



# FENIX

RESEARCH INFRASTRUCTURE

## Using ICEI resources for processing personal data

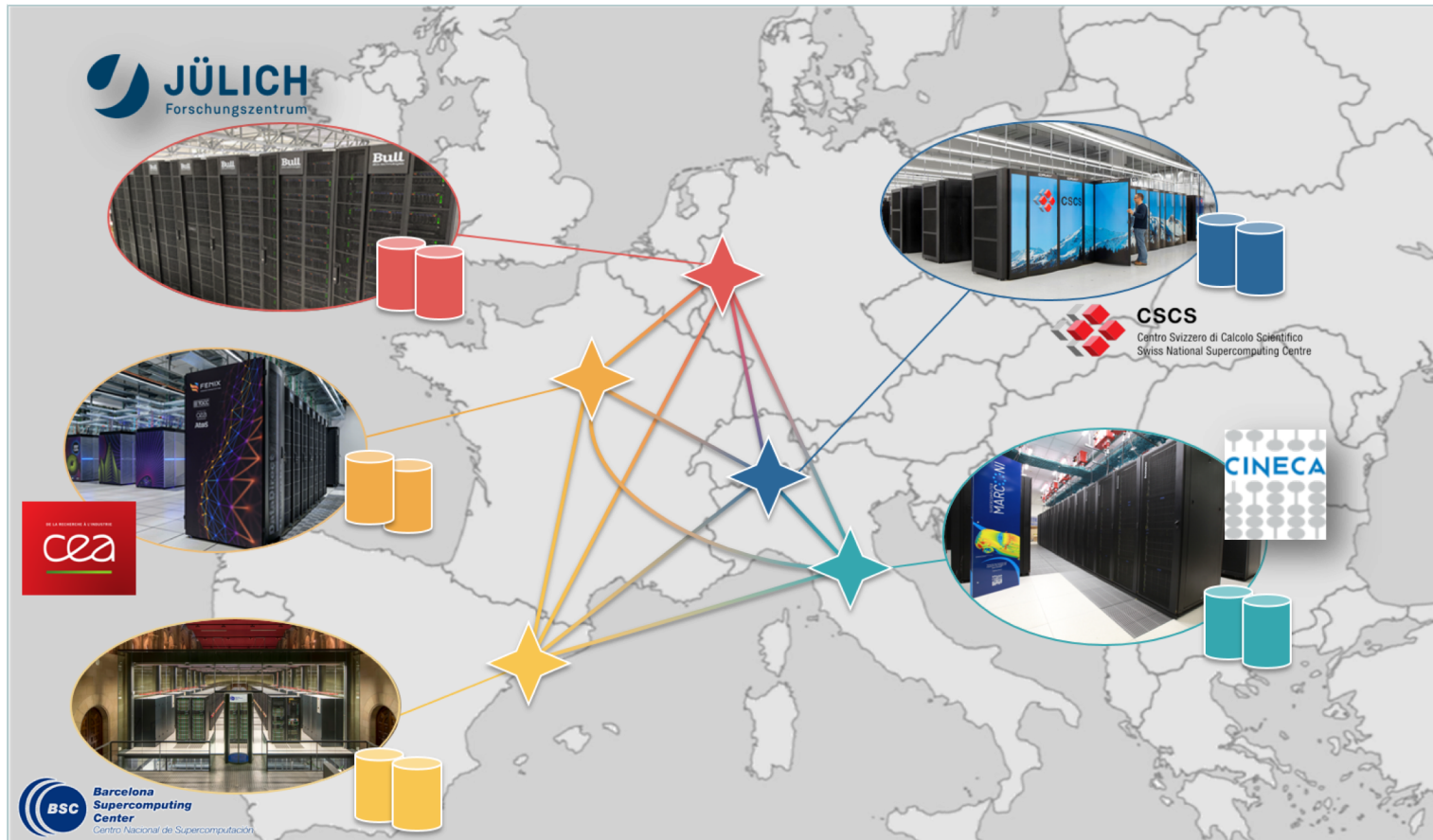
8<sup>th</sup> Fenix Research Infrastructure Webinar

Anne Nahm, Boris Orth (JSC) - December 15, 2020



The ICEI project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 800858.

