Responsibility and Accountability under the GDPR

Regina Becker
ELIXIR-LU

ELIXIR Workshop Data Protection
ECCB 2018 / Athens
11. September 2018

GDPR is catching up with us…

— GDPR: General Data Protection Regulation

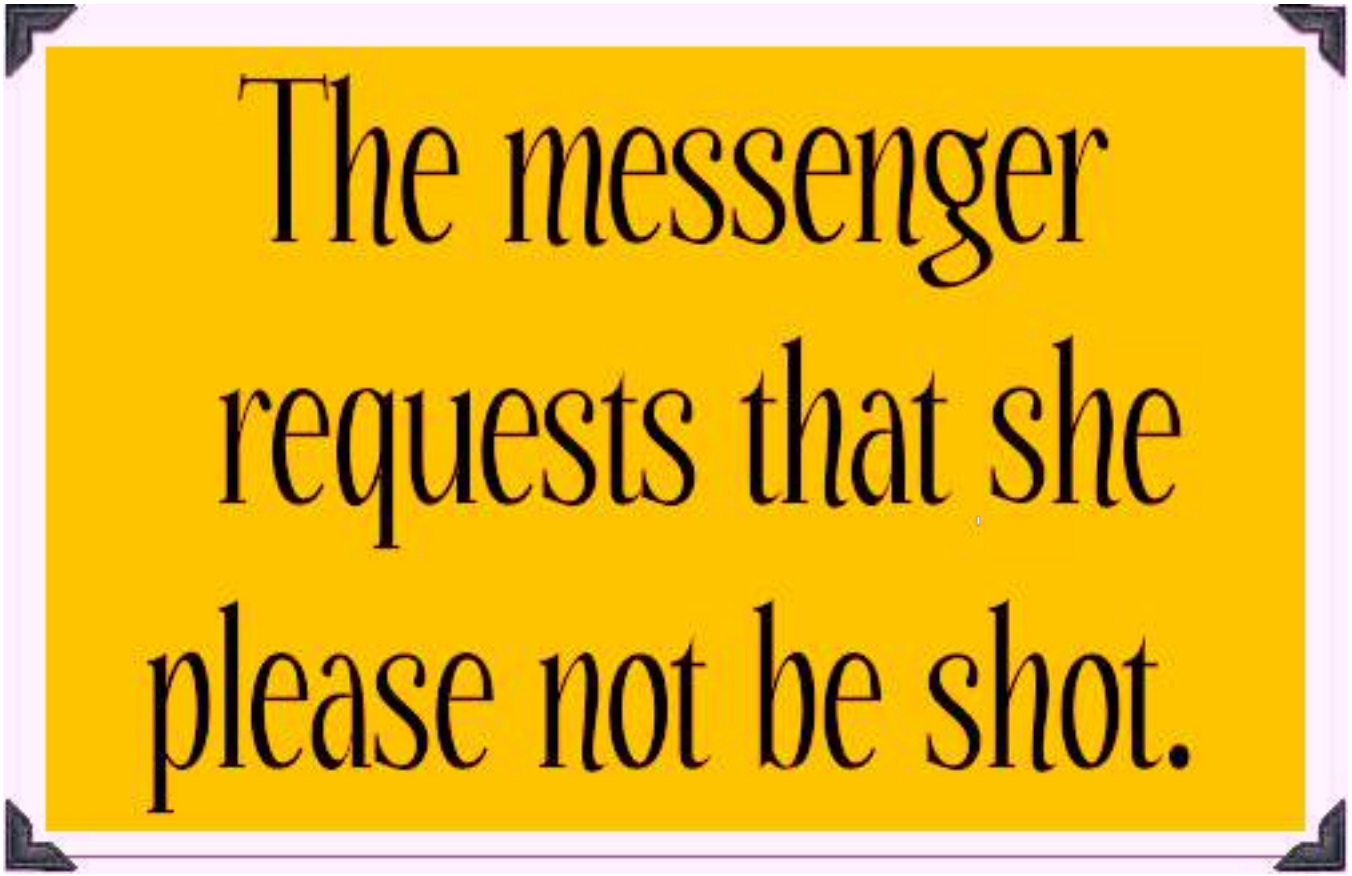
GDPR

- Became effective on 25 May 2018
- Is directly applicable as law
- Considerable consequences for processing of personal data
- Defined scope of opening clauses for national specifications to further complicate the situation

