ENVRI
FAIR

GDPR in Context

ENVRIWEEK WP6 Training 20210204

Presenter: Keith G Jeffery (UKRI/BGS and EPOS-ERIC/ECO)

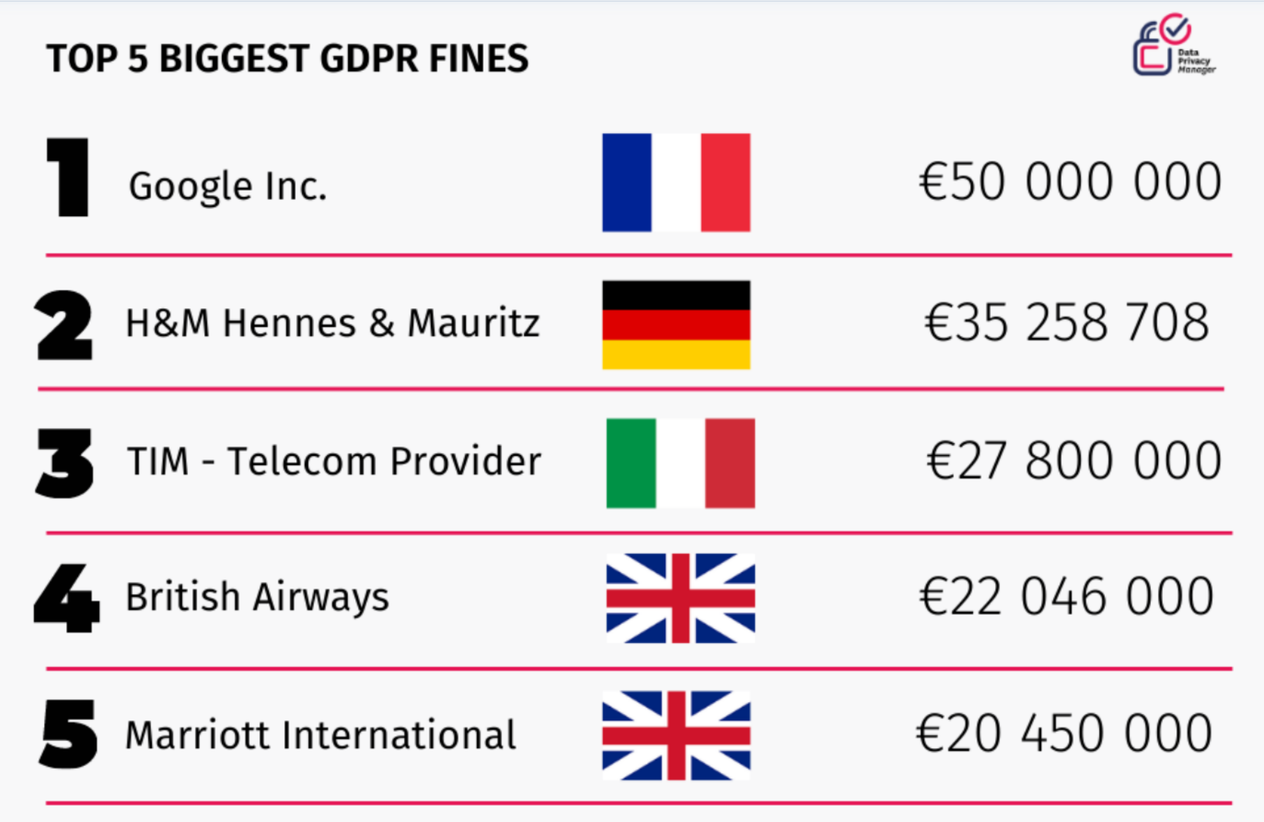
keith.jeffery@keithgjefferyconsultants.co.uk

CAVEAT: I am not a lawyer – take legal advice

ENVRI-FAIR has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 824068

CONTEXT

GDPR: What is all the fuss about?



TOP 5 BIGGEST GDPR FINES

1	Google Inc.	🇫🇷	€50 000 000
2	H&M Hennes & Mauritz	🇩🇪	€35 258 708
3	TIM - Telecom Provider	🇮🇹	€27 800 000
4	British Airways	🇬🇧	€22 046 000
5	Marriott International	🇬🇧	€20 450 000

GDPR: What is it?

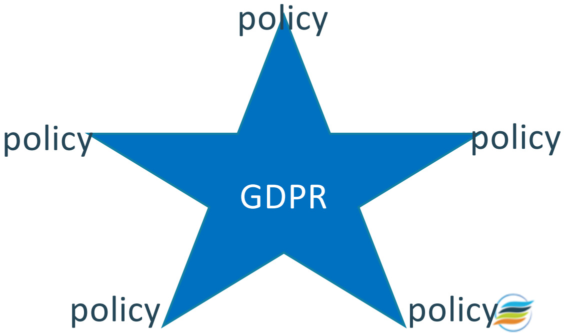
And why should we care?

- A law to protect the privacy rights of a data subject
    - Data subject = EU/EEA citizen (living)
    - Applies globally
- Responsibility is on the data controller
    - Organisation gathering and storing the personal data
- As we have seen, compliance is mandatory
    - Huge fines for infringements

Now I have your attention

Let us put it in context

- GDPR is an evolutionary descendant of various ‘data protection’ laws in various countries since ~1980
- So, many organisations have some percentage of the required documentation and procedures in place although GDPR is much more fierce
- GDPR does not stand alone, it depends on an integrated network of policies and their implementation
  - e.g. protecting personal data in an IT system implies security and authorisation
  - and tracing to discover breaches involve provenance



Context: Policy Areas Involved

- Asset Provision (data, data products, software, documentation, publications….)
- Asset Access (data, data products, software, documentation, publications….)
- Personal Data Protection (including GDPR)
- Security (including privacy and authorisation)
- Responsible Research and Innovation

- For each, the following need to be defined to proceed to IT implementation:
  - Issues
  - Actors and Skills
  - Potential solutions and Priorities (short-term and long-term)
  - Implementation Plan (which may include contracts)

Context: Needed Policies

RRI and Assets

- Responsible Research and Innovation (RRI)
  - Ethics
  - Governance
  - Societal engagement
  - Gender equality
  - Open Access
  - Education

RRI policy is concerned with persons (and their rights).