# 5 European supercomputing centres are running the Fenix infrastructure within the ICEI project\*



\* The ICEI (Interactive Computing E-Infrastructure for the Human Brain Project) project is funded by the European Commission under the Framework Partnership Agreement of the Human Brain Project (HBP) (SGA ICEI 800858).



# Agenda

- General introduction to the Protection of Personal Data (POPD)
- Current regulations for storing/processing of personal data within the Fenix infrastructure
- Example of an ICEI-HBP project that involves personal data
- Q&A

# Agenda

- General introduction to the Protection of Personal Data (POPD)
- Current regulations for storing/processing of personal data within the Fenix infrastructure
- Example of an ICEI-HBP project that involves personal data
- Q&A



# Introduction

- Through the ICEI project, Fenix provides basic computing and storage infrastructure services for HBP/EBRAINS and other communities
  - See <https://fenix-ri.eu/infrastructure/services> for details

# Introduction

- Through the ICEI project, Fenix provides basic computing and storage infrastructure services for HBP/EBRAINS and other communities
  - See <https://fenix-ri.eu/infrastructure/services> for details
- Important use cases require the processing of personal data
  - Example involving UK Biobank data will be presented later by Anne

# Introduction

- Through the ICEI project, Fenix provides basic computing and storage infrastructure services for HBP/EBRAINS and other communities
  - See <https://fenix-ri.eu/infrastructure/services> for details
- Important use cases require the processing of personal data
  - Example involving UK Biobank data will be presented later by Anne
- Need to ensure appropriate protection of personal data

# Introduction

- Through the ICEI project, Fenix provides basic computing and storage infrastructure services for HBP/EBRAINS and other communities
  - See <https://fenix-ri.eu/infrastructure/services> for details
- Important use cases require the processing of personal data
  - Example involving UK Biobank data will be presented later by Anne
- Need to ensure appropriate protection of personal data
- Fenix partners providing ICEI resources are distributed across EU member states (D, E, F, I) and Switzerland

# Introduction

- Through the ICEI project, Fenix provides basic computing and storage infrastructure services for HBP/EBRAINS and other communities
  - See <https://fenix-ri.eu/infrastructure/services> for details
- Important use cases require the processing of personal data
  - Example involving UK Biobank data will be presented later by Anne
- Need to ensure appropriate protection of personal data
- Fenix partners providing ICEI resources are distributed across EU member states (D, E, F, I) and Switzerland
- Legal basis: General Data Protection Regulation (GDPR)
  - <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>
  - Applies in the EU; Switzerland has been recognized by the EC as providing adequate protection

# GDPR Art. 4: Personal data and pseudonymisation

## ■ Personal data

- *Any **information relating to an identified or identifiable natural person ('data subject')**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, [...]*

# GDPR Art. 4: Personal data and pseudonymisation

## ■ Personal data

- Any **information relating to an identified or identifiable natural person ('data subject')**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, [...]

## ■ Pseudonymisation

- Processing of personal data in such a manner that the **personal data can no longer be attributed to a specific data subject without the use of additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

# GDPR: Whereas...

- (26) [...] Personal data which have undergone pseudonymisation [...] should be considered to be information on an identifiable natural person. [...]*
- (28) [...] The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.*



# GDPR: Whereas...

- (26) [...] Personal data which have undergone pseudonymisation [...] should be considered to be information on an identifiable natural person. [...]
- (28) [...] The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

**Pseudonymised data is still personal data falling under the GDPR.**

# GDPR Art. 4: Data controller and processor

## ■ Controller

- *Natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; [...]*

# GDPR Art. 4: Data controller and processor

## ■ Controller

- *Natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; [...]*

## ■ Processor

- *Natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller***

# GDPR Art. 4: Data controller and processor

## ■ Controller

- *Natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; [...]*

## ■ Processor

- *Natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller***

Fenix sites as infrastructure service providers will always be **Data Processors**.

Organisations that apply for Fenix resources will typically act as **Data Controllers**.\*

# GDPR Art. 4: Data controller and processor

## ■ Controller

- *Natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; [...]*

## ■ Processor

- *Natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller***

Fenix sites as infrastructure service providers will always be **Data Processors**.

Organisations that apply for Fenix resources will typically act as **Data Controllers**.\*

\* In the future, EBRAINS platform service providers may also act as Data Processors. This will require a suitable contractual framework involving the relevant Fenix sites, organisations offering EBRAINS services, and EBRAINS users.

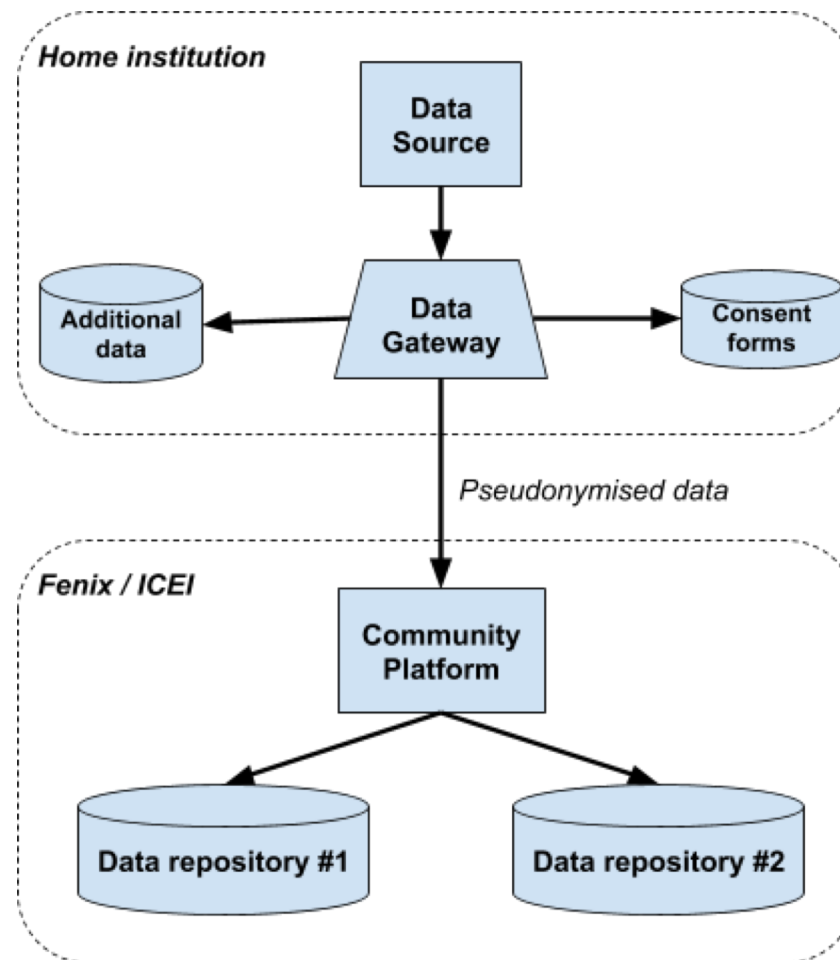
# Overview of Fenix data classes

Class	Description	Currently allowed by Fenix
A	Data sets containing information relating to an identified data subject.	✗
B	Data sets containing information relating to an identifiable data subject, i.e., there is a known systematic way to (re)identify the data subject.	(✓)
C	Data sets containing personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	✓
D	Data sets that contain no information relating to an identified or identifiable data subject.	✓

