
Bubl Cloud
Access, management and monitoring
bubl cloud

Inhoud

Introduction

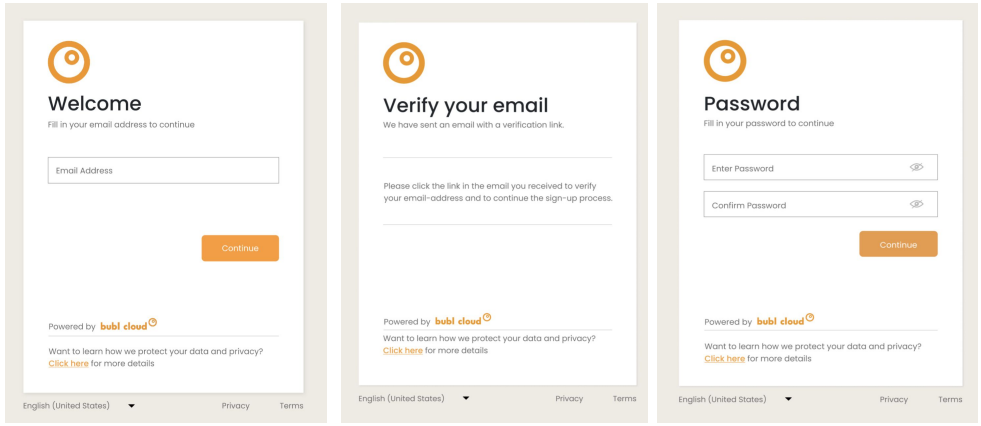
Bubl Cloud's vision is that privacy and security should be accessible and understandable for everyone at all times. If this is not the case, it misses its purpose and has no added value.

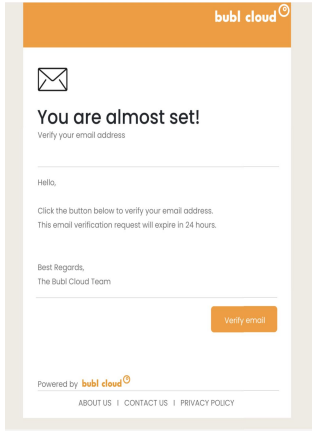
To achieve this, Bubl Cloud has developed a method that keeps things as simple as possible for most users, while enabling detailed control for expert users. This vision and method are applied to all components of the Bubl platform. From granting and managing rights, to providing insights into data sharing, to delivering a natural way of logging in.

bubl cloud

Access

First time login





Steps

1. The user enters an email address on the login screen in the "look and feel" of the service provider.
2. The user receives a verification email which he/she confirms. The user is automatically redirected to his/her newly created Bubl.
3. The user enters his/her password. The password component runs within the Bubl at this point, so the providing service can never see it.
4. The application is started

Simplicity where possible

If the user uses a service running on the Bubl platform for the first time and therefore has no other applications running in their Bubl yet, then the login procedure and access rights requests will be much simpler. After all, there is no danger yet of data sharing to other services.

Look & Feel

To give users the "look and feel" of a specific service, Bubl Cloud has developed a login framework where the layout and appearance of the login screen looks entirely like the design of the service. This gives Bubl Cloud users extra confidence and allows the service to continue profiling itself as itself. The user then transitions "seamlessly" from the service's website into their own Bubl.

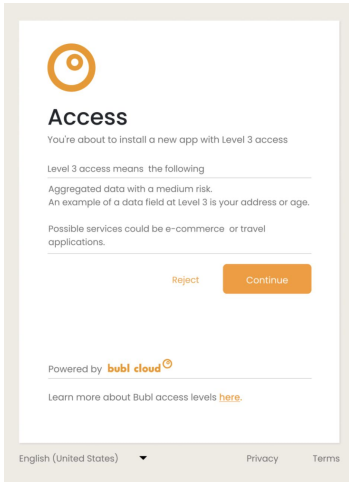
Access

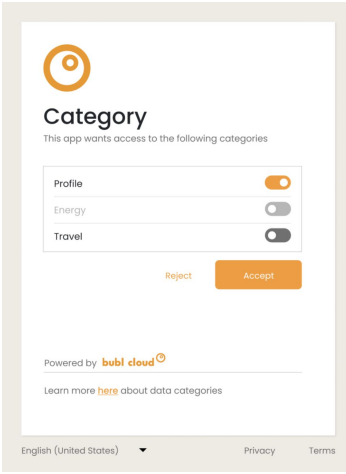
Login with multiple services already active

Extra questions when needed

If the user already has applications running on his/her Bubl, then the user will be asked 2 additional questions to give permission to activate the new application.