- Assets
  - Security
  - Privacy (includes GDPR)
  - Licensing
  - Authorisation (CRUDEL)
  - Curation (DMP)
  - Provenance

Asset policy is concerned with assets (and their management).

IT Implementation concerns the **relationship** between them.

We have to pull these together for **each of the policy areas** outlined previously

GDPR

GDPR

What is it?

- General Data Protection Regulation https://gdpr.eu/
- Applies to personal data on EU (EEA) data subjects anywhere
  - Personal data: relates to an identified or identifiable* person
  - Data subject: EU (EEA) citizen (living)
- Seven Principles
  - Lawfulness, fairness and transparency.
  - Purpose limitation.
  - Data minimisation.
  - Accuracy.
  - Storage limitation.
  - Integrity and confidentiality (security).
  - Accountability.

*

Apart from an ID or name, a person may be identified by one or more attributes of that person stored in a system.

Example:

HR System: an employee has attributes of qualification, **job title….**

Website: has **job title** and employee email address for contact purposes.

GDPR

The document

- It is a large document
- 9 chapters
- 91 articles
  - With quite a lot of cross-reference between articles
  - Not easy to understand

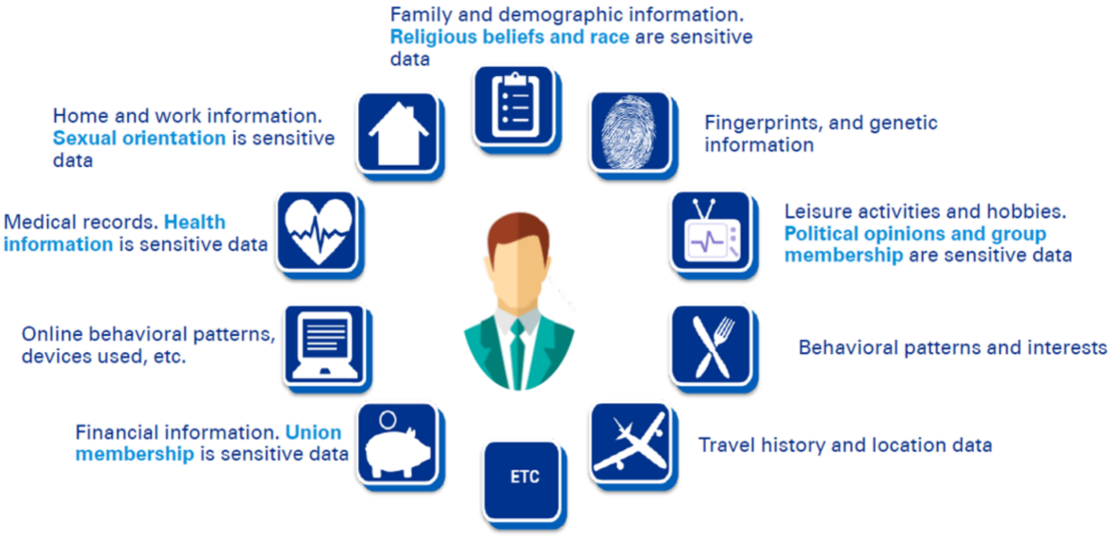
- Here I shall just outline the major provisions and their implications
- This is not a tutorial on all aspects of GDPR

CAVEAT: I am not a lawyer – take legal advice

Personal Data

some examples (not exhaustive)

- name
- phone number
- address / email address
- date of birth
- bank account
- passport number
- social media posts
- geotagging
- health records
- race
- religious and political opinion



Family and demographic information. **Religious beliefs and race** are sensitive data

Home and work information. **Sexual orientation** is sensitive data

Fingerprints, and genetic information

Medical records. **Health information** is sensitive data

Leisure activities and hobbies. **Political opinions and group membership** are sensitive data

Online behavioral patterns, devices used, etc.

Behavioral patterns and interests

Financial information. **Union membership** is sensitive data

Travel history and location data

(Informed) Consent

Should be obtained

- Obtaining consent simply means asking users for permission to process their data. Companies must explain their data collection and processing practices in clear and simple language, and then users must explicitly agree to them.
  - Privacy Policy
  - Asset Register
- These new standards of consent prohibit the use of sneaky pre-selected settings in apps, as well as pre-checked tick-boxes on websites.

ENVRI FAIR

Lawful Purposes

(else cannot process personal data)

- (a) If the data subject has given consent to the processing of his or her personal data;
- (b) To fulfil contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
- (c) To comply with a data controller's legal obligations;
- (d) To protect the vital interests of a data subject or another individual;
- (e) To perform a task in the public interest or in official authority;
- (f) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).