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

First things first…



steemkr.com

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

The axiom of Article 5

Art. 5.2 The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

stratford.edu

YOU are responsible for your processing

elixir LUXEMBOURG

Understanding the GDPR

— The most important principles

Lawfulness

Art. 6 Legal Basis

Art. 9 Special categories of data

Art. 44-49 Transfer to third countries or international organisations

Fairness

Art. 5.1 (b) purpose limitation

Art. 5.1 (c) data minimisation

Art. 5.1 (d) accuracy

Art. 5.1 (e) storage limitation

Art. 5.1 (f) integrity and confidentiality

Art. 16-21 data subjects' rights

Art. 5.1 Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

Transparency

Art. 12-15 data subjects' rights, Art. 30 Records of processing

What you need to know

— Processing

- Any operation […], such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;[…] Art. 4 (2)

Asseco Poland

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

The heart of the GDPR

— The most important principles

Lawfulness

Art. 6 Legal Basis

Art. 9 Special categories of data

Art. 44-49 Transfer to third countries or international organisations

Fairness

Art. 5.1 (b) purpose limitation

Art. 5.1 (c) data minimisation

Art. 5.1 (d) accuracy

Art. 5.1 (e) storage limitation

Art. 5.1 (f) integrity and confidentiality

Art. 16-21 data subjects' rights

Art. 5.1 Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

→ Sarion Bowers

Transparency

Art. 12-15 data subjects' rights, Art. 30 Records of processing

The heart of the GDPR

— The most important principles

Lawfulness

Art. 6 Legal Basis

Art. 9 Special categories of data

Art. 44-49 Transfer to third countries or international organisations

Fairness

Art. 5.1 (b) purpose limitation

Art. 5.1 (c) data minimisation

Art. 5.1 (d) accuracy

Art. 5.1 (e) storage limitation

Art. 5.1 (f) integrity and confidentiality

Art. 16-21 data subjects' rights

Art. 5.1 Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

Transparency

Art. 12-15 data subjects' rights, Art. 30 Records of processing

Purpose limitation

— Stick to your promise!

Beware:

- Stay within scope of your communicated purposes at the time of collection

Further processing

- Should be “not incompatible” according to Art. 5.1
- May not be available under consent in all countries (See statements preparations for Swedish Research Act / p32: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2017/06/sou-201750/)
- Requires advance information (independent of the legal basis)

Data Sharing

- Responsibility to ensure by contract the adherence to the purpose limitation

elixir LUXEMBOURG

Data minimisation

— What is minimal enough?

Collection

- Collect only what is needed
  — which can be a lot considering the determinants of health and disease are unknown

Purpose

- Where no directly identifying data is needed
  → pseudonymise or anonymise data
- Data analysis plans should specify which data types are needed

Access

- Access only on a need basis, not by default

Retention

- Delete data if no longer needed
  — avoid data graveyards!

