FOODITY

FOODITY dataU Guide

JIBE

A GDPR-compliant consent management platform

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement nº 101086105. This document reflects only the author's view, and the EU Commission is not responsible for any use that may be made of the information it contains.

Contents

1. What is dataU?

The vision behind the platform

DataU is a decentralised, GDPR-compliant data-sharing platform designed to empower individuals and organisations to securely manage and share personal data. Unlike traditional data-sharing systems that rely on centralised storage and oversight, DataU operates as a peer-to-peer (P2P) network, ensuring that data sovereignty, privacy, and security remain in the hands of the data subject (the citizen or entity that owns the data).

The core vision of DataU is to redefine data ownership by ensuring that individuals retain full control over their personal data while allowing organisations to access and utilise this data in a transparent, ethical, and consent-driven manner.

The platform is built to support the principles of data minimisation and sovereignty, meaning that:

- No personal data is stored or controlled by dataU itself — data remains with the processors who collect it.
- Consent is explicit, dynamic, and revocable, ensuring compliance with GDPR and the EU's ethical standards for data usage.
- All actions related to data permissions are recorded on a blockchain, creating an immutable and verifiable audit trail.

To make all of this work in a decentralised and user-centric way, the platform relies on four core components:

1. **dashboardU** - This is the user interface for data subjects (citizens or organisations), where they can view and manage the consent they've given to different services; see exactly which data they've shared, with whom, and for what purpose; and revoke consent at any time.

2. **nodeU** - This is the backbone of the decentralised network. Each nodeU registers consent from users; validates permissions between data subjects and processors; ensures these permissions are stored immutably on the blockchain; and is deployed by participants in the network, making it fully distributed.

3. **proxyU** - This secure connector lives on the data processor's premises (e.g. an app or web service). It handles encrypted peer-to-peer data transfers; authenticates with nodeU to verify consent before any data exchange; and establishes a secure tunnel

with another proxyU to deliver the data.

4. **Integration Layers (SDK & APIs)** - Developers can use the DataU SDK to design data request forms; connect their apps to the network through proxyU; and integrate GDPR-compliant consent flows directly into their user experience.

This architecture ensures that the **user remains in charge** and that data processors — whether they're startups, public institutions, or research projects — operate with transparency and accountability from the very first connection.

More information on their stakeholders and their benefits is below in *Chapter 2: Who is it for?*

2. Who is it for?

The stakeholders

DataU is designed with the *people* in mind. The everyday citizens who generate data simply by living their lives, whether they're logging their meals in a health app, scanning loyalty cards at the supermarket, or using digital services that touch on food, health, and lifestyle.

In the dataU ecosystem, these individuals are known as **data subjects**, and they are the true *owners* of their personal data. DataU's role is to empower them to make informed decisions about what data they'd like to share, as well as provide them with an easy to access overview of all the apps that currently have access to their data, to minimise any risks of unauthorised companies still receiving personal information long after the users have stopped interacting with their service.

With that being said, the platform has the capacity to serve a wide variety of stakeholders, spanning across public, private, and governmental sectors, each playing a distinct role in the data-sharing chain. Here's who benefits from DataU and how:

A. Citizens

The data subjects

These are the primary data owners. The platform ensures they remain in full control of their personal information. Whether it's identity data, dietary habits, lifestyle preferences, or other personal information, citizens can decide *who* accesses their data, *when*, *why*, and *for how long*. And crucially, they can **revoke that access at any time**, in line with GDPR's strict requirements.

In the FOODITY context, this means a citizen might use a nutrition app or a shopping app and decide to share select data points with services that help them eat better, live healthier, or contribute to more sustainable food systems — **but only when they choose to do so**.

B. Companies

As data subjects or data processors

In DataU, companies can be both data subjects and data processors, depending on the use case:

- **As data subjects**: Businesses can be the owners of sensitive operational data, like supply chain details, proprietary recipes, or customer insights. When they choose to share this kind of information (for instance, with a partner in a joint project), dataU allows them to do so *securely* and *with full traceability*, under a formal agreement such as a Non-Disclosure Agreement (NDA).