Lawful Purposes

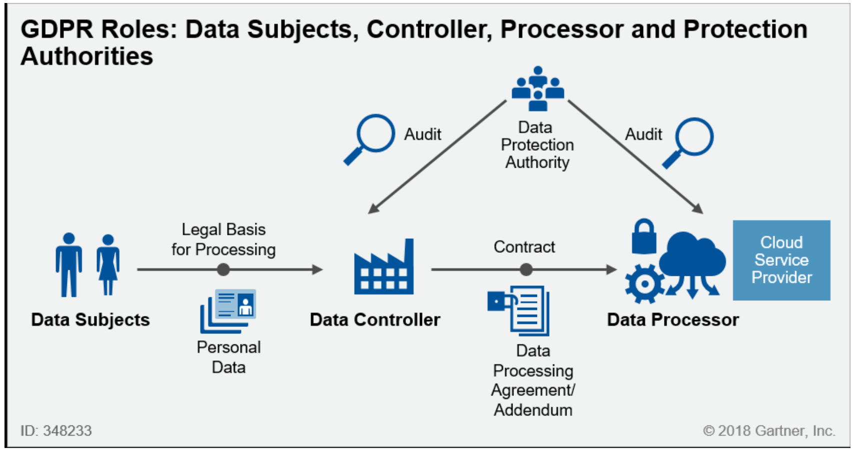
(else cannot process personal data)

- **(a) If the data subject has given consent to the processing of his or her personal data;**
- (b) To fulfil contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
- (c) To comply with a data controller's legal obligations;
- (d) To protect the vital interests of a data subject or another individual;
- (e) To perform a task in the public interest or in official authority;
- **(f) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).**

The Actors

And roles

- **Data Subject:** an EU/EEA Citizen whose personal data is stored
- **Data controller**: is any entity that gathers and stores data - for example, a business.
- **Data processor**: is who a data controller hires to process data on their behalf. Example: a payroll company.
- **Supervisory Authority**: Each country in the EU has its own supervisory authority. Like a data privacy sheriff, they enforce the GDPR in their region and hand out penalties.
- **DPO**: Companies and public bodies that process lots of data need to appoint a data protection officer (DPO) to handle all their GDPR activities and paperwork.



GDPR Roles: Data Subjects, Controller, Processor and Protection Authorities

ID: 348233

© 2018 Gartner, Inc.

Breach and Penalty

Severe Risk!

- Any incident that leads to personal data being **lost, stolen, destroyed, or changed** is considered a data breach. Unfortunately, breaches happen all the time.
- The GDPR threatens would-be violators with some severe penalties. To make sure companies handle your personal data in a legal, ethical way, the fines for noncompliance are:
- **Up to €20 million ($23 million) or 4% of annual global turnover.**
- Some big names have already been hit with these noncompliance fines:
  - **British Airways — $230 million (reduced to ~ $30m on appeal)**. The UK airline set the record for fines when the booking details of 500,000 customers were stolen in a cyberattack.
  - Marriott — **$123 million (reduced to ~$24m on appeal)**. After buying the Starwood Hotels group, Marriott failed to update an old system belonging to the group. This system was hacked, revealing information about 339 million guests.
  - **Google — $57 million**. Important information was hidden when users set up new Android phones, meaning they didn't know what data collection practices they were agreeing to. The Google GDPR fine shows even tech giants aren't immune to GDPR enforcement.

(GDPR) Privacy Policy

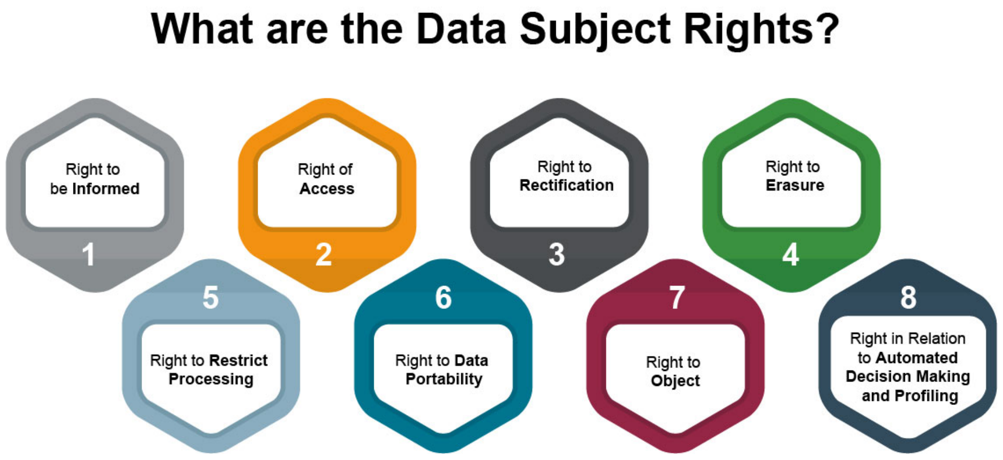
mandatory

- A data subject must be able to see the privacy policy of the organisation
- Privacy policies must:
  - Include contact details of the company and its representatives
  - Describe why the company is collecting the data
  - Say how long the information will be kept on file
  - Explain the rights users have
  - Be written in simple language
  - Name the recipients of the personal data (if the company shares data with another organization)
  - Include contact details for an EU-based representative and the DPO (if necessary)

Data Subject rights

What a person can do

- You are entitled to know exactly **how your data is collected and used**
- You can ask **what information has been collected** about you (without paying anything)
- If there are **mistakes in your data**, you can **request to have them corrected**
- You can **have your data deleted from records** (just in case you need to disappear!)
- You're allowed to **refuse data processing**, for example, marketing efforts



What are the Data Subject Rights?

1 Right to be Informed

2 Right of Access

3 Right to Rectification

4 Right to Erasure

5 Right to Restrict Processing

6 Right to Data Portability

7 Right to Object

8 Right in Relation to Automated Decision Making and Profiling

To answer data subject questions, a Record of Processing Activity (ROPA) is necessary (provenance)

Article 89 of GDPR

scientific or historical research purposes

- Derogation by Member States possible for Articles 15, 16, 18 and 21
    - 15: data subject right of access
    - 16: right to rectification
    - 18: right to restriction of processing
    - 21: right to object
- Where the interest of the data controller is balanced against the interest of the data subject (by the Supervisory Authority)
- Different Member States interpret differently – and some add additional constraints
- But nevertheless, the protection of personal data of the data subject is paramount.

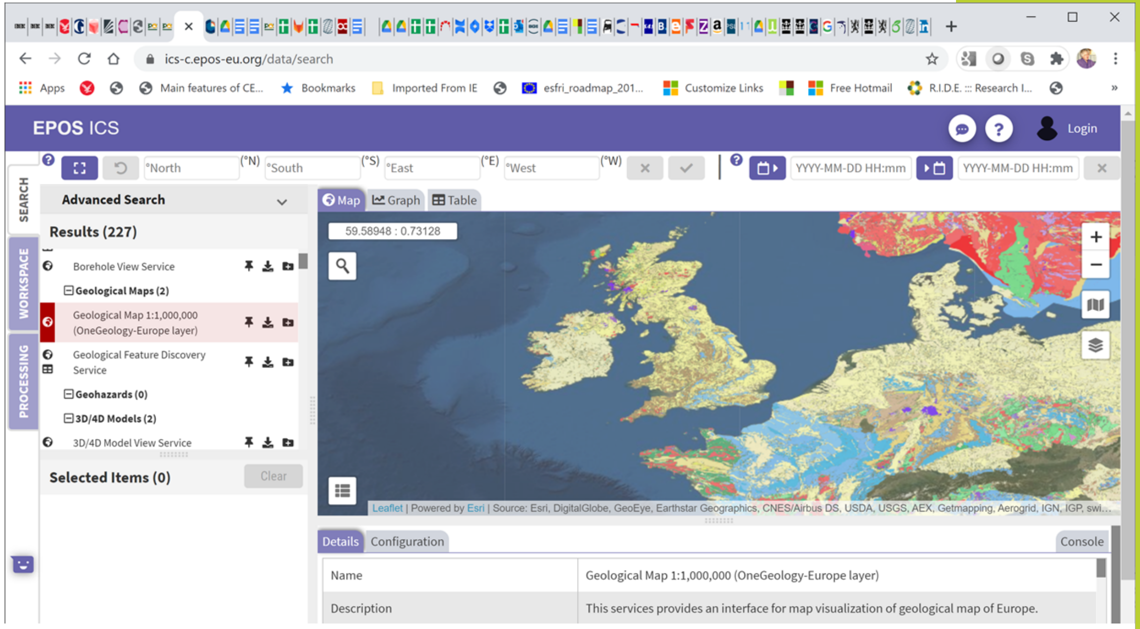
Article 89 of GDPR

scientific or historical research purposes

- Derogation by Member States possible for Articles 15, 16, 18 and 21
  - 15: data subject right of access
  - 16: right to rectification
  - 18: right to restriction of processing
  - 21: right to object
- Where the interest of the data controller is balanced against the interest of the data subject
- Different Member States interpret differently – and some add additional constaints
- But nevertheless, the protection of personal data of the data subject is paramount.

NOT AN ESCAPE ROUTE

EPOS ACTIVITY



Results (227)

- Borehole View Service
- Geological Maps (2)
  - Geological Map 1:1,000,000 (OneGeology-Europe layer)
  - Geological Feature Discovery Service
- Geohazards (0)
- 3D/4D Models (2)
  - 3D/4D Model View Service

Selected Items (0)

Name	Geological Map 1:1,000,000 (OneGeology-Europe layer)
Description	This services provides an interface for map visualization of geological map of Europe.

Version: 0.19.0 Commit hash: acbd6647 Commit date: Fri Nov 27 11:19:57 2020 +0000

What does this mean for EPOS? Or ENVRI

- GDPR
  - Define Data Controller and Data Processor(s)
  - Provide DPO (Provide a privacy policy and asset register for GDPR purposes)
  - On Website (portal) ensure users give informed consent (positive action)
    - This may be linked with conditions of use, disclaimers, consent to cookies etc.
  - Provide a mechanism for user complaint and management of personal data (data subject rights)
    - Automated or manual through e.g. DPO
- But also
  - Security to keep personal data protected from unauthorised access;
  - Authorisation mechanisms to control access to (personal) data;
    - We may also need to know who, when, from where, why and how which personal data was accessed - provenance

ENVRI FAIR

The Case of EPOS and GDPR

Work in progress

- A ‘pitch’ in IT development was set up and is being executed:
  - DPO appointed (Lucio Badiali);
    - Note his job is not just EPOS but wider including e.g. INGV personnel data
  - EPOS-ERIC is data controller represented by Executive Director (and DPO);
    - Asset suppliers in TCS also data controllers thus co-controllers for EPOS;
  - Data processors not yet defined fully – likely to be ICS-C hosting organisations and all asset suppliers in the TCS;
  - Draft privacy policy for GDPR produced;
  - Asset register compiled and being updated;
  - Much discussion leading to improved understanding of the implications of GDPR;
  - We have not yet specified exactly how the EPOS user interface should ensure consent (linked with conditions of use, disclaimers, cookie consent etc.)
- In parallel work on a ‘pitch’ on authorisation is progressing with TCS participation;