- Access level
- Category





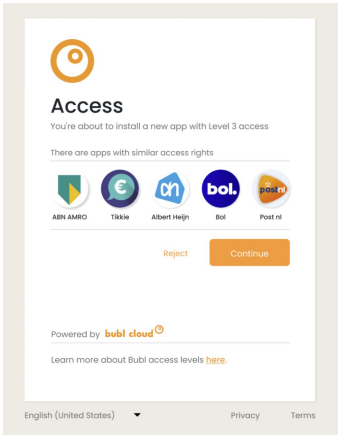
Goedkeuren

De gebruiker zal ook gevraagd worden de categorieën goed te keuren en/of uit te zetten.

Hierbij kan het zijn dat de ontwikkelaar van de applicatie sommige categorieën als benodigd aangeeft voor een goede werking van de applicatie. Deze zullen dan licht grijs aangegeven worden en niet aan te passen zijn.

Less than five

If the user has less than 5 applications running with the same access level as the newly requested application, then a screen will appear with explanation about the access level and permission will be requested.



More than five

If the user has five or more applications running with the same access level, then the screen will show some of these applications to give the user a faster indication of what the access level entails. This is to facilitate and speed up the access permission for the user through a more visual interface. The access level will still be shown as a link with additional explanation.

Rights system

Category

Uniform data model

To easily share data among each other and to be able to supervise this, there is a uniform data model within the Bubl vaults, also called common data model (CMD).

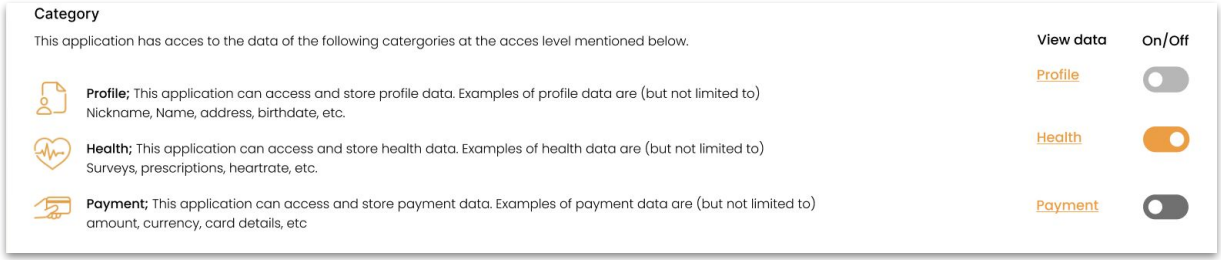
Category

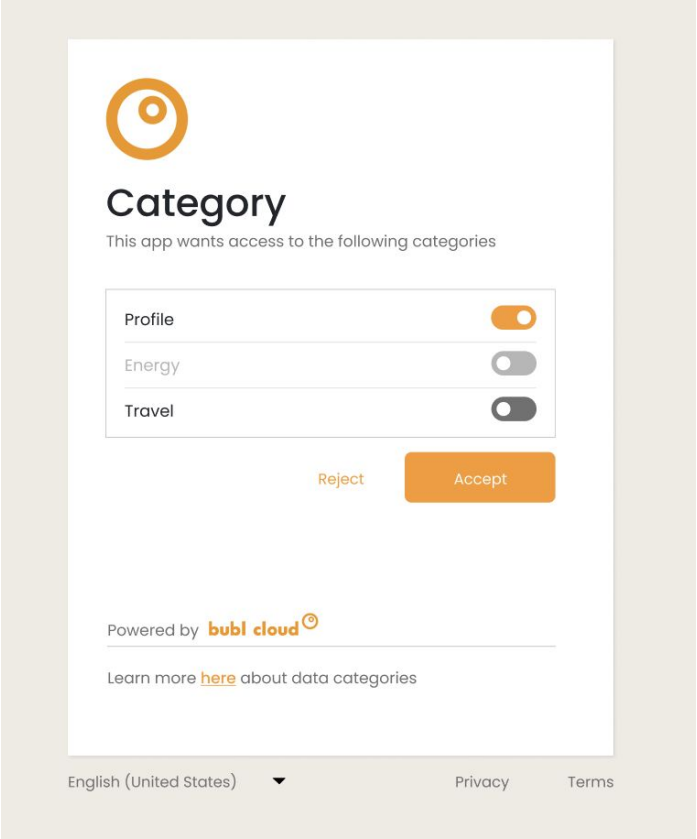
Every uniform data model falls within a certain category. Examples of categories are "profile", "energy" and "health". A user always explicitly gives permission for access to a category. Within this category, the application then has full access to all fields within its access level.

