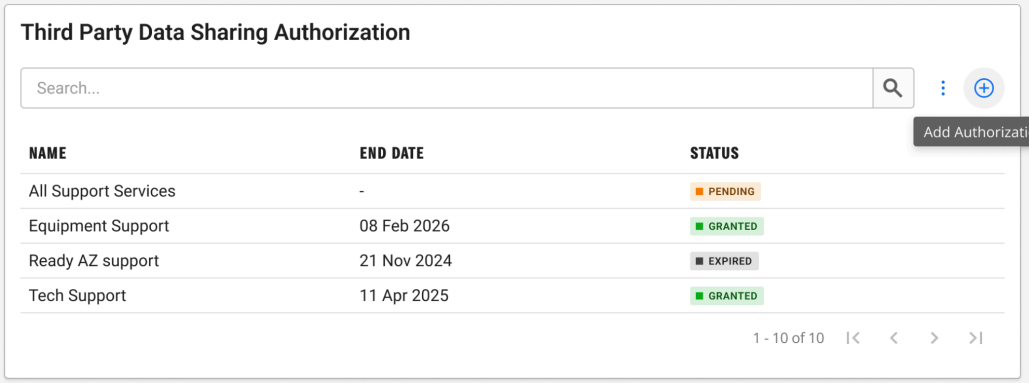


The third party self-registers and accepts the data holder's terms and conditions. Activation is subject to the data holder's approval.

Management of user requests to share raw data with a third party

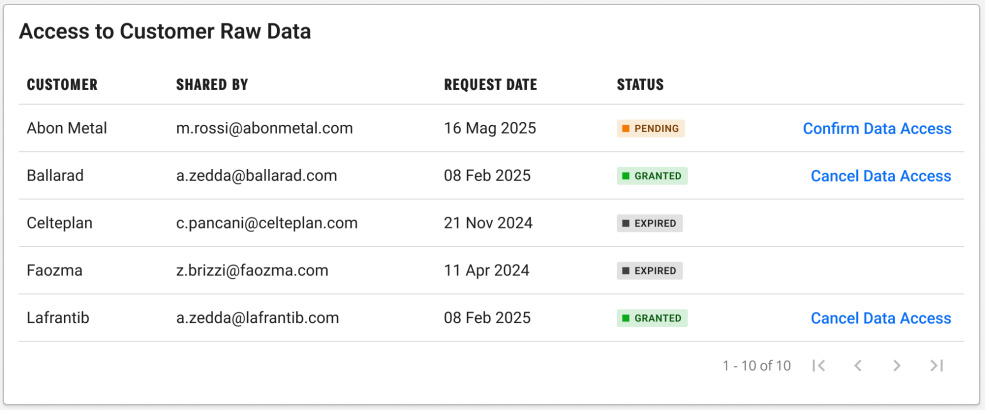
To allow users to easily exercise their right to share data with a third party, it may be useful to implement a structured flow like this:

1. the user access the list of approved third parties in your IoT system
2. if the third party with whom they want to share data is not present on the list, they will invite the third party to self-register on your IoT system.
3. the user identifies the third party in the list and sends a sharing request.
4. the user may indicate an expiry date
5. the third party receives the sharing request sent by the user and confirms it.



The user adds the authorization to share data with the chosen third party. This authorization must be confirmed by the third party.

The third party must have an overview of the status of data sharing authorizations and the related confirmations.