# Fenix regulations on data classes

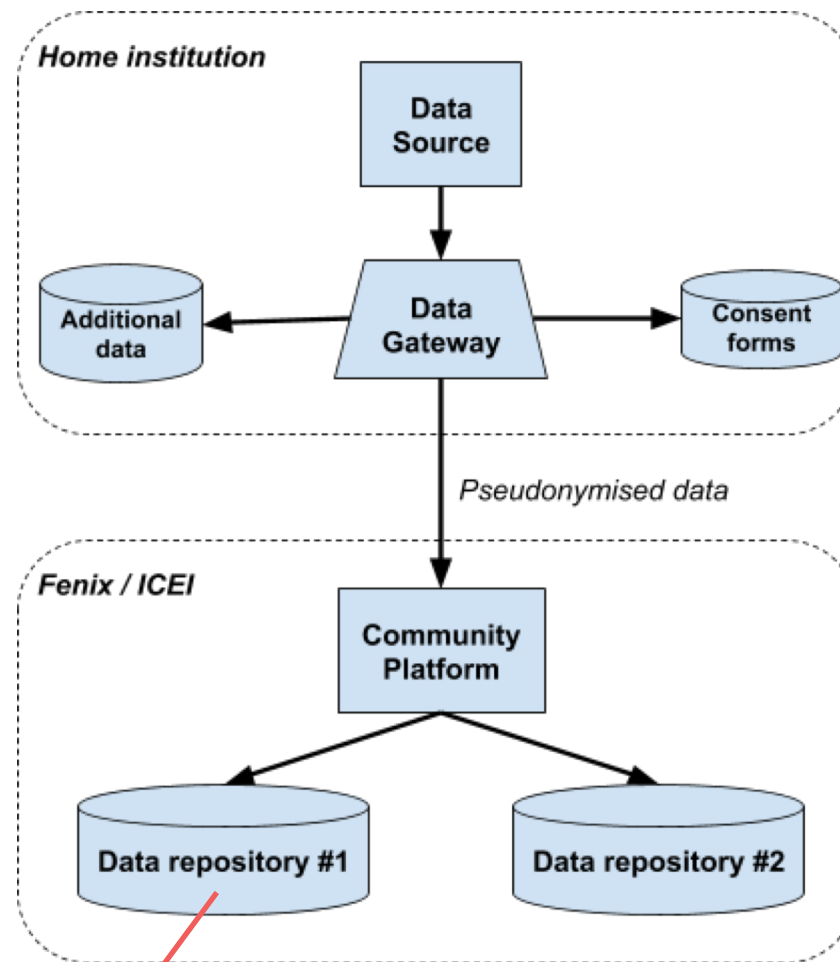
- **Class A:** This data must not be stored within the Fenix infrastructure.
  - Fenix Users have to confirm that they will comply with this rule by signing a user agreement before they get access to Fenix resources.
- **Class B:** Restrictions apply.
  - See following slides.
- **Class C:** Allowed.
  - But: Responsibility for assessing and monitoring if there are known technical means to transform the data such that it would allow to identify a data subject remains with the Data Controller, i.e., the Fenix User.
- **Class D:** No restrictions (GDPR does not apply).