Own application data

Besides applications writing their data to the vault as shared data, they also have their "own" data storage. This data is not shared with others. Think of data such as logs, data for backend connections, security codes, data for specific service handling. Furthermore, intermediate data transformations or operations for the front-end are also stored here.

Examples of granting and revoking access to categories





Above: On the application settings page

Left: During login

Rights system

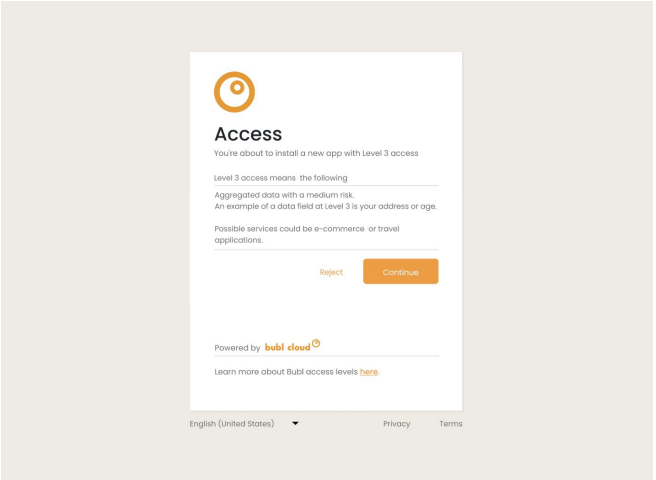
Access level

Access levels

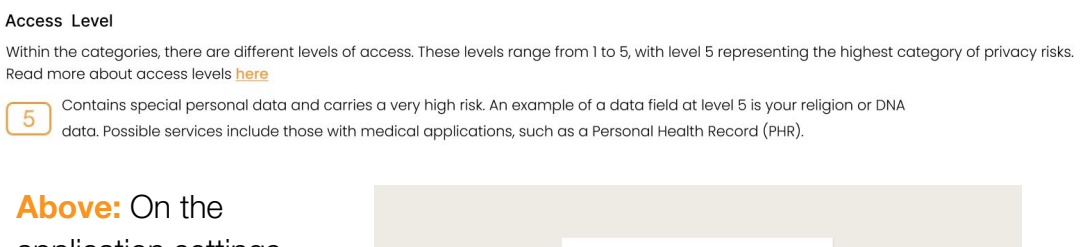
Within a category are the data fields. Access to these fields is restricted by an assigned access level. All fields within this category and access level are then available. The fields are currently not restricted individually.

- **Level 1** contains public data and poses no risk. An example of a data field at level 1 is a profile name on a website for example. Possible services are forums like nu.nl and reddit.com
- **Level 2** contains publicly available data on the Bubl Cloud platform and has a low risk. An example of a data field at level 2 is your name or email. Possible services are discord or slack.
- **Level 3** contains aggregated data with a medium risk. An example of a data field at level 3 is your address or age. Possible services for e-commerce applications like AH app or booking.com.
- **Level 4** contains personal data with a high risk. An example of a data field at level 4 is your date of birth, passport ID or digID. Possible services with financial applications or smart meter data at minute level.
- **Level 5** contains special personal data and has a very high risk. An example of a data field at level 5 is your religion or DNA data. Possible services with medical applications, a PGO.

Examples of granting and revoking access level

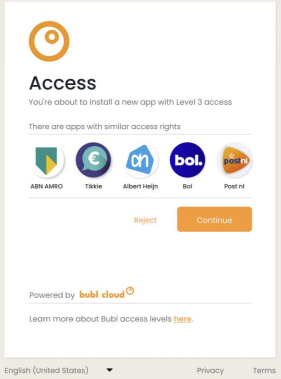


Left: during login with multiple services already active in the vault.



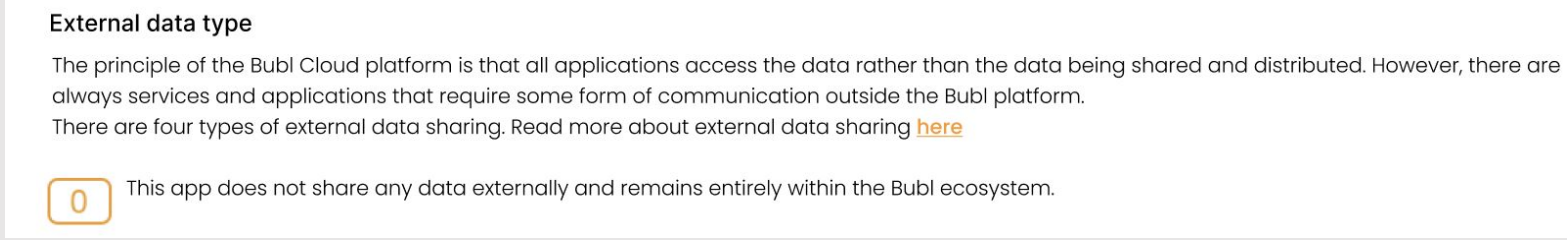
Above: On the application settings page.

Right: During login with multiple services active on the same access level.



Rights system

External sharing type



Four types of sharing

The reverse data model assumes that all services go to the data instead of the data being distributed, however there are always services and applications that require some form of communication outside the Bubl platform.

Bubl Cloud distinguishes four types of external data sharing

- **Type 0:** An application that does not share any data externally in its entirety and only remains within the Bubl ecosystem.
- **Type 1:** An application that only uses "own" data and does not collect "shared" data, where the own collected data goes outside.
- **Type 2:** An application that communicates "own data" and self-collected "shared data", or "shared data" that the application also uses itself (clear to user, for example an address for online purchases) externally, for example to the carrier.
- **Type 3:** An application that processes "own data" and also all "shared data" within its category and access level, think of an application for medical research.

Timeline (Max last 3 items)