- **As data processors**: Companies may also be service providers or application developers who collect, use, and process data, either from citizens or other companies. In this role, they must ensure they handle data *ethically*, *securely*, and *transparently*. DataU helps them achieve this by automating GDPR-compliant consent collection and providing a secure channel for peer-to-peer data sharing.

For instance, a startup in the FOODITY pilot might receive permission from users to analyse their eating habits for a personalised nutrition service. Thanks to dataU, this consent is logged immutably on a blockchain, ensuring trust, transparency, and traceability. To read more about the FOODITY innovators, please proceed to page ...

C. Governments

As data processors

DataU was originally conceptualised in a government context during the POSEIDON project, where the Italian Ministry of Finance explored ways to allow citizens to share personal data with public services *without compromising privacy*.

That work laid the groundwork for DataU's B2G (Business-to-Government) capabilities. In this context, public authorities — such as ministries, regulatory bodies, or local governments — act as data processors. They can request access to citizen data (say, for policy development or public health monitoring), but only with informed and revocable consent.

This model opens the door to powerful citizen-centred public services that are also ethically sound and legally compliant.

3. How to use it?

The user-facing dashboard (for the data subject)

DataU puts you in full control of your personal data. Here's how to register and start managing your data-sharing permissions in just a few steps.

Step 1: Register for an Account

Visit the DataU Pilot registration page.

You'll need to provide:

- **First name**
- **Last name**
- **Email**
- **Username**
- **Password** (and confirmation)

Once your account is created, you can log in to access your personal dashboard. (see figure 1)

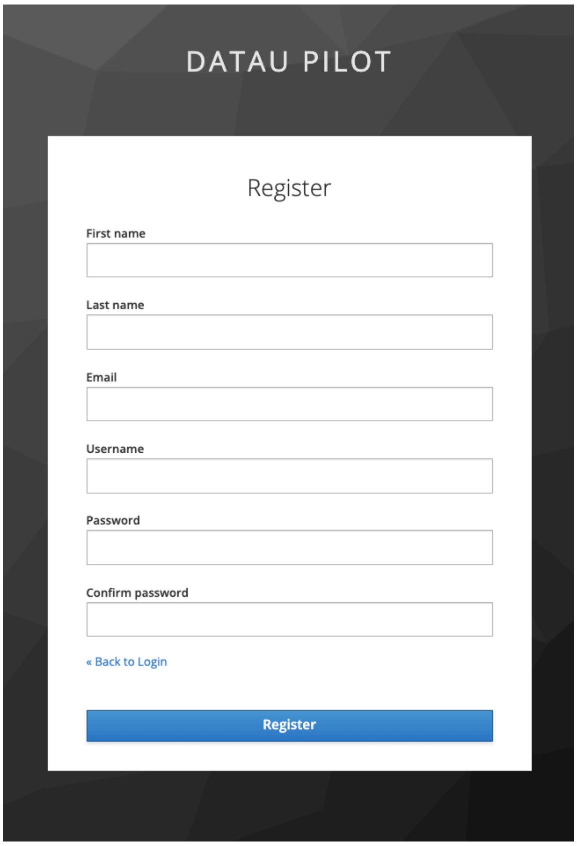
Step 2: Consent to Share or Decline

When a service requests access to your personal data, you are presented with a screen of the exact data that is being requested. (Figure 2)

You have three clear options:

- **Continue** – Grant access
- **Edit** – Make changes to the shared info
- **Decline** – Refuse access entirely

This ensures that **you're always in control**, and consent is specific, informed, and revocable, in alignment with GDPR.



DATAU PILOT

Register

First name

Last name

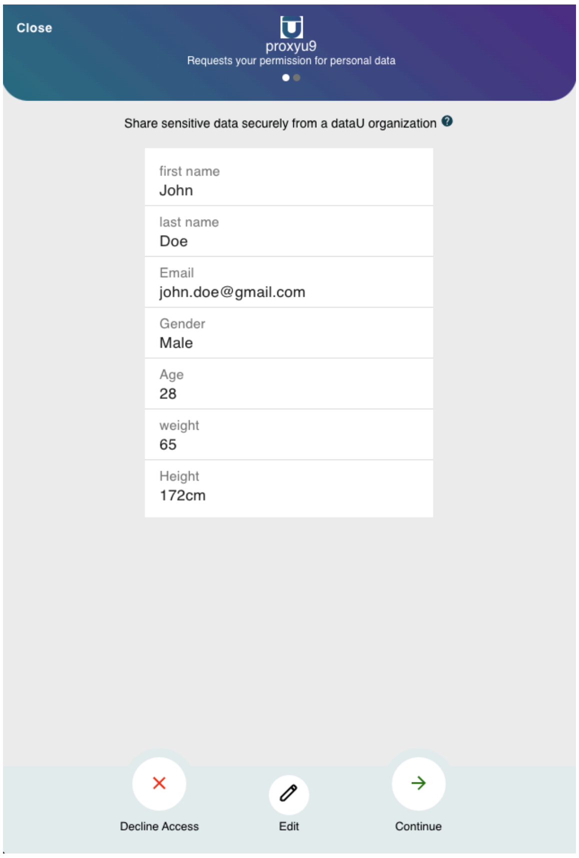
Email

Username

Password

Confirm password

Figure 1: Registration page



proxyu9

Requests your permission for personal data

Share sensitive data securely from a dataU organization

first name
John

last name
Doe

Email
john.doe@gmail.com

Gender
Male

Age
28

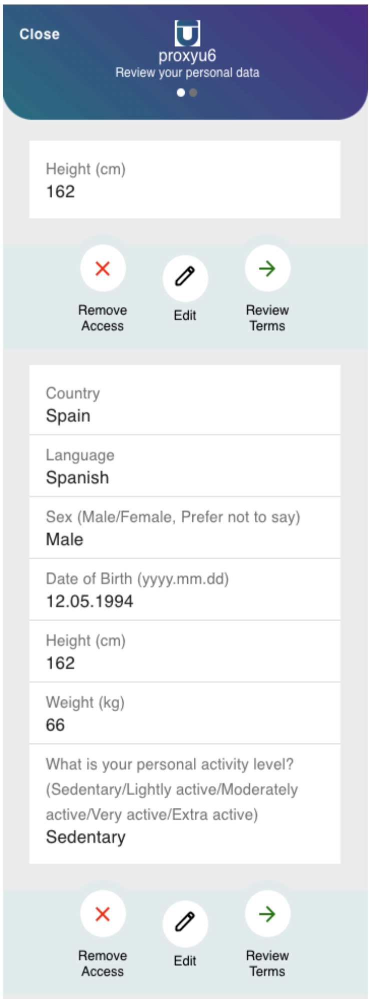
weight
65

Height
172cm

Figure 2: Data request

Step 3: Review Terms Before Sharing

When you click "Continue," you are presented with an overview of the approved data (Figure 3) and directed to the **Terms and Conditions** screen, where you are informed of what you are consenting to. (Figure 4)



