6.4. Data privacy

Data privacy has been one of the key considerations will design the data architecture of the RNCV. you will find below the key principle we followed during the development of the data architecture.

Principle 1: Data minimisation

Description

Only data that is strictly necessary to the RNCV will be collected. Each field collected is documented, justified and approved.

Implementation

4.4.1. Data models

Principle 2: Do not store private data if not absolutely needed

Description

Private data should not be stored except in very exceptional cases. Each field of data model where private data is stored or could be stored is documented, justified and approved by MyConnectivity.

Implementation

4.4.1. Data models

Principle 3: Fine-Grained Access Rights

Description

Each field stored in the RNCV will be limited in access (read and/or write) to the user roles that need it. Furthermore certain fields can only be modified/accessed from via specific APIs only exposed to a management and / or administration network.

> E.g. Links between datasets and specific users that produced them are only visible by administrators, via the administration API that is only accessible via the Management access / network.

Implementation

3. User management & user roles

4. User stories

8. Data architecture

Principle 4: Purpose limitation

> TODO with lawyers

The Organisations that receive access to the data should be contractually limited on what they can do with the accessed data.

Revision #6
Created 16 October 2025 12:33:55 by Sergio Sousa
Updated 25 November 2025 10:19:33 by Sergio Sousa