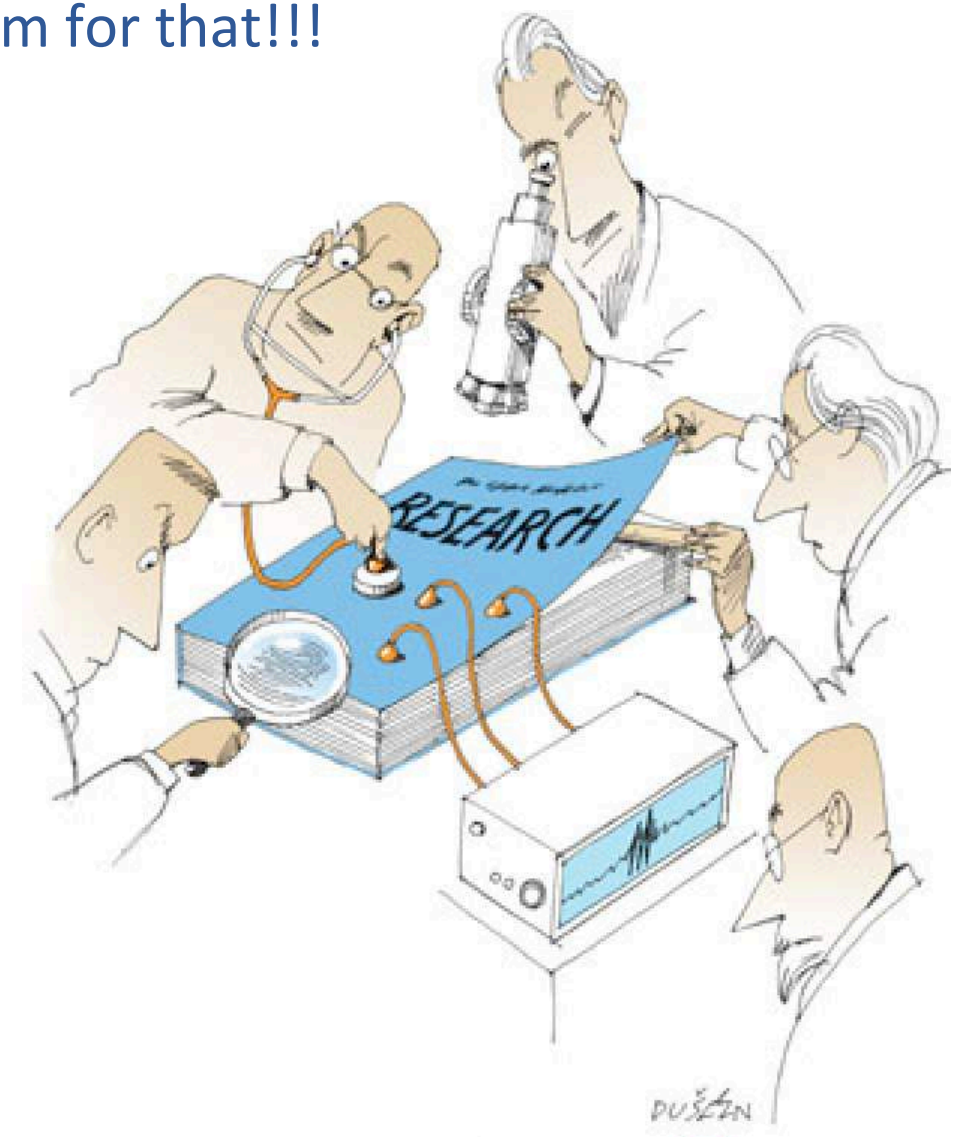
Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Accuracy

— Data needs to be accurate

- We all aim for that!!!



the-scientist.com

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Storage limitation

— Nothing lasts forever!

- Defined time point to be given
- Alternative: criteria how long data will be kept
- Independent of choice:
  needs to be told to the study participants
- Beware: don't forget your archiving obligations in the communication with the study participants

What do you mean, we need to delete the data right after the project?

What about archiving?