ENVRI FAIR

Current Problems

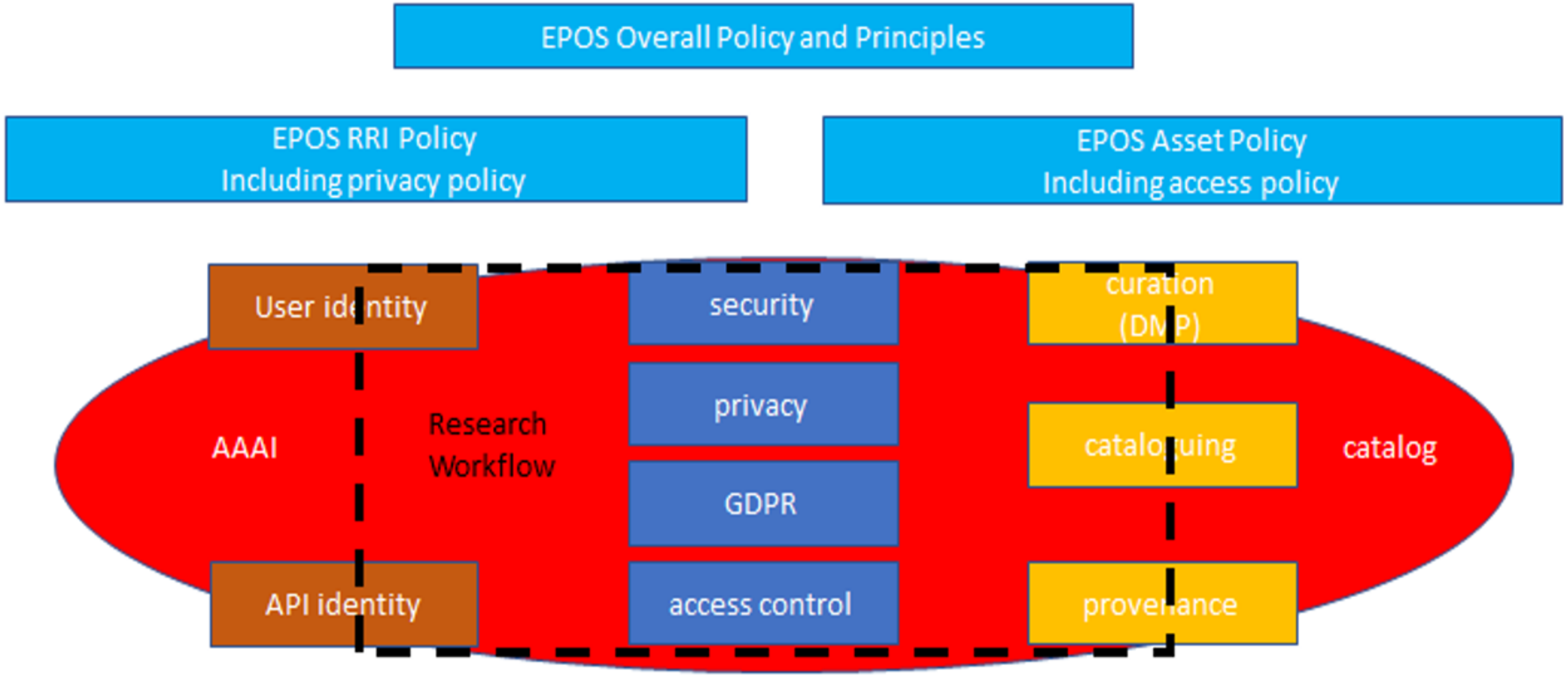
Likely changes

- There is little case law yet on GDPR so neither is everything is clear nor even fixed fully
  - Things may change quickly
  - Derogations to Member States
- At the moment personal data of data subjects cannot be moved (including being seen) outside of the EU/EEA
  - EPOS cannot interoperate with e.g. Americas, Asia/Pacific or Africa unless we remove or anonymise personal data (e.g. asset owner)
  - This may change if the EU accredits as adequate GDPR-like laws in third countries or International Organisations
  - Or if EPOS-ERIC and the organisation(s) involved have an appropriate legal contract covering the issues (approved by the Supervisory Authority)
  - It may be over-ruled by data subject consent (especially if second and third bullets are honoured) [https://www.securityprivacybytes.com/2019/01/does-the-gdpr-allow-for-the-use-of-consent-for-the-international-transfer-of-data/]

A general word of warning

- Do NOT make policy without considering the IT implementation
  - Example: BREXIT: there are many affected systems and there is no way the systems were/are ready
- Do NOT build IT systems without considering the policy
  - Example: Twitter: effect of ‘fake news’ and use by a President to bypass usual (moderated) communication channels

How it all links together and to IT



EPOS Overall Policy and Principles

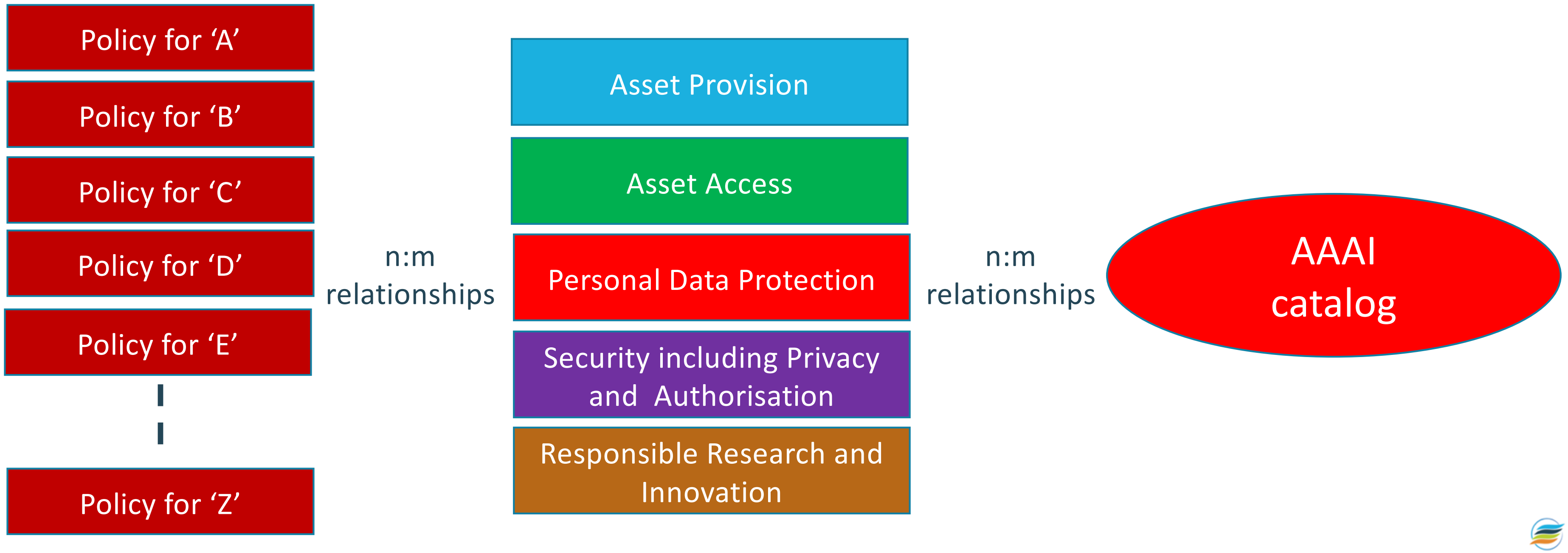
EPOS RRI Policy
Including privacy policy

EPOS Asset Policy
Including access policy

ENVRI FAIR

Policies, Policy Areas, IT Systems

How it relates



Policy for ‘A’

Policy for ‘B’

Policy for ‘C’

Policy for ‘D’

Policy for ‘E’

Policy for ‘Z’

n:m relationships

Asset Provision

Asset Access

Personal Data Protection

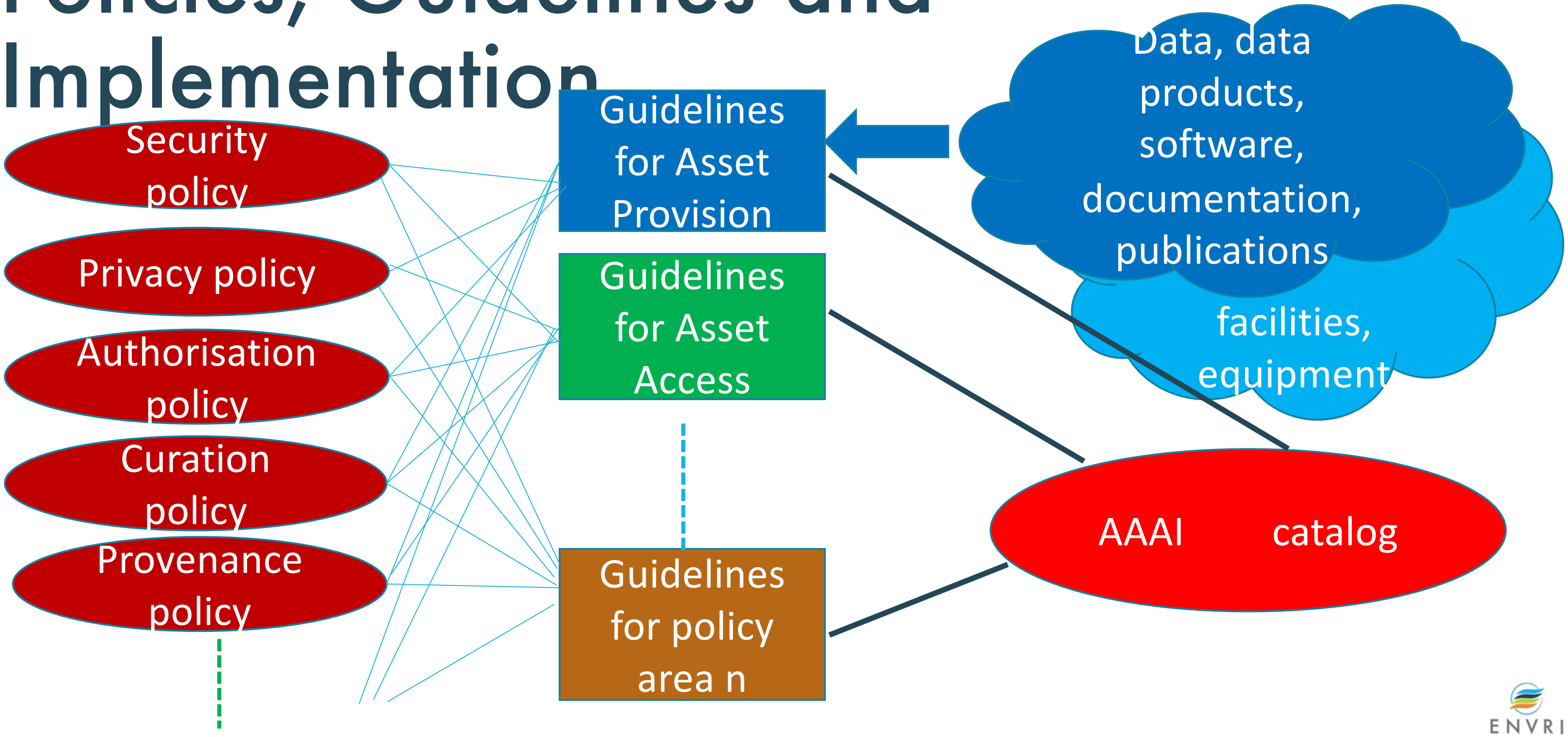
Security including Privacy and Authorisation

Responsible Research and Innovation

n:m relationships

AAAI catalog

Policies, Guidelines and Implementation



Security policy
Privacy policy
Authorisation policy
Curation policy
Provenance policy
Guidelines for Asset Provision
Guidelines for Asset Access
Guidelines for policy area n
Data, data products, software, documentation, publications
facilities, equipment
AAAI
catalog

ENVRI FAIR

Concluding Remarks on EPOS

- The next three slides are:
- 1,2: the conclusions of the Policy Group in EPOS as presented to the Services Coordination Committee and the Executive Committee;
- 3: the action given to the Policy Group;

- Although EPOS-Specific the points are – I believe – applicable generally to ENVRI

CONCLUSIONS 1-3

The first and most obvious conclusion is that the development and maintenance of EPOS policies and their support in the IT system is a huge undertaking but necessary because of law and accepted best practice.
⇒ **EPOS-ERIC governance and management bodies need to be informed of this**

The second conclusion is that EPOS needs to have a clear understanding of the policies required (by law or governance), their relationships (dependencies and constraints) and the implications for the behaviour of both persons and the IT system.
⇒ **an introductory document should be prepared for the governance and management bodies of EPOS**

The third conclusion is that policies should be co-designed by appropriate experts in the policy area (e.g. human rights law or licensing) and appropriate IT experts.
⇒ **this ensures that the IT support for policies is appropriate**

CONCLUSIONS 4-5

The fourth conclusion is that EPOS needs a roadmap to prioritise policy formulation, development and implementation (including the IT support) involving relevant stakeholders and subject to appropriate governance taking into account importance, urgency and dependencies of the policies.