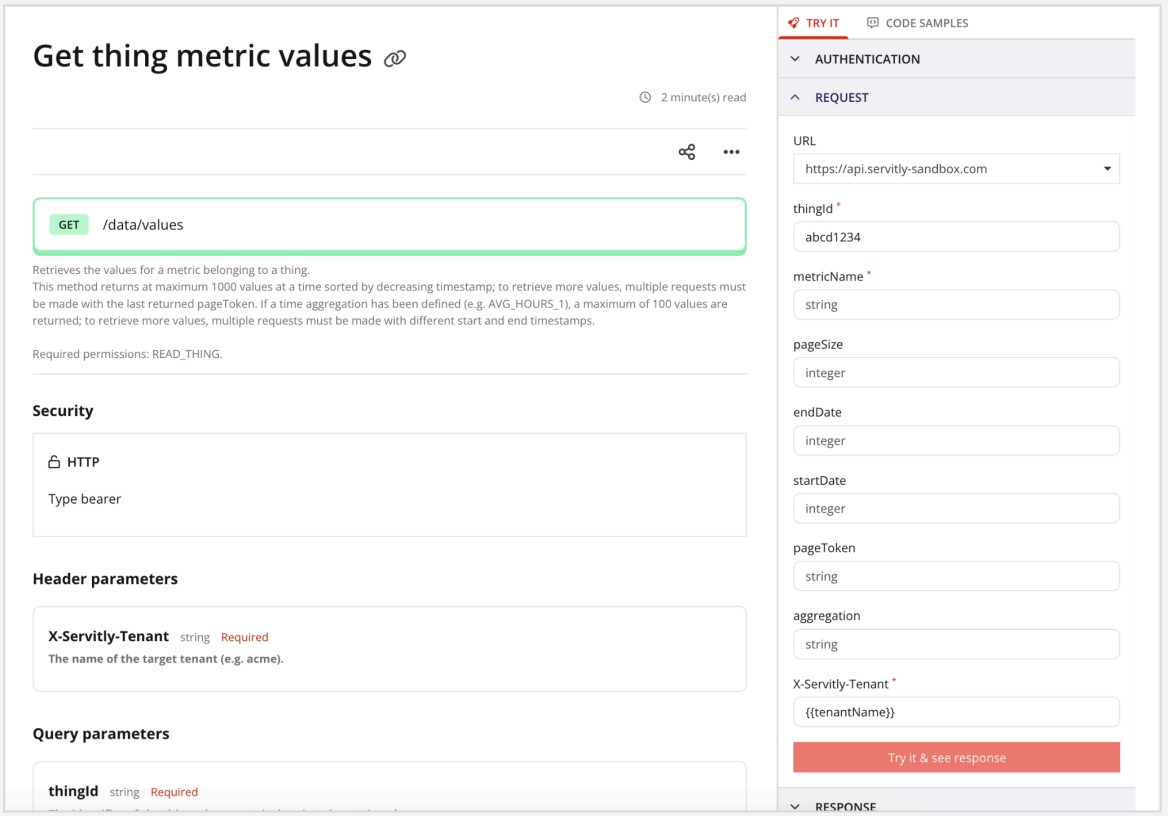


The third party receives the request and confirms it.

Sharing data with third parties

The most effective way to share raw data with third parties is through APIs.

For ease of management, it's a good idea to give each third party a single API access key and manage authorization for accessing raw user and product data internally within the IoT system.



Third parties access the raw data via APIs. APIs are automatically restricted to allow access only based on authorizations.

Functions for collecting compensation from third parties

The regulation allows data holders to request compensation from third parties with whom they are obliged to share data. A suitable way to do this is through subscriptions.

Therefore you need subscription and payment management functions.

REGULATORY REFERENCES

Article 9

1. Any compensation agreed upon between a data holder and a data recipient for making data available in business-to-business relations shall be non- discriminatory and reasonable and may include a margin.
2. When agreeing on any compensation, the data holder and the data recipient shall take into account in particular:
    a. costs incurred in making the data available, including, in particular, the costs necessary for the formatting of data, dissemination via electronic means and storage;
    b. investments in the collection and production of data, where applicable, taking into account whether other parties contributed to obtaining, generating or collecting the data in question.
3. The compensation referred to in paragraph 1 may also depend on the volume, format and nature of the data.
4. Where the data recipient is an SME or a not-for-profit research organisation and where such a data recipient does not have partner enterprises or linked enterprises that do not qualify as SMEs, any compensation agreed shall not exceed the costs referred to in paragraph 2, point (a).