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Integrity

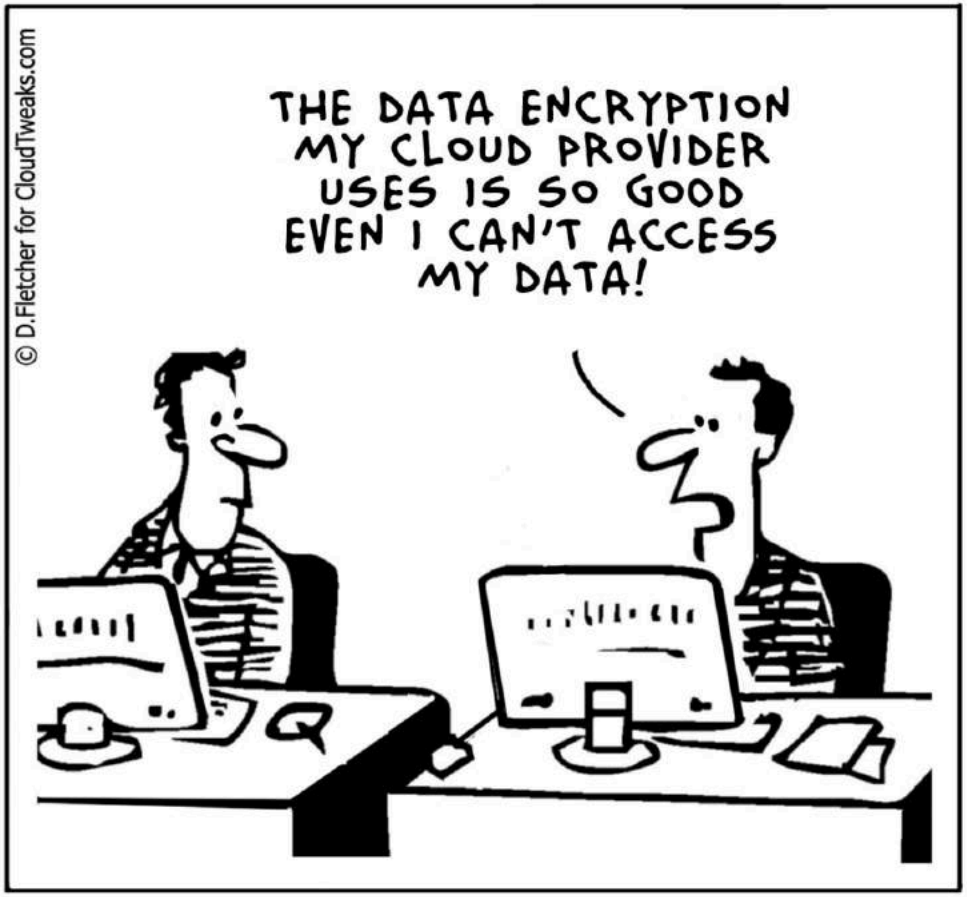
— Avoid data corruption or data loss

- Use checksums to test for corruption
- Backups are important
  — we know that anyway! ☺

Confidentiality

— Art. 25 & 32: Organisational and technical measures

- Technical security measures
  (pseudonymisation, encryption, access restriction,
  event logging, compliance monitoring, …)
- Policies
- Training
- Security clauses



Luxembourg Centre for Systems Biomedicine

Data subjects' rights: Articles 15 – 21

— Actions to be taken on demand of the data subject

- Give access to data
- Inform about every user and every project
- Have data deleted or rectified – even from subsequent recipients
- Withdrawal of consent or objection to processing
- Portability - transfer data to another processor or controller

A2jlab.org

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

The heart of the GDPR

— The most important principles

Lawfulness

Art. 6 Legal Basis

Art. 9 Special categories of data

Art. 44-49 Transfer to third countries or international organisations

Fairness

Art. 5.1 (b) purpose limitation

Art. 5.1 (c) data minimisation

Art. 5.1 (d) accuracy

Art. 5.1 (e) storage limitation

Art. 5.1 (f) integrity and confidentiality

Art. 16-21 data subjects' rights

Art. 5.1 Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

Transparency

Art. 12-15 data subjects' rights, Art. 30 Records of processing

Art. 13 - 15: Information provision

— "The data subject should never be surprised…"

- Inform about:
  Identity and contact of controller, legal basis, purpose of processing, recipients, transfers outside the EU, source of the data, automated decision making, rights of the data subject
- Important guidance from European Data Protection Board (EDPB)
  https://edpb.europa.eu/our-work-tools/our-documents/guideline/consent_en
- Beware: EDPB states that ethics information must be separate from data protection information
- Keep in mind: information obligation applies in the same way to your website privacy notes!!

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Record keeping following Art. 30.1
— Documentation is key under GDPR

Content of processing records

- Contact details of controller:
  representative and data protection officer
- Purposes of the processing
- Categories of data subjects and categories of personal data
- Categories of recipients, in particular:
  recipients in third countries or international organisations
- Transfers outside the EU including safeguards
- Envisaged time limits for erasure of different categories of data
- Description of technical and organisational security measures