Height (cm)
162

Country
Spain

Language
Spanish

Sex (Male/Female, Prefer not to say)
Male

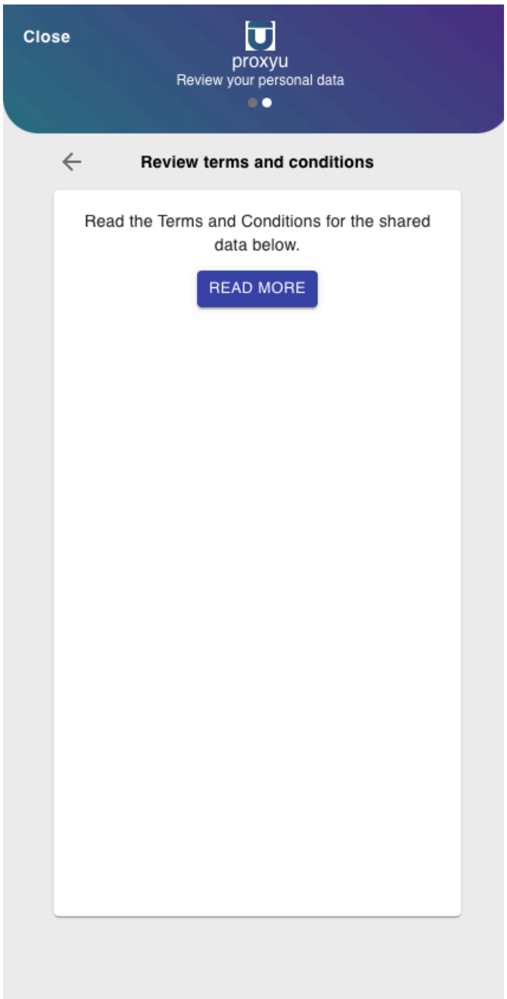
Date of Birth (yyyy.mm.dd)
12.05.1994

Height (cm)
162

Weight (kg)
66

What is your personal activity level? (Sedentary/Lightly active/Moderately active/Very active/Extra active)
Sedentary

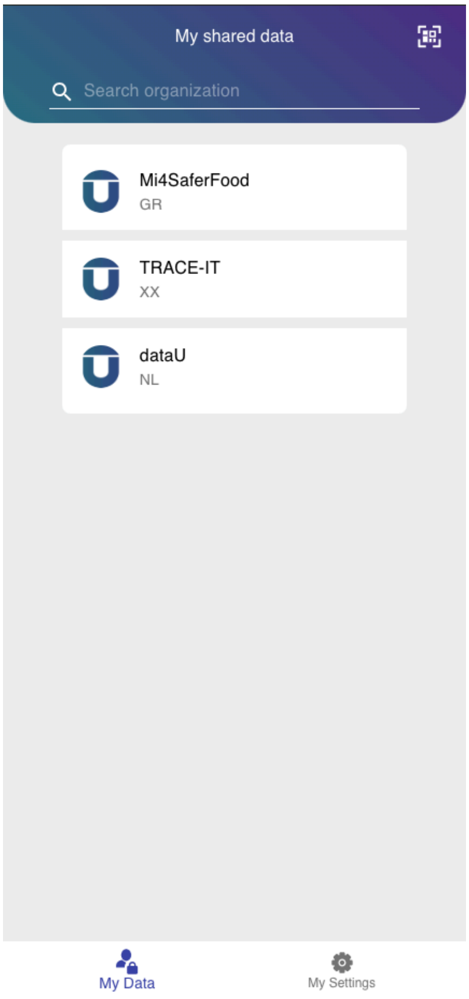
Figure 3: Approve data



Review terms and conditions

Read the Terms and Conditions for the shared data below.

Figure 4: Review T&C



Mi4SaferFood
GR

TRACE-IT
XX

dataU
NL

Figure 5: Review services

Step 4: Track What You’ve Shared

Once you’ve started using DataU, your dashboard helps you stay on top of what you’ve shared and with whom.

In the **“My Data”** tab *(figure 5)*, you can:

- See which organisations currently have access
- View, manage, or revoke consent
- Search through your data permissions

For data processors, there is no UI available; instead, a backend is provided, which is detailed below in the next point.

4. How to connect to it?

The guide (for developers and data processors)

If you're developing a digital service that collects, uses, or shares personal or sensitive data, you can refer to this section as your technical onboarding point.

Here's how to connect your service to the DataU infrastructure.