Recital 46

[…] this Regulation contains the principle that in business-to-business relations data holders may request reasonable compensation when obliged […] to make data available to a data recipient. Such compensation should not be understood to constitute payment for the data itself.[…]

Recital 47

[…] reasonable compensation […] may include compensation for the costs incurred in making the data available. Those costs may be technical costs, such as the costs necessary for data reproduction, dissemination via electronic means and storage, but not for data collection or production. Such technical costs may also include the costs for processing, necessary to make data available, including costs associated with the formatting of data. Costs related to making the data available may also include the costs of facilitating concrete data sharing requests. They may also vary depending on the volume of the data as well as the arrangements taken for making the data available. Long-term arrangements between data holders and data recipients, for instance via a subscription model or the use of smart contracts, may reduce the costs in regular or repetitive transactions in a business relationship.[…] Second, reasonable compensation may also include a margin, except regarding SMEs and not-for-profit research organisations. A margin may vary depending on factors related to the data itself, such as volume, format or nature of the data. It may consider the costs for collecting the data. […]

Let's recap:

- the data holder may ask for compensation for sharing data with third parties
- in case the third party is an SME or a non-profit research organisation the compensation must not exceed the costs incurred in making the data available.
- in other cases the compensation may include a margin
- the amount of compensation may vary depending on the volume, format and nature of the data
- in the case of long-term agreements it is possible to establish subscription models

Functions to be implemented

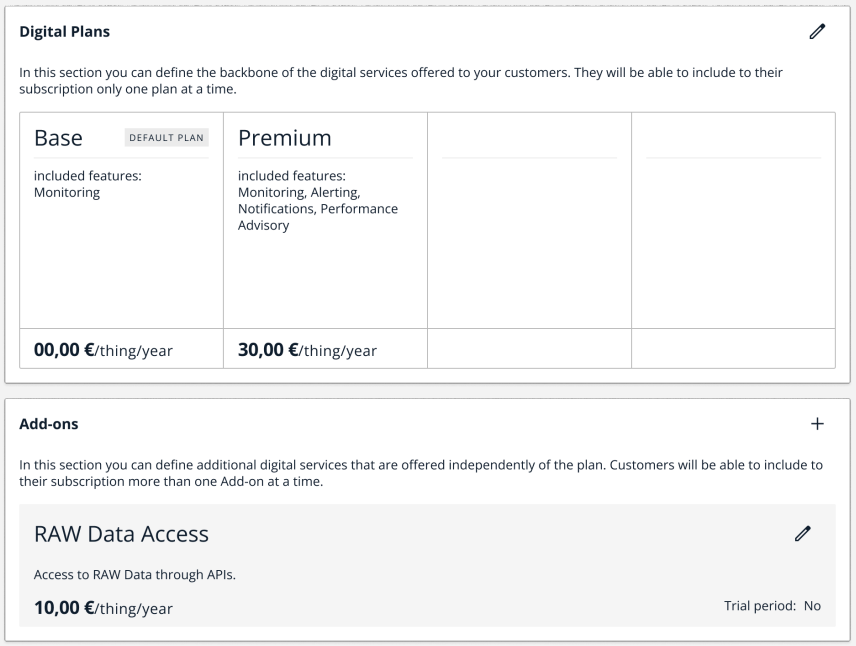
So, you need to implement the following functions:

- subscription plan management
- compensation calculation
- payment collection management

Let's see an implementation example.

Subscription plan management

An appropriate way to obtain compensation from third parties is through subscriptions. In doing so, you will need to define different plans. In fact, compensation must be differentiated according to the size of the third party (SME and Large Enterprise). Furthermore, the regulation allows to define variable compensation based on the volume, format, and nature of the shared data.



As a data holder, you can define different subscription plans for third parties.

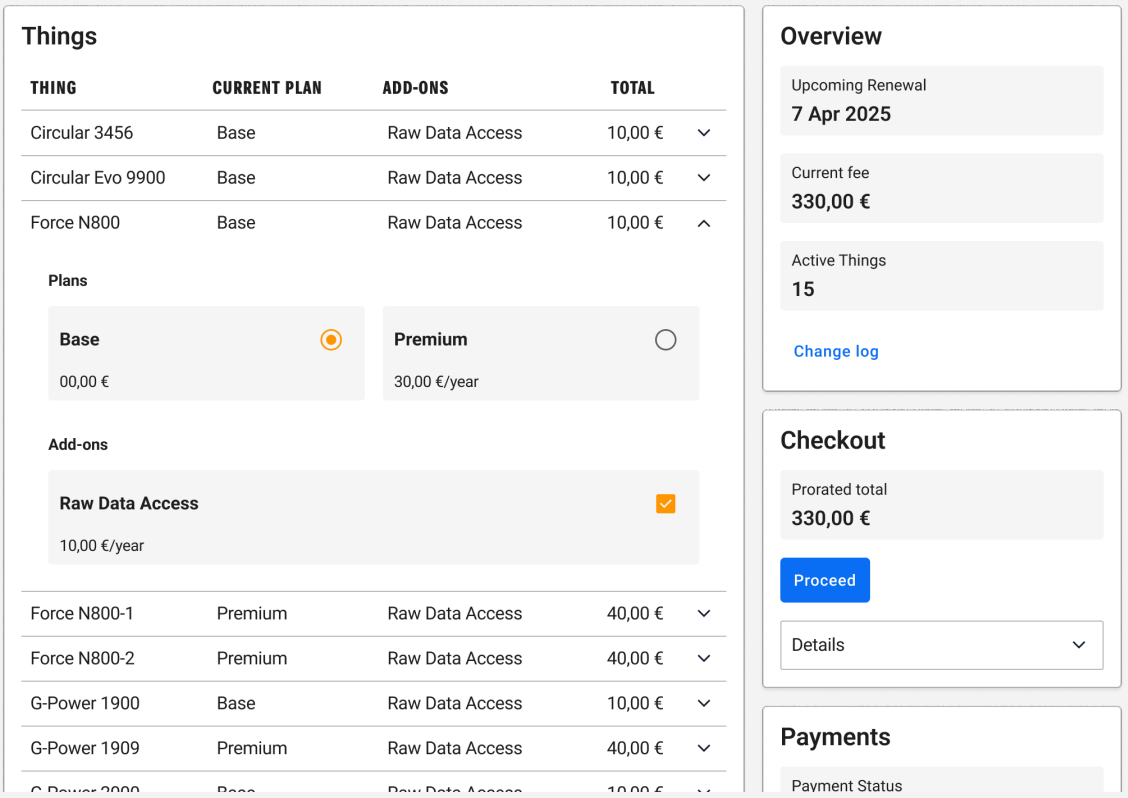
Compensation calculation management

It's possible that multiple users will want to share data with the same third party over time. In this case, the compensation the third party will have to pay you will vary over time, depending on the number of users and products they access.

Therefore, you will need to calculate periodically, for example on a monthly basis, the compensation that the third party will have to pay based on the number of products they access and the subscription plans associated with them.

Payment collection management

If the number of third parties and authorizations starts to grow, you will probably also need a system that automatically manages payments.



The third party pays for the additional user within their subscription. Payment is handled through Stripe, which allows for various payment methods, including credit cards.

What to do now

If you wish to implement these functions by yourself, you can share this document with your development team and use it as a foundation for defining technical specifications and your evolutionary project.

If instead you want to evaluate an alternative approach to 'make', you can contact us at: contact@servitly.com

We will show you how Servitly can be an effective Data Act compliance solution perfectly integrated with your IoT system.