⇒ **this is the pathway to achieving appropriate implemented policies so that EPOS-ERIC behaves correctly within law and best practice and is appropriately governanced**

The fifth conclusion is that policy work can be both endless and resource-intensive. The development of policies, their documentation and their implementation in IT requires appropriate project management.

⇒ **this relates to the fourth conclusion: EPOS-ERIC has to decide the balance appropriate between minimal acceptable implementation and full implementation and then resource appropriately for the planned timescale**

ACTION

EPOS Services Coordination Committee and Executive Board

- Team to continue the work
  - Bringing in additional expertise as needed
- Incline to minimal compliance rather than full implementation
  - While ensuring all legal aspects are covered

ADVICE FOR ENVRI

I have been asked to add this section to the presentation.

I do so with some trepidation and remembering Benjamin Franklin:
“Wise men don’t need advice. Fools won’t take it”.

CAVEAT: I am not a lawyer – take legal advice

ADVICE

For ENVRI

- There are two aspects: ENVRI as a whole (ENVRI-Hub) and RIs in ENVRI
  - ENVRI is not a ‘legal person’ (i.e. an established organisation) which complicates things;
  - RIs in ENVRI usually have some sort of legal personality (e.g. an ERIC or an association)

CAVEAT: I am not a lawyer – take legal advice

Minimal Compliance

What you might get away with

- Declare data controller(s), data processor(s), DPO
- Declare a privacy policy and asset register
- Implement a consent button at the GUI (next to link to the policy and register)
  - It is not clear how this would be done with an API: assumed some GUI (human interaction) somewhere leads to the API
- Have a Record of Processing Activity (ROPA) (to answer requests)
- Have DPO deal manually with any data subject requests
- Ensure security and authorisation implementation protects assets that may have personal data - on an identified or identifiable person - from cyberattack

CAVEAT: I am not a lawyer – take legal advice

ENVRI FAIR

Ideal Compliance: Policies and Guidelines

All of the minimal compliance desiderata but also:

- Have a full set of policies covering
  - Assets and their management
  - Persons (RRI)

(see next slide – list is the same for implementation)

CAVEAT: I am not a lawyer – take legal advice

Have a full set of guidelines covering:

Asset Provision (data, data products, software, documentation, publications….)

Asset Access (data, data products, software, documentation, publications….)

Personal Data Protection (including GDPR)

Security (including privacy and authorisation)

Responsible Research and Innovation

ENVRI FAIR

Ideal Compliance: Implementation

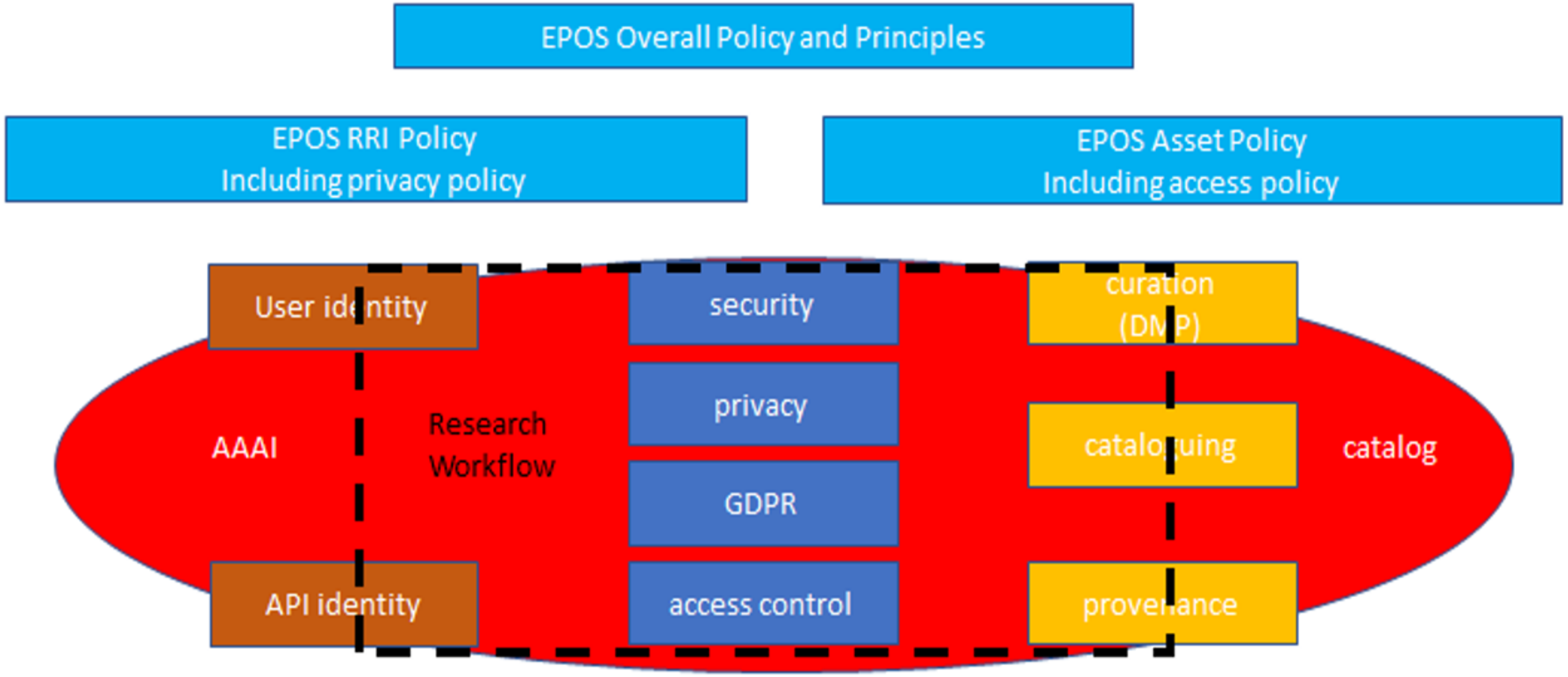
Have an implementation integrating

- Ethics
- Governance
- Societal engagement
- Gender equality
- Open Access
- Education
- Security
- Privacy (includes GDPR)
- Licensing
- Authorisation
- Curation
- Provenance

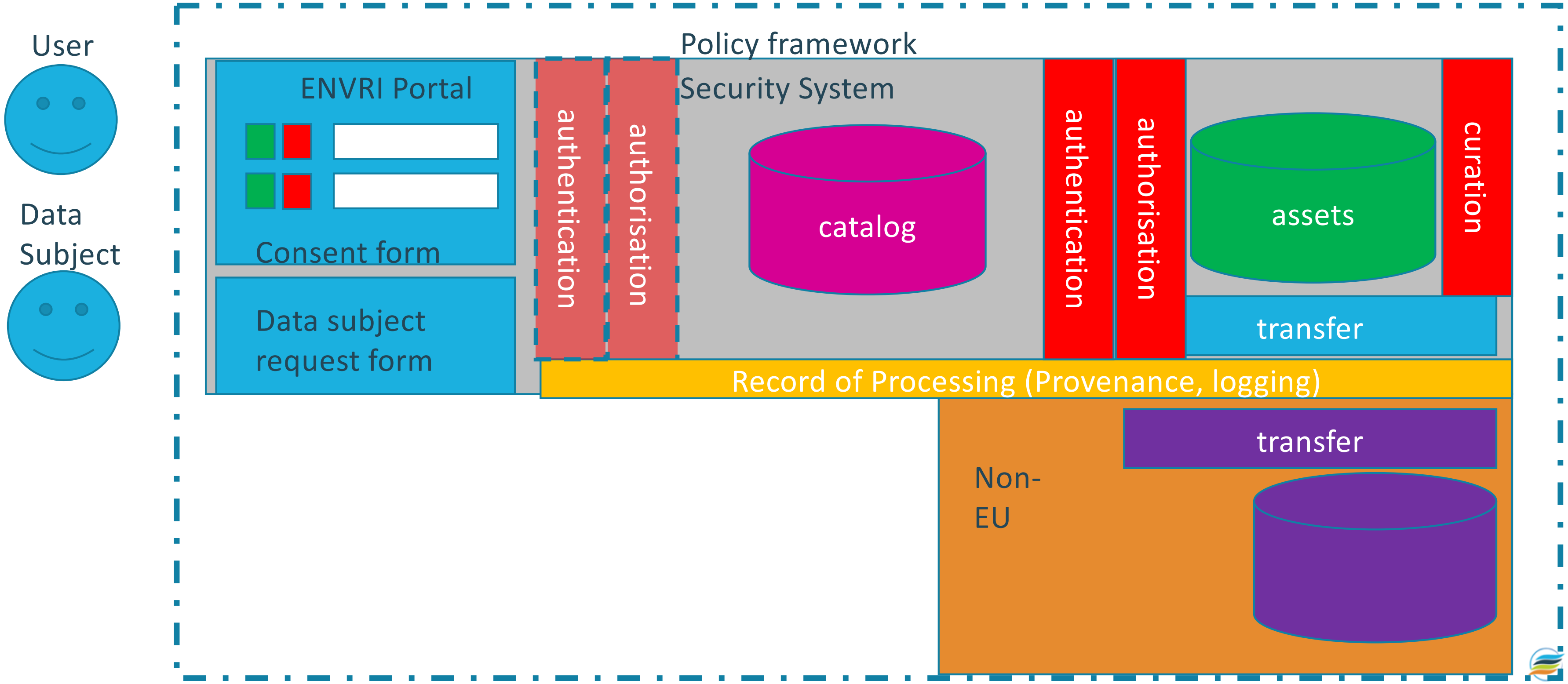
Consistently across the policy areas
With ‘self-service’ data subject access

CAVEAT: I am not a lawyer – take legal advice

Leads to something like this



What You Need: IT Systems



User

Data Subject

Policy framework

ENVRI Portal

Consent form

Data subject request form

authentication

authorisation

Security System

catalog

authentication

authorisation

assets

curation

transfer

Record of Processing (Provenance, logging)

Non-EU

transfer

BACK MATTER

Reading Material

- The official website with the law
  - https://gdpr.eu/
- A fairly easy-to read synopsis
  - https://termly.io/resources/articles/gdpr-for-dummies/
- A useful overview
  - https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
- About Article 89
  - https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/
- The website our (Italian) DPO uses for advice
  - https://ico.org.uk/

Acknowledgements

The EPOS Policy Team

- Chris Luton BGS-Legal:
  - Providing the initial privacy policy and asset register, liability disclaimer
- Lucio Badiali ECO-DPO:
  - Ensuring alignment with state of EPOS-ERIC
- Daniela Mercurio ECO-policy:
  - Aligning terms and conditions
- Lorenzo Fenoglio ECO-IT:
  - Aligning licensing and cookies

From an initial group with Keith Jeffery (BGS and ECO) working on legal disclaimers and GDPR

From an initial group with Daniele Bailo (ECO) and Carmela (Lilli) Freda (ECO) working on EPOS policies

ENVRI
FAIR

envri.eu/envri-fair

@envri_fair

company/envri-fair

facebook.com/ENVRIcomm