Step 1: Get Started with the DataU SDK

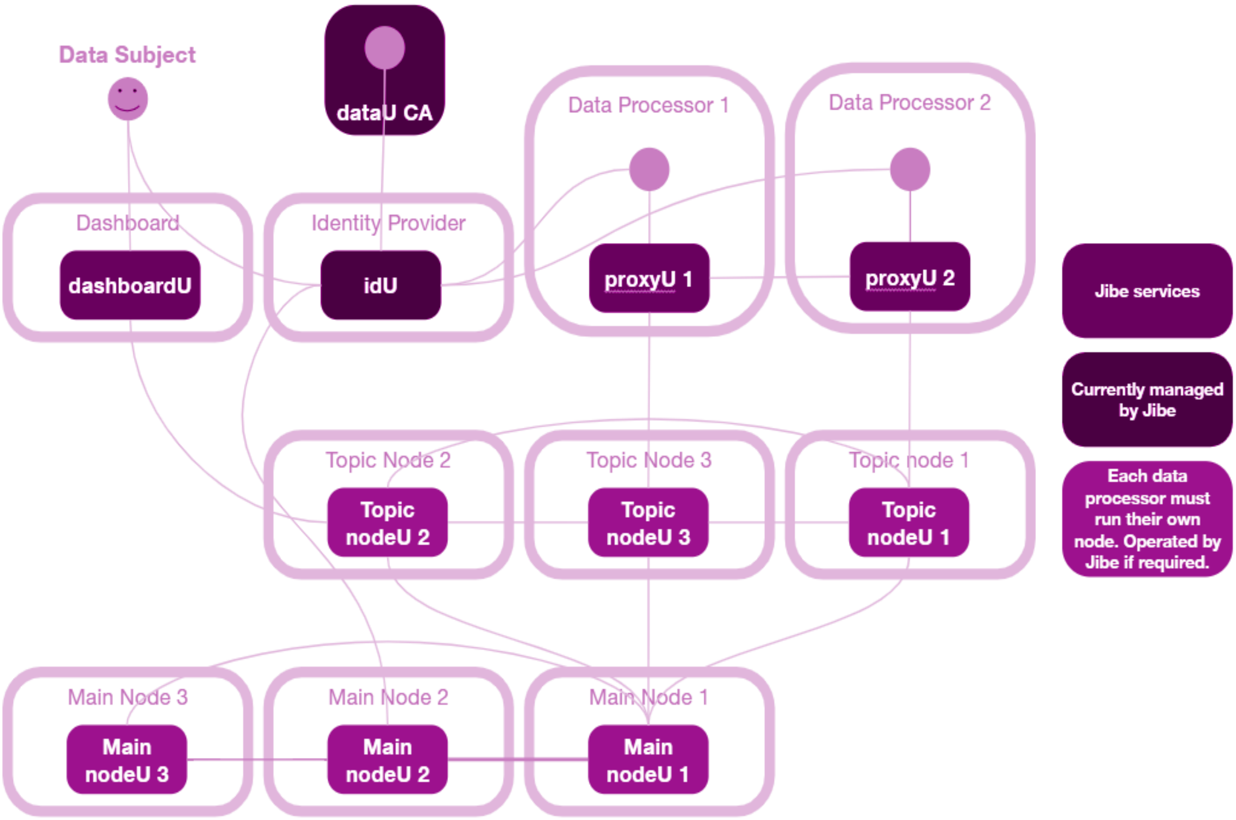
The **DataU SDK** (Software Development Kit) is the entry point for integrating your application or digital service with the DataU platform. It is a set of tools, libraries, and documentation that allows developers to:

- Connect to the decentralised DataU network
- Design and register custom data request forms
- Implement consent-based data access workflows
- Handle secure peer-to-peer (P2P) data transport
- Comply with GDPR standards using built-in protocols

The SDK includes:

- **API Documentation**: gRPC-based endpoints to integrate with nodeU and proxyU
- **Form Templates**: For requesting specific datasets from users
- **Sample Consent Flows**: Predefined interfaces for requesting and managing consent
- **ProxyU Setup Guide**: Instructions for installing and configuring the data tunnel
- **NodeU Integration Snippets**: Registering permissions and verifying consent on-chain
- **Test Environment Credentials**: For sandbox deployment and validation

In the following schematic, we've illustrated how the system components interact:



The diagram outlines how data processors connect via proxyU, how data subjects give consent through dashboardU, the interaction between the decentralised nodes (nodeU, topicNode, mainNode) and how P2P data flow is triggered securely based on blockchain-recorded permissions.