# Fenix approach for Class B data





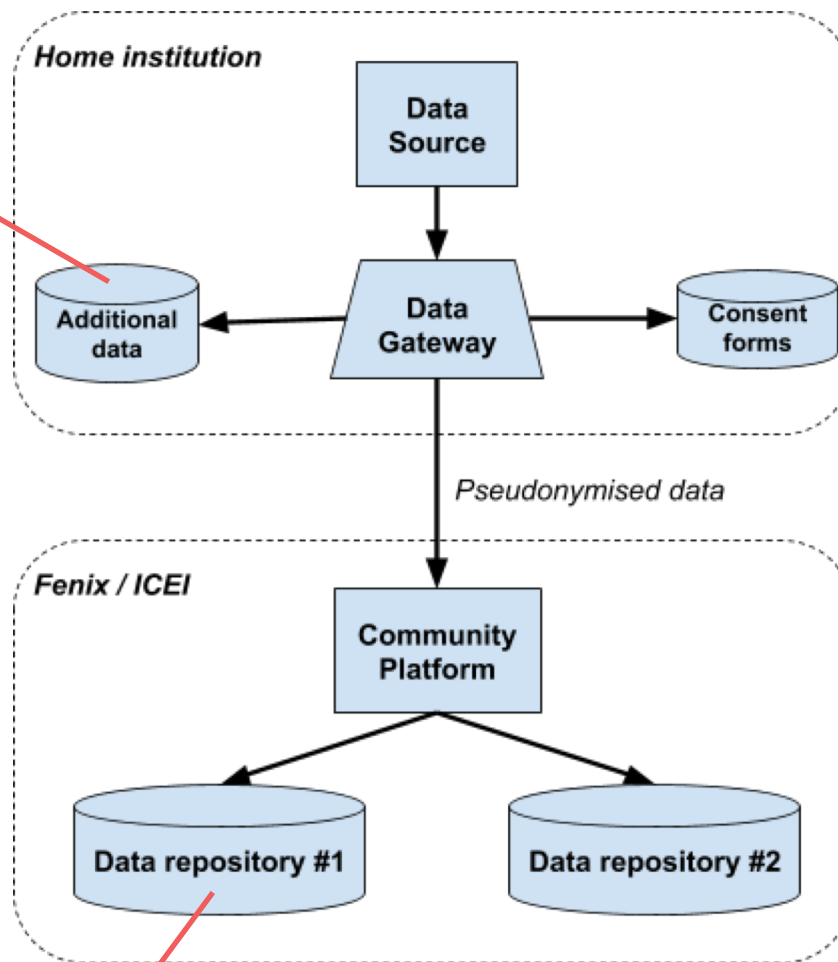
# Fenix approach for Class B data



Class B data: A systematic way to (re)identify the data subject by combining the pseudonymised data with additional information is known.

# Fenix approach for Class B data

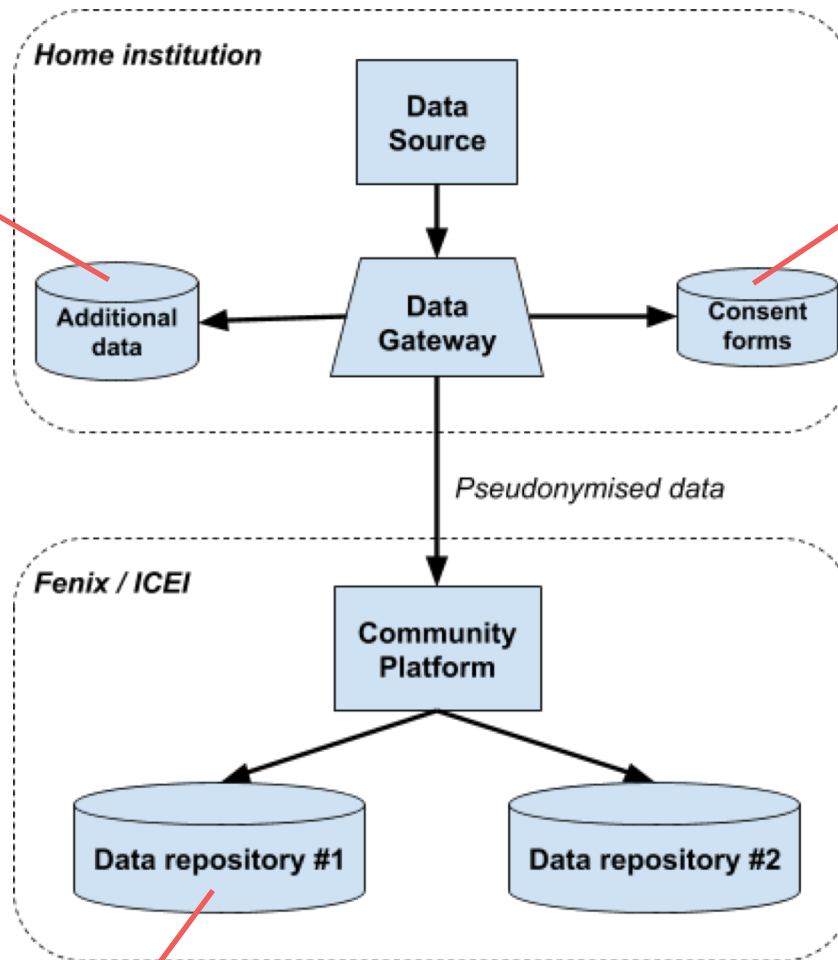
The Fenix User as Data Controller is responsible for **storing this additional data outside of the Fenix Infrastructure**, ensuring adequate protection.



Class B data: A systematic **way to (re)identify the data subject** by combining the pseudonymised data with additional information **is known**.

# Fenix approach for Class B data

The Fenix User as Data Controller is responsible for **storing this additional data outside of the Fenix Infrastructure**, ensuring adequate protection.



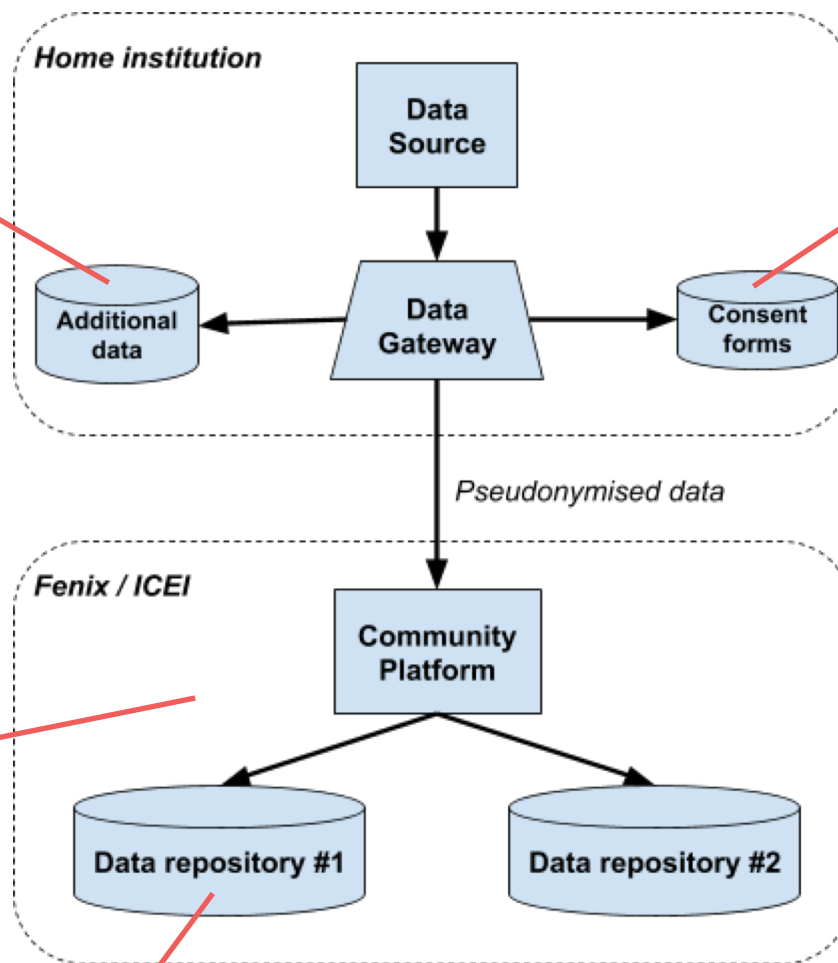
The Fenix User is also responsible for **protecting the data subject rights**, e.g., for managing consent forms

Class B data: A systematic way to (re)identify the **data subject** by combining the pseudonymised data with additional information **is known**.

# Fenix approach for Class B data

The Fenix User as Data Controller is responsible for **storing this additional data outside of the Fenix Infrastructure**, ensuring adequate protection.

As Data Processor, Fenix supports the Fenix user by, e.g., **implementing appropriate technical and organizational measures**.



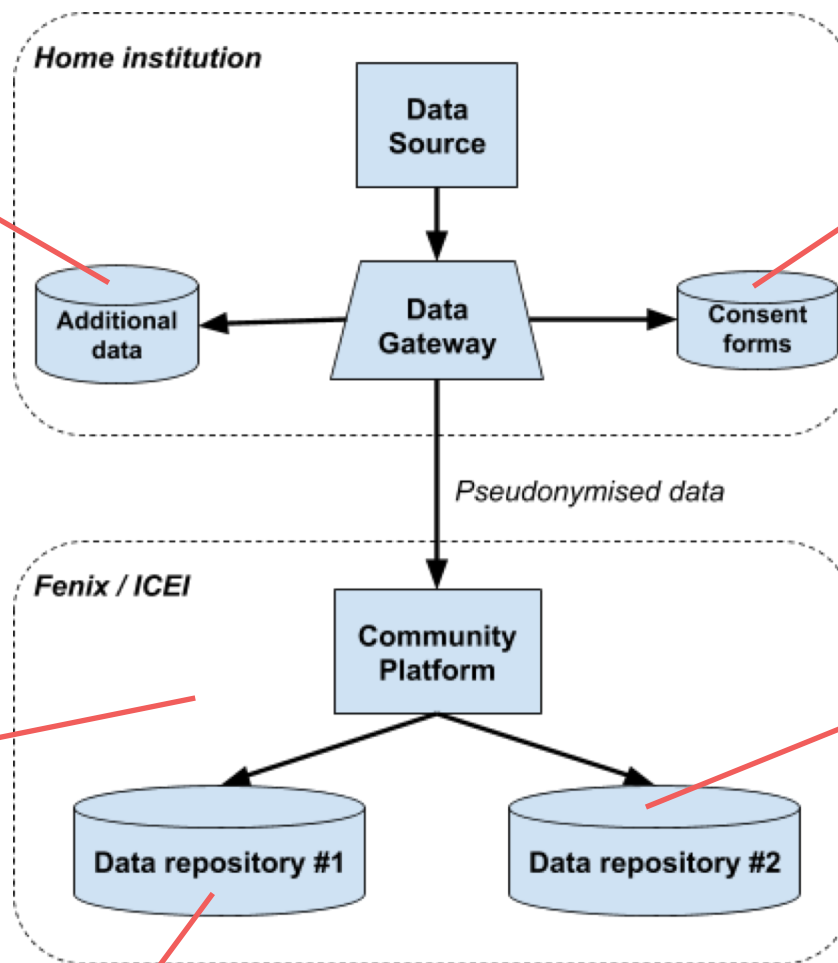
The Fenix User is also responsible for **protecting the data subject rights**, e.g., for managing consent forms

Class B data: A systematic way to (re)identify the **data subject** by combining the pseudonymised data with additional information **is known**.

# Fenix approach for Class B data

The Fenix User as Data Controller is responsible for **storing this additional data outside of the Fenix Infrastructure**, ensuring adequate protection.

As Data Processor, Fenix supports the Fenix user by, e.g., **implementing appropriate technical and organizational measures.**



The Fenix User is also responsible for **protecting the data subject rights**, e.g., for managing consent forms

Fenix monitors the Class B datasets in the infrastructure to **minimize the risk of data subjects being re-identified by combining different pseudonymised data sets from the same data source**

Class B data: A systematic **way to (re)identify the data subject** by combining the pseudonymised data with additional information **is known.**

# Data locality

- Fenix infrastructure services do not guarantee a certain data location, nor do they automatically change data locations.

# Data locality

- Fenix infrastructure services do not guarantee a certain data location, nor do they automatically change data locations.
- Fenix Users must specify a repository when uploading data to the Fenix federated archival data repositories.

# Data locality

- Fenix infrastructure services do not guarantee a certain data location, nor do they automatically change data locations.
- Fenix Users must specify a repository when uploading data to the Fenix federated archival data repositories.
- Fenix services support data transfer between federated archival data repositories at different locations, but these transfers must be initiated by a Fenix User.



# Data locality

- Fenix infrastructure services do not guarantee a certain data location, nor do they automatically change data locations.
- Fenix Users must specify a repository when uploading data to the Fenix federated archival data repositories.
- Fenix services support data transfer between federated archival data repositories at different locations, but these transfers must be initiated by a Fenix User.
- No services are foreseen that would result in an automatic geo-redundant replication of data without involvement of Fenix Users. Fenix Users thus have full control of the geo-location of their data.

# Exceptions for scientific research

- GDPR provides certain allowances for data processing for scientific research purposes.

# Exceptions for scientific research

- GDPR provides certain allowances for data processing for scientific research purposes.
- Allowances or exemptions are 'derogations' under the GDPR, which will vary by member state, and will likely result in different legal requirements across the EU.

# Exceptions for scientific research

- GDPR provides certain allowances for data processing for scientific research purposes.
- Allowances or exemptions are 'derogations' under the GDPR, which will vary by member state, and will likely result in different legal requirements across the EU.
- ICEI infrastructure services do not provide the means of preventing replication of data between archival data repositories located at different sites and thus possibly different countries.

# Exceptions for scientific research

- GDPR provides certain allowances for data processing for scientific research purposes.
- Allowances or exemptions are 'derogations' under the GDPR, which will vary by member state, and will likely result in different legal requirements across the EU.
- ICEI infrastructure services do not provide the means of preventing replication of data between archival data repositories located at different sites and thus possibly different countries.
- Fenix Users that upload Class B data must therefore check if a derogation applies to the Fenix site to which the data is uploaded.