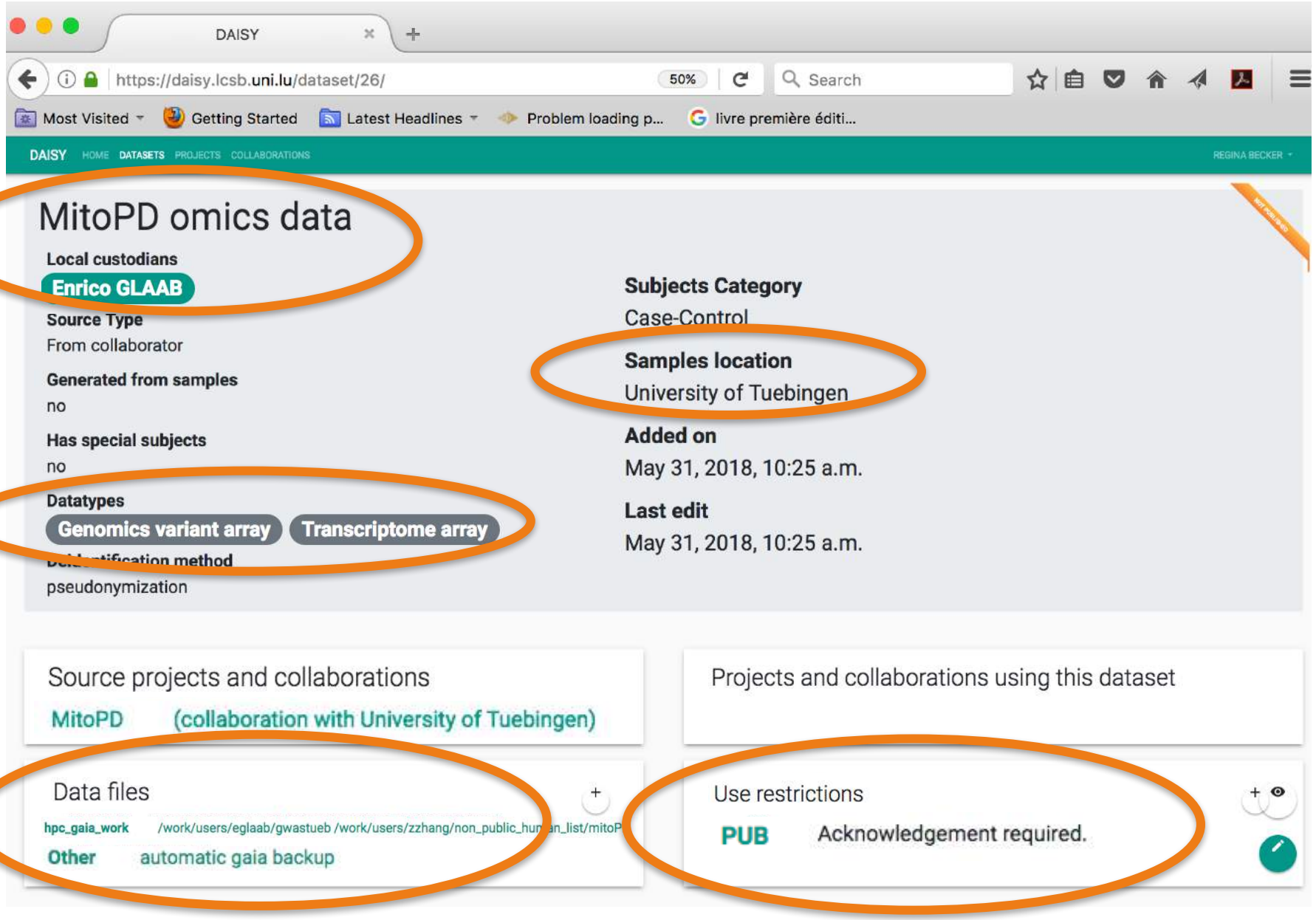
Problem for most institutions

- Registries need to cover a wide field of activities:
  Personnel administration, teaching, research, …