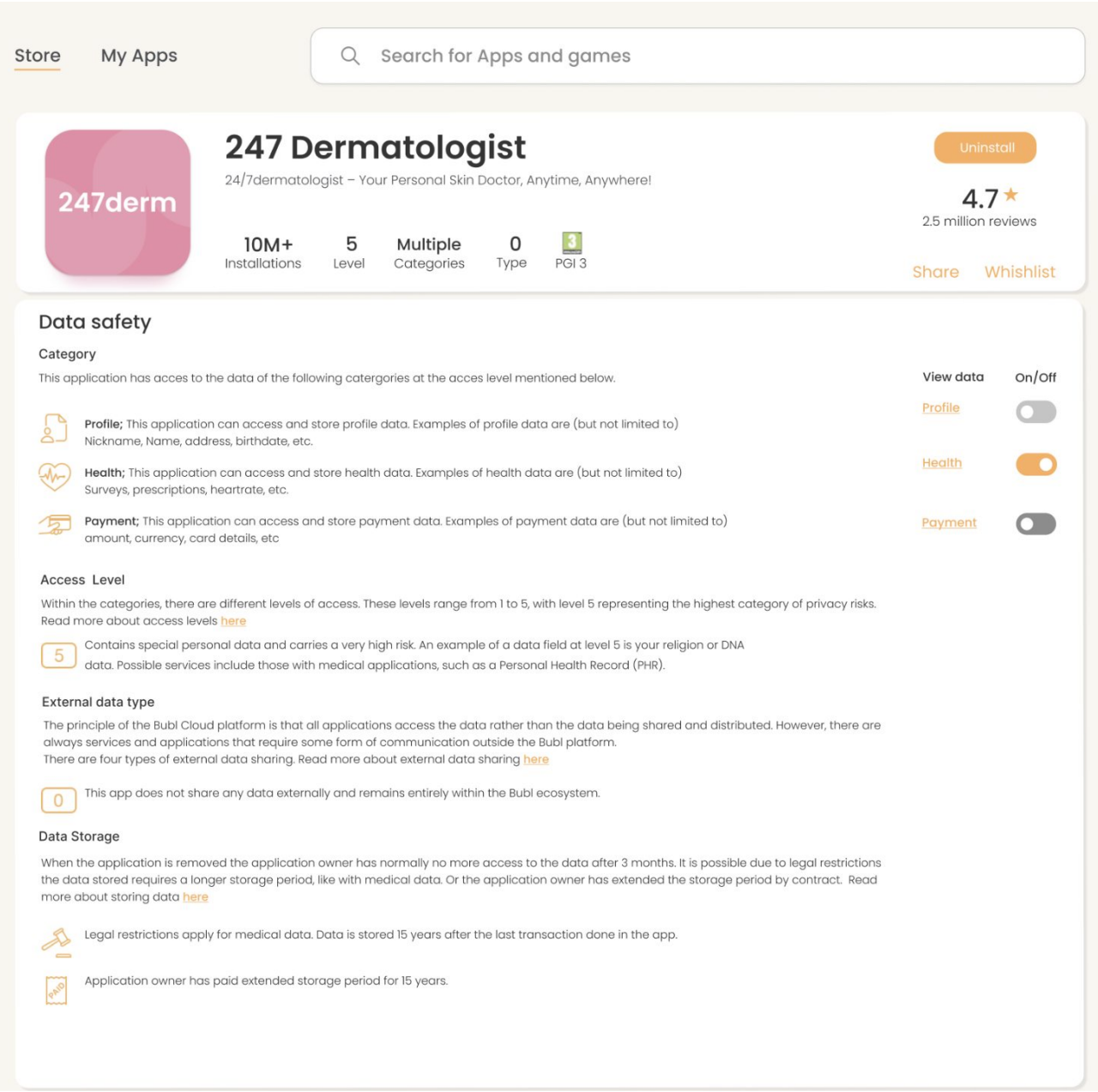
Date & time	Receiving party	Reason (token name)	Sample data
21 augustus 2024 12:14	615912bubl514298bubl734118.0.0.0.0.1.0.bubl.cloud	review of medical records dermatological consultation, dermatologist Jolanda de Vries	Sample of outgoing data
10 juni 2024 10:18	615912bubl514298bubl734118.0.0.0.0.1.0.bubl.cloud	review of medical records dermatological consultation, dermatologist Jolanda de Vries	Sample of outgoing data

Rights system:

Rules

Application rules

- **Rule 1:** An application can always access its "own application data", but can never access the "own application data" of another application.
- **Rule 2:** An application can always access all fields within its assigned category and access level.
- **Rule 3:** An application with an access level of 2 or higher can also always access data from lower access levels within its category.
- **Rule 4:** An application cannot be blocked for a specific field within its permitted category and access level.
- **Rule 5:** Applications may use each other's functionality within the Bubl Cloud platform. However, they may only share the results and not the underlying "uniform data model data".
- **Rule 6:** An application may communicate data externally (type 1, 2 & 3) only if explicit permission has been given by the user.
- **Rule 7:** Bubl Cloud will at all times during the evaluation process block services that collect, process and/or communicate data externally that have no added value to the application.



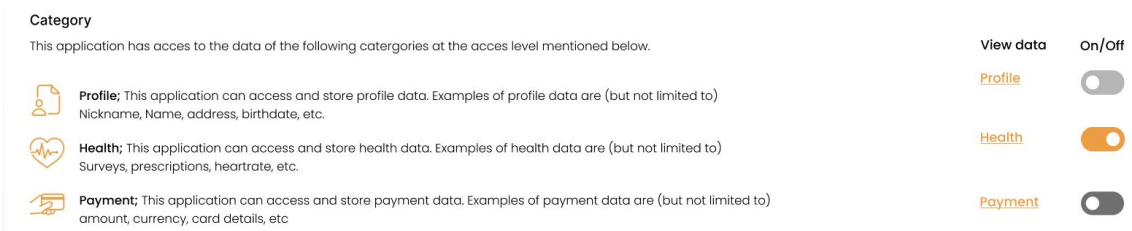
Management
Monitoring

Central Management

The user can view and modify previously granted rights per application in the Bubl Store in his/her Bubl. Here the user can also see who has had access to his/her data, which data is stored, export the data and completely remove applications. The Bubl Store is the central point for the user regarding managing his Bubl and data.

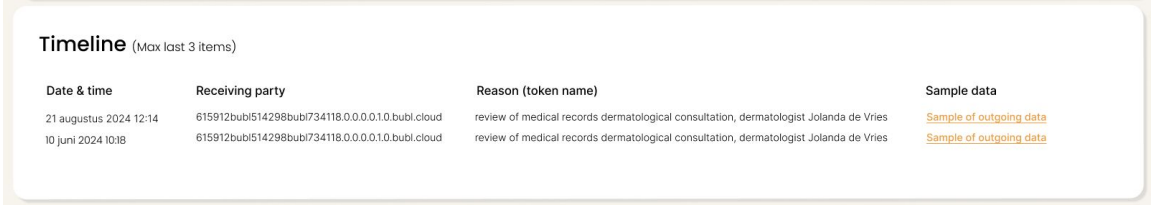
Access per category

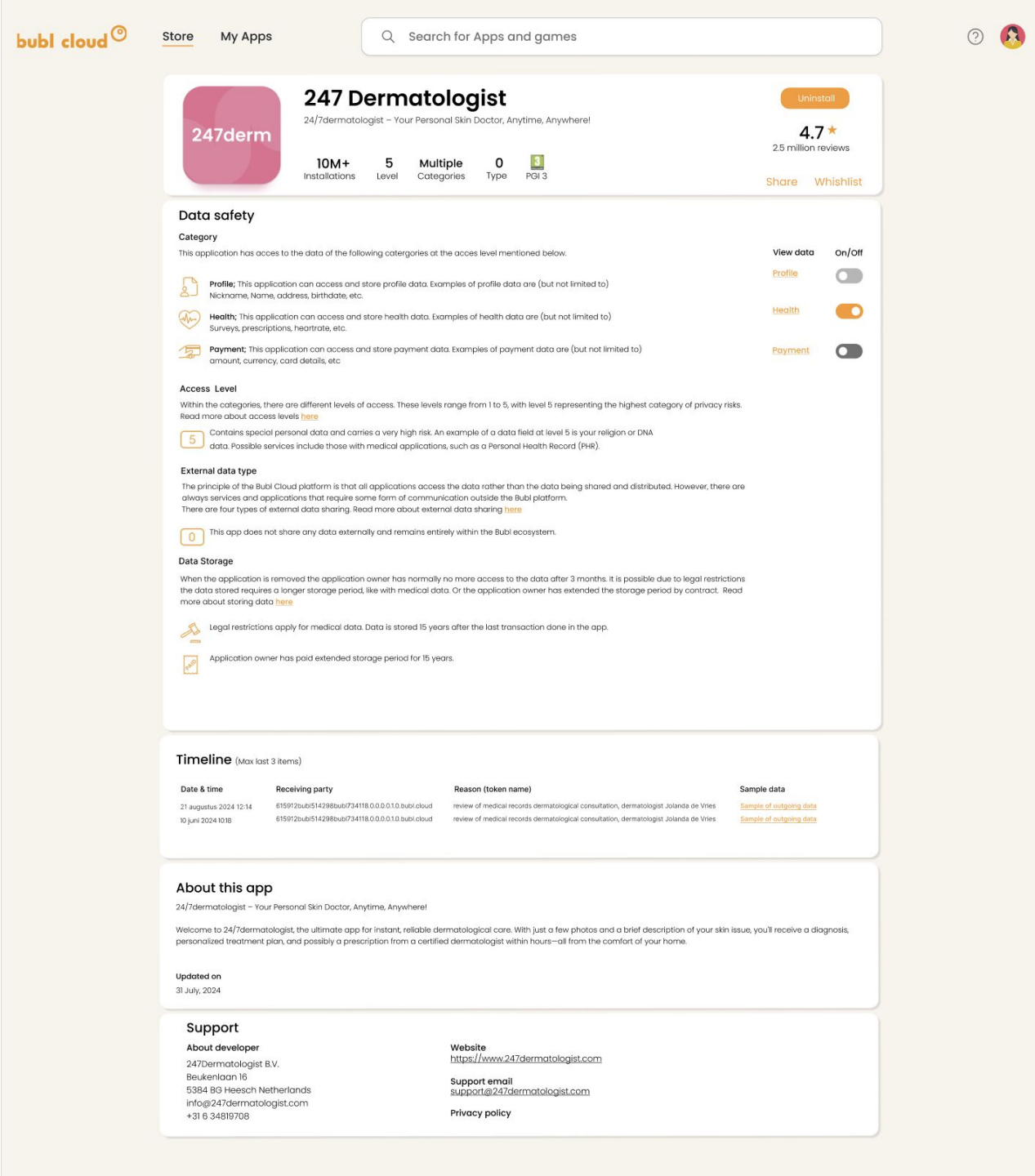
On the application settings screen, the user can indicate per category whether the user still wants to continue granting access. Access can only be granted and revoked per category.



Timeline

On the timeline on the application settings page, the user can easily view the last three events of the application.





Management

Data insights

Expert mode

Under "expert mode" in the Bubl settings menu, "view logs" and "data stored" can be selected.

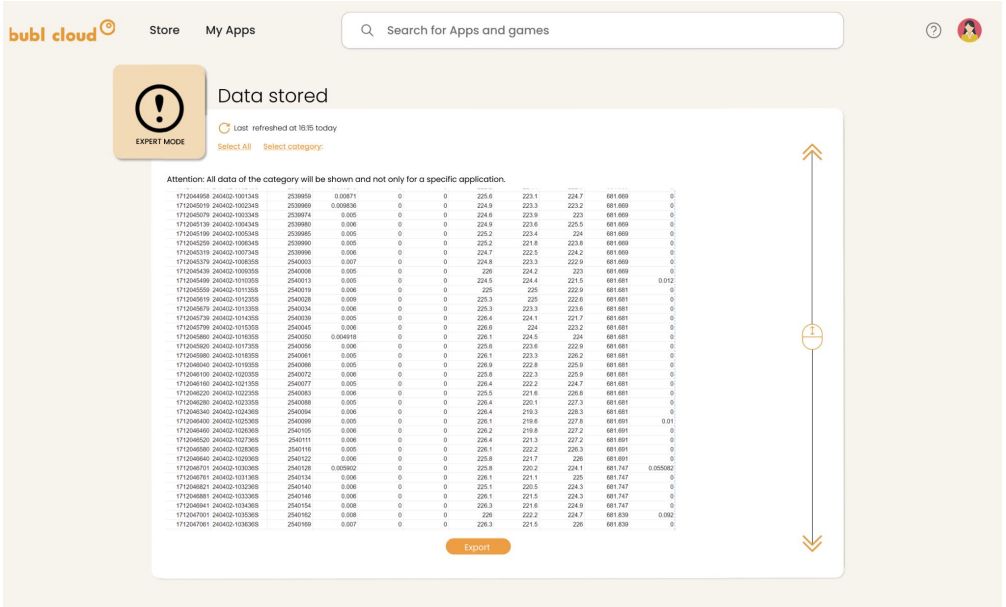
Logs

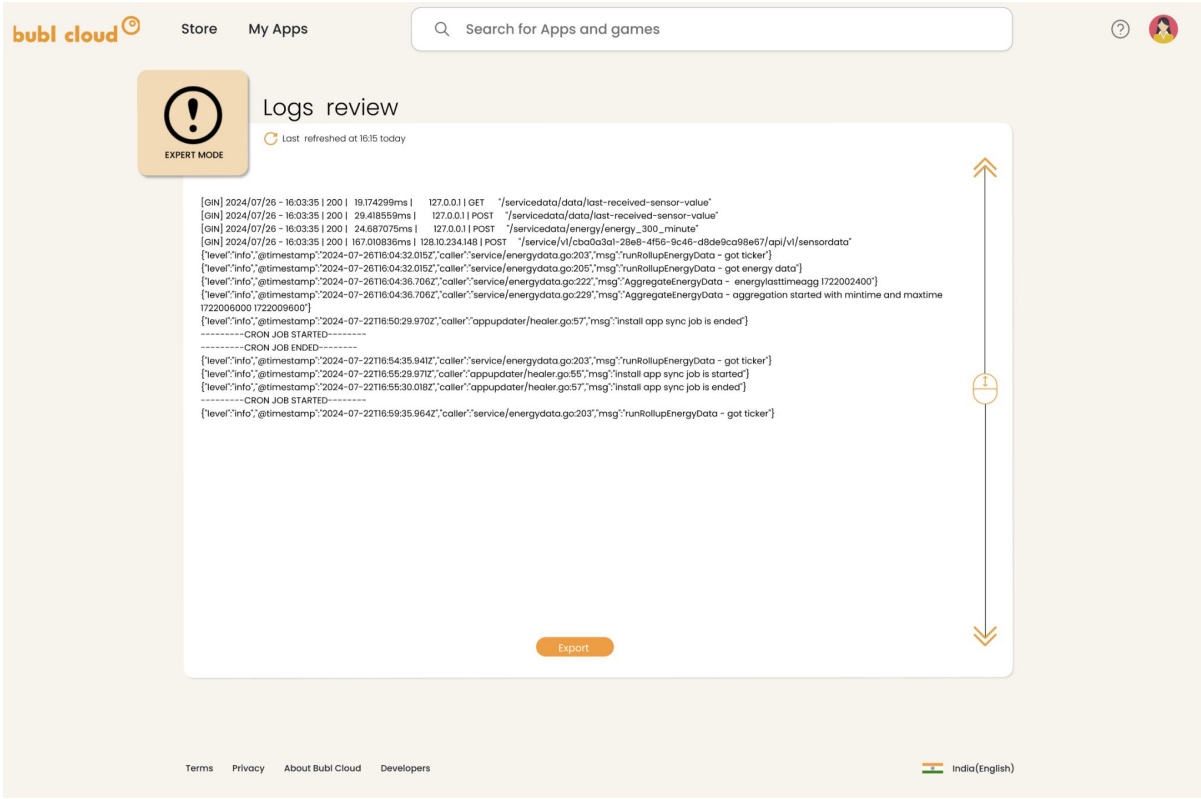
On this screen, the user can see a number of things in the logs such as:

1. Access requests
2. Write and read activities
3. The application, category and level.

Data

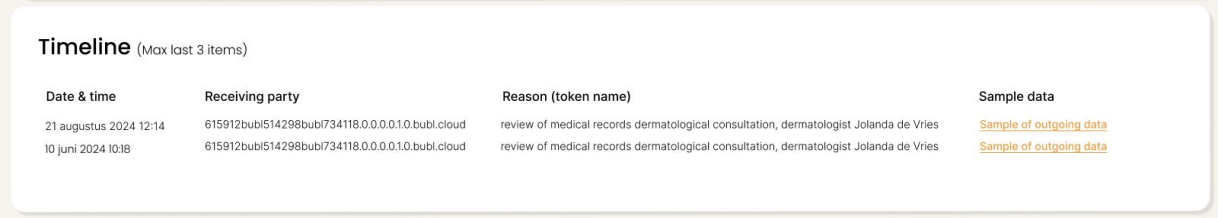
This screen will show the entire stored content of the uniform data model per category or the entire uniform data model.





Timeline

In addition to the expert mode data insights, a sample of processed and/or outgoing data from the last 3 operations is also shown on the timeline of the application settings page




JOIN
THE
PERSONAL
DATA CLOUD
Unlocking the potential
of personal data
Seamless. Secure. Privacy safe.
bubl cloud