By using the SDK, you don't need to build your own consent system or reinvent GDPR compliance. DataU handles immutable consent logging via blockchain, revocation logic, data minimisation, and time-limited access, as well as encryption and identity validation.

Step 2: Set Up Your ProxyU

The **proxyU** component is the secure channel through which your application will exchange data with another node in the DataU network. It runs locally on your server and:

- Verifies consent through the **nodeU** network
- Establishes encrypted peer-to-peer tunnels with other proxyU nodes
- Handles data transport (but **not** storage)

Think of proxyU as your application's secure passport into the decentralised DataU ecosystem.

Step 3: Integrate the Consent Flow

DataU provides a plug-in UI component for end users to review and approve any data sharing request, which is illustrated in Chapter 3. How to use it?

To connect this UI to your service:

- Use the **gRPC API** endpoints documented in the SDK
- Pass consent requests through your proxyU instance
- Await user confirmation before accessing any personal data

Step 4: Dashboard Customisation (Optional)

If you're building your own front-end, the **Dashboard Development Kit (DDK)** allows you to customise the consent and settings dashboards. With it, you can:

- Embed user dashboards directly in your app
- Tailor message flows and data displays
- Align the visuals with your app's design system

Step 5: Testing & Going Live

Before connecting to the production network, you'll first be onboarded into a **staging environment**. Here, you can test:

- Permission workflows
- Data requests
- Error handling and consent revocation

Once verified, your app can go live with full blockchain-backed traceability and GDPR compliance.

Example Integration Scenario

Let's say your service helps users track their carbon impact based on grocery purchases. With DataU:

1. Your app registers as a **data processor**.
2. A citizen logs in via their DataU dashboard.
3. Your app requests permission to access grocery data.
4. The user reviews and approves the request.
5. Data is shared securely, and the action is recorded immutably via blockchain.

For more details on the technical aspects of the dataU platform, you are welcome to review the following folder, which contains additional instructions. Please also contact Jibe for more information. Contact details are available in section 6.

5. How is it currently being used?

Use cases from the 12 FOODITY Innovators

As part of the FOODITY project, 12 projects were selected through two open calls to develop digital solutions that make food systems healthier, more sustainable, and more citizen-centric.

DataU was used in both B2C (Business-to-Consumer/Citizen) and B2B (Business-to-Business) contexts, handling consent in various use cases, such as food and nutrition recommendation apps that suggest recipes or provide ratings of grocery products, for instance, to optimise the impact on consumers and the planet alike. Several apps were also developed to specifically support cancer patients during their ongoing battles, where access to doctors and recommendations is pivotal, and the data shared is highly sensitive.

In B2B aspects, the FOODITY innovators also brought solutions to optimise supply chains, digitalise the traceability of international logistics from farm to retailer, and reduce food waste in public canteens. Technological advancements were also made in spoilage detection, both at home and during food transportation, using smart sensors and AI-driven tools.

This showcases the platform's flexibility in supporting different scenarios and facilitating the safe transport of personal and company data. For more details on the Open Call projects, please refer to their relevant sections on the FOODITY website.

6. How to contact the dataU team?

For any additional details and further interest

Whether you're a developer, a policy-maker, a researcher, or just curious about ethical data-sharing, the dataU team is here to help and answer questions, provide guidance, and explore how dataU can support your project or organisation's needs.

dataU is developed by Jibe Company, a Netherlands-based software company with a technical branch in Romania. Jibe specialises in secure, decentralised data technologies and has been actively involved in EU-funded projects promoting citizen data sovereignty.

To get in touch with the dataU support team, you can reach out to us via email at:

datau.support@jibecompany.com

We're available for:

- Technical support with integration
- Guidance on using the dashboard and SDK tools
- Questions about data protection, GDPR compliance, or consent flows
- Exploratory conversations about new use cases or partnerships

For more information about the company behind dataU, please visit:

www.jibe.company

Or connect with us on LinkedIn:

linkedin.com/company/jibecompany