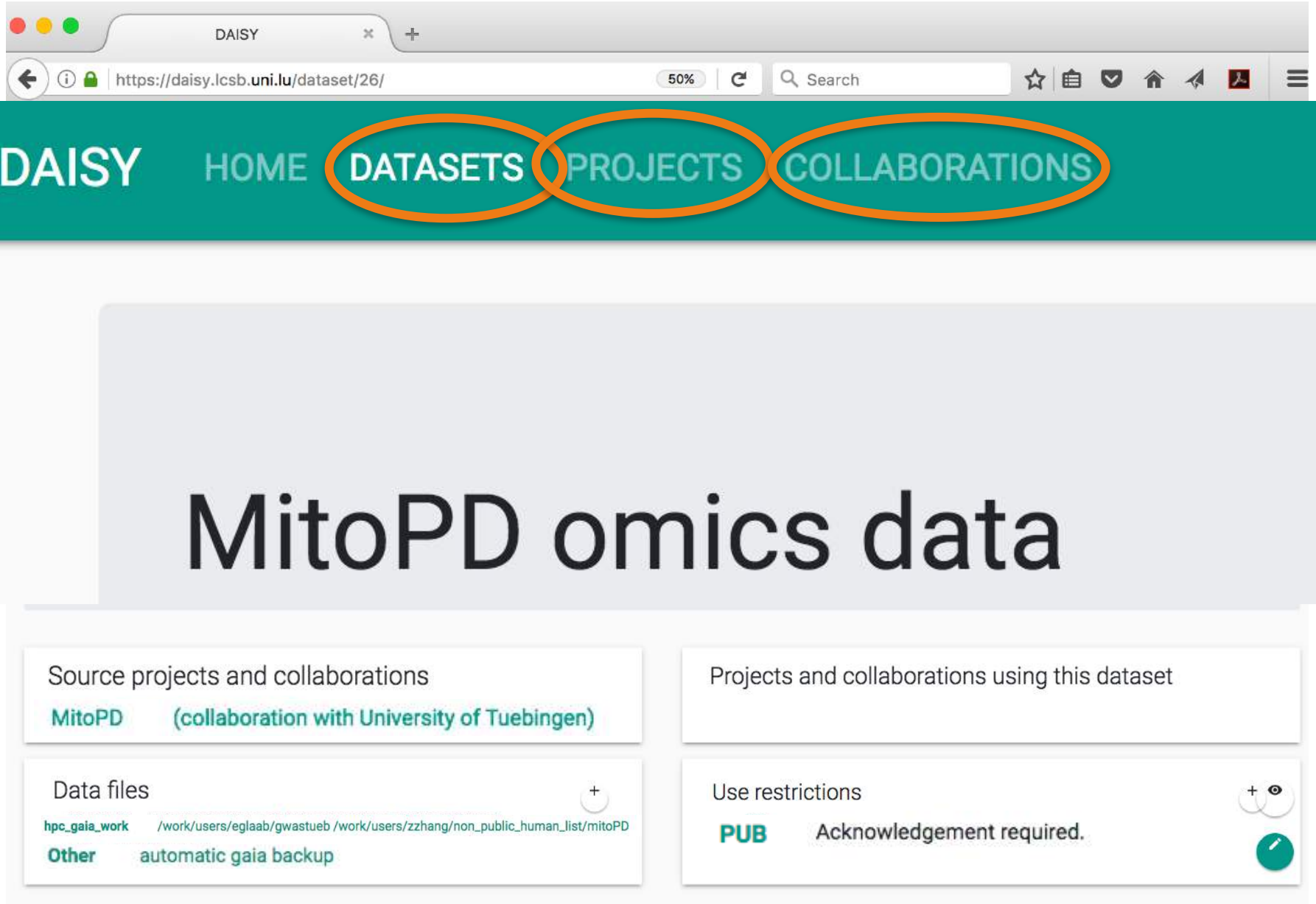
Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

DAISY – a GDPR registry for research data



DAISY – a GDPR registry for research data



DAISY: metadata about our data…

— What is collected about the datasets

- Responsibles
  - Internal principal investigator
  - Role as processor or controller
  - Where external controller: PI, legal representative, DPO
- Study type
  - E.g. Case / control, cross-sectional / longitudinal
- Confirmation of ethics approval for collection and sharing
- Data subjects
  - E.g. Minors, subjects not able to give consent
- Data types and size
- Retention information
- Use conditions
  - Processing of data for certain diseases / health research in general
  - Homogeneity / heterogeneity of consent
  - Other, e.g. data sharing

elixir LUXEMBOURG

DAISY: Processing information

— To become audit proof

- Reference to data locations
- Documentation
  - Legal and ethics documents (e.g. contracts, ethics approvals)
  - Data protection management plans (reference)
  - Data protection impact assessment (reference)
- Processing information
  - Projects (description, publications)
  - Legal basis of processing (e.g. consent, public interest, …)
  - Access rights with duration and purpose
  - Upload / download
  - Changes to data set (e.g. pseudonymisation) or metadata

DAISY: Additional features

— Support responsible processing

- Monitoring tool
  - Data storage duration
  - Ethics approval renewal
- Automated request tool
  - Data use expiry (request for renewal or confirmation of erasure)
  - Request information on publication on data
- Consent management
  - Match Access Request with Use Restrictions from Consent

Under development

→ **Automated features to comply with responsibility requirements**

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Accountability is more than transparency!

— How to document your compliance with the GDPR

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Accountability is more than transparency!

— How to document your compliance with the GDPR

Transparency

- Document what you do

Accountability

- Document why you believe what you do is enough

Data Protection Impact Assessment

- Assess if your information provision and processing will not pose a risk or violate the data subjects' rights and freedom
- Affects security measures, bridging situations, ambiguities (e.g. profiling), …
- Involve your Data Protection Officer

Audits

- Where documentation demonstrates a responsibly performed assessment
  → no fines to be expected

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

THANK YOU!

BioCore
Valentin Groues
Yohan Jarosz
Christophe Trefois
Sarah Peter
Kavita Rege
Wei Gu
Venkata Satagopam
Reinhard Schneider

ELIXIR-LU
Pinar Alper
Jacek Lebioda
Noua Toukourou

LCSB/UL
Sandrine Munoz (DPO)
Clemens Ostrowicz

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG