ENVRI-FAIR WP4 Third Policy Workshop

Helen Glaves, UKRI/BGS

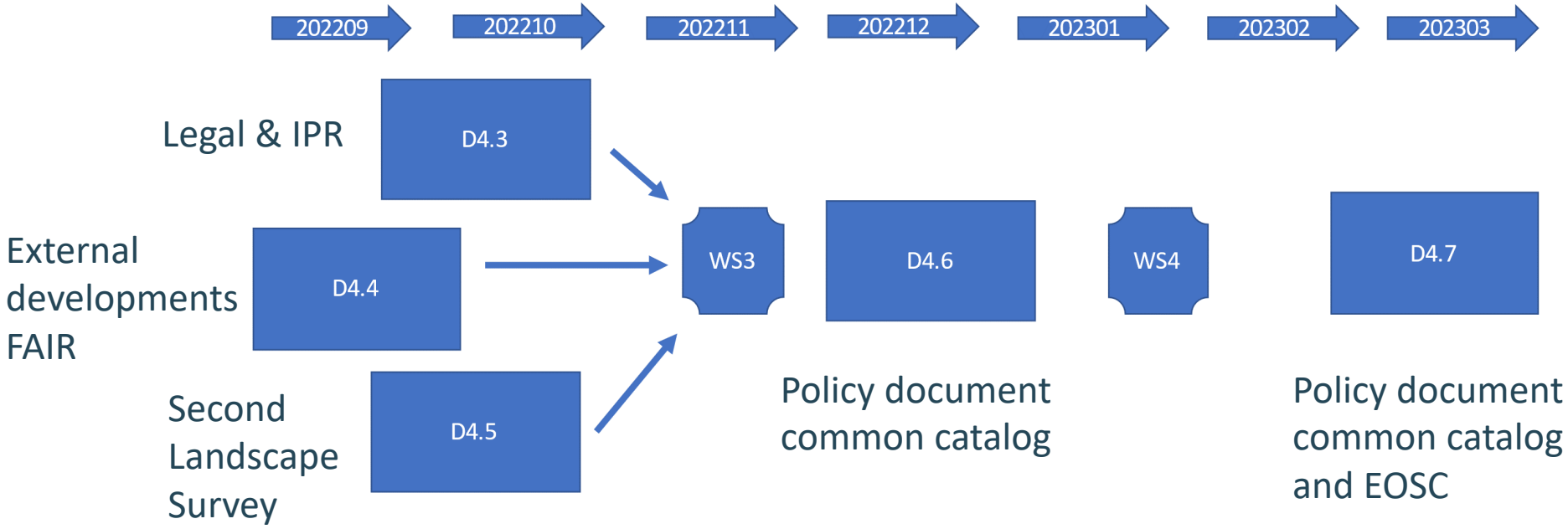
Keith G Jeffery, UKRI/BGS

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

Agenda

- 1. Introduction (Helen Glaves)
- 2. summary of workshop 1
- 3. summary of workshop 2
- 4. creating policies from policy statements
- 5. creating guidelines
- 6. IT implementation
- 7. the three key documents related to policy
- 8. Policy related to ENVRI Catalog
- 9. Discussion and conclusion (Helen Glaves)

WP4: Where are we?



Workshop 1

A Framework for Policy

- 1. Why policies needed?
  - Legal (with implications of liability)
  - Governance (ensure activities are done correctly)
- Constraints and drivers for policies in ENVRI and ENVRI RIs
  - EOSC: has its own policies, guidelines and conditions
  - FAIR: the FORCE11 FAIR principles
  - ENVRI-Hub: the requirememts of the architecture
- Framework for policy/governance
  - Policies : the organisational intent
  - Guidelines (best practice): the way this intent is achieved
  - IT Implementations (technology): how the governance is supported by IT
- ENVRI Policy Model

Missing from Workshop 1

- The need for Policy in ENVRI RIs and ENVRI-Hub
  - for interoperability, FAIR and EOSC
- There is no point having technical interoperability
  - Conversion to common canonical rich metadata format describing digital assets;
  - Mechanisms for discovery, contextualization
  - Mechanisms for download
  - Mechanisms for workflow composition / orchestration / deployment
- If the technical infrastructure cannot be activated due to
  - Legal obstructions (e.g. GDPR)
  - Terms and Conditions of use of digital assets and access to them
  - Licensing (dealing with rights and obligations of provider and user)

Pause

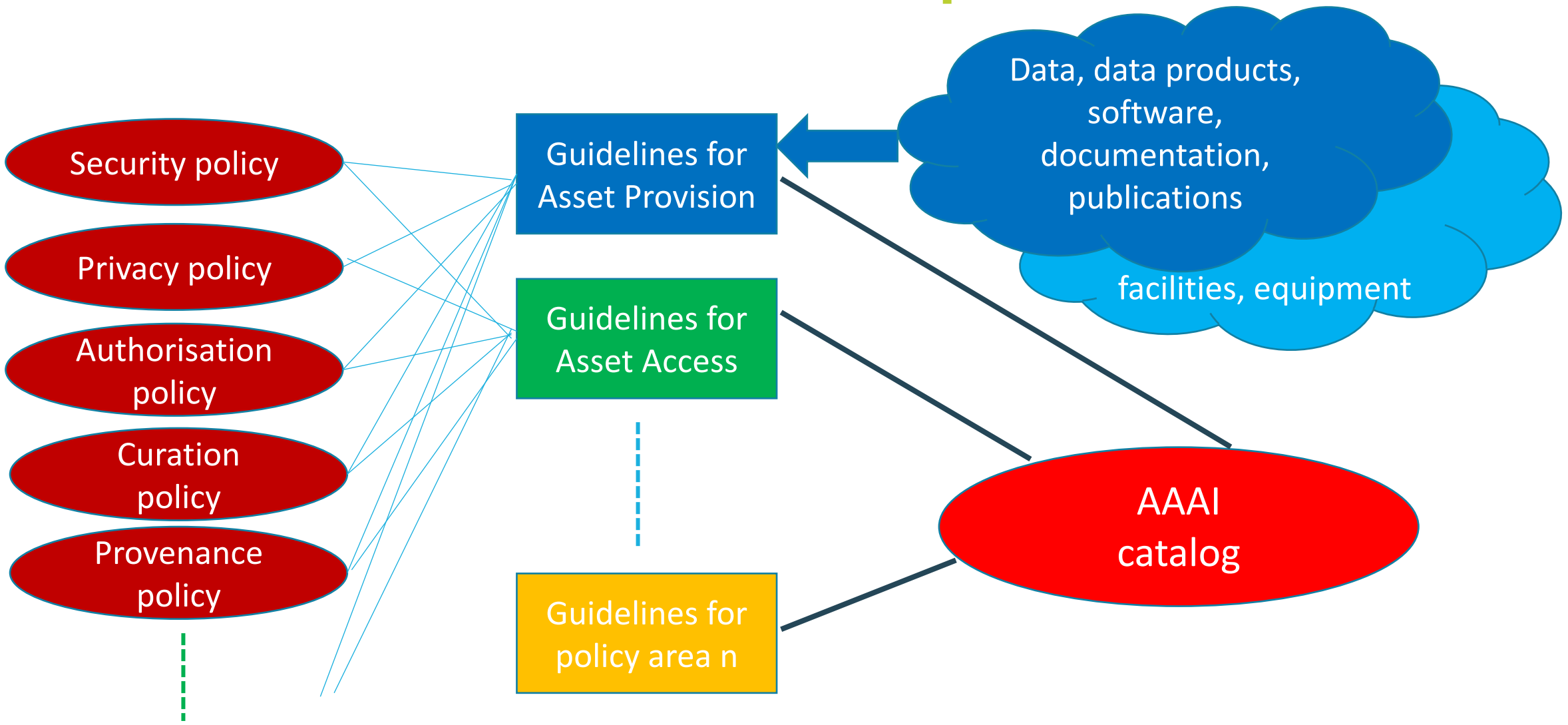
- Audience comments on Workshop 1 (from questionnaire and now)
  - Did the workshop assist in your RI?
  - Did it cause any changes in approach to policy?
  - Did it provide what you needed to reconsider policy in your RI?

Workshop 2

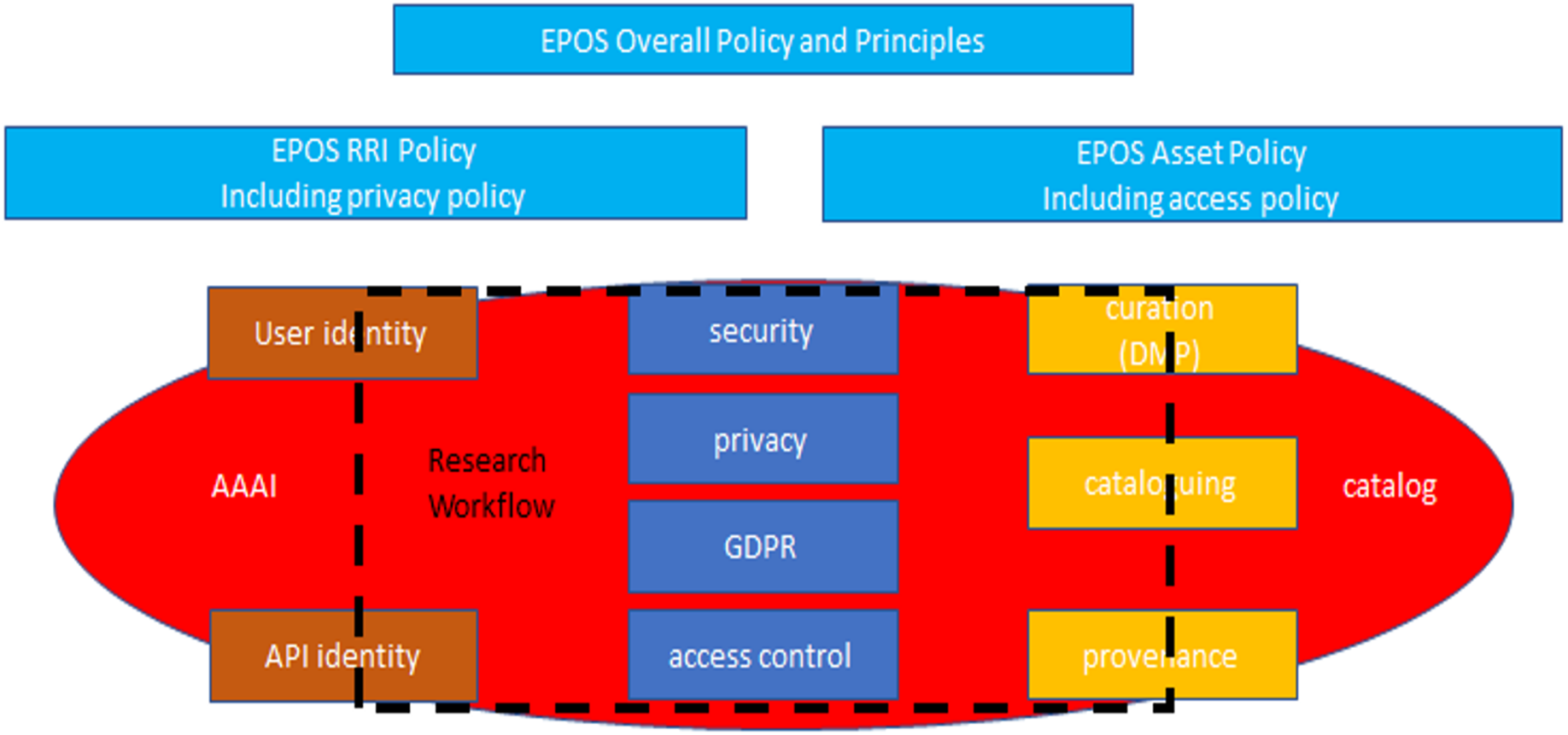
Requirements, Policy Statements

- 1. Framework agreed
- 2. Group discussions on policy statements
- 3. Relationship of policies/guidelines/IT implementation agreed (next slide)
- 4. Relationship to IT: EPOS example (slide after next) discussed

Policies, Guidelines and Implementation



How it all links together (EPOS example)



What is Missing from the Framework?

(1) There is no mention of cookies;

(2) Liability is mentioned (under sustainability) but its relationship to Terms and Conditions (T&C) generally is unclear, although mentioned with respect to the T&C for conditions of use of EOSC, namely SROP7, SROP28;

(3) More generally, T&C is not mentioned in the context of policies;

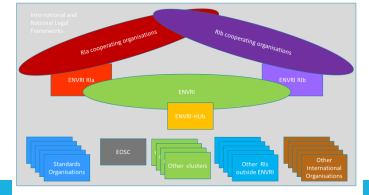
(4) The General Data Protection Regulation (GDPR) is also only mentioned in the context of EOSC conditions namely SROP23 yet has much wider application (and legal consequences) throughout ENVRI related to a policy on personal privacy;

(5) The e-Privacy Directive of the European Commission is not mentioned;

(6) There is no mention of Responsible Research and Innovation (RRI);

(7) There is no mention of physical security, disaster recovery and related policies

- These deficiencies are serious, pervasive and also have potential consequences if not addressed. Thus, the policy environment for ENVRI has been re-drawn to take account of the wider context (a few slides ahead)



Missing after Workshop 2

- Despite the landscape survey (D4.2)
  - A clear picture for each RI of
    - Where we are now
    - The roadmap for the future
- Agreement on and understanding of the list of missing items in the previous slide
- A method to get from a hypothetical framework
  - To usable policy documents
    - For each RI
    - For ENVRI-Hub
  - That are congruent so that technical interoperability is supported by policy interoperability
- A method to get from policies to guidelines to IT implementation
  - Throughout ENVRI and interfacing to external systems such as EOSC

The Way Forward

"We have to acknowledge the progress we made, but understand that we still have a long way to go. That things are better, but still not good enough."

Barack Obama

Pause

- Audience comments on Workshop 2 (from questionnaire and now)
  - Did the workshop assist in your RI?
  - Did it cause any changes in approach to policy?
  - Did it provide what you needed to reconsider policy in your RI?
  - Was the framework useful?
  - Could you use the policy statements in your own RI?
  - Did it influence your approach to integrating your RI with ENVRI-Hub?

Pause

- Workshop 3 what do you expect? (from questionnaire and now)
  - To confirm that my RI has the appropriate policies in place for the RI?
  - To identify policies that are missing or incomplete at my RI?
  - To contribute to the definition of policies for the ENVRI-Hub catalog?

Workshop 3

Today

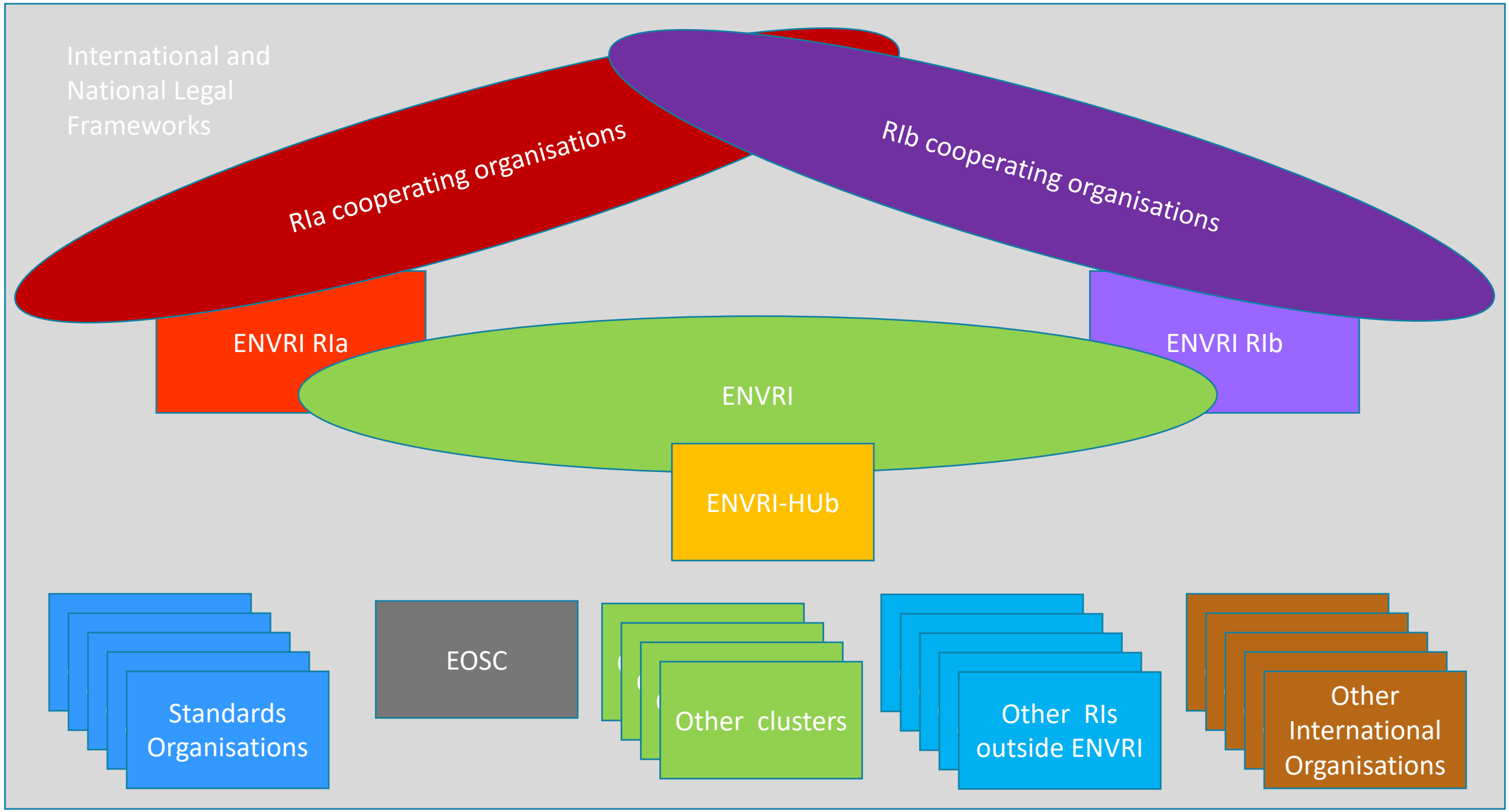
- Creating policies from policy statements
- Creating guidelines (introduction)
- IT implementation (introduction)
- The three key documents related to policy
- Policy related to ENVRI Catalog
- Discussion and conclusion

Taking into account the deficiencies discovered in analysis of the framework and its policy statements, and incorporating those aspects of policy

- This is based on the work done by the Policy Group within EPOS which is used as an example.

1. the overall landscape for ENVRI (next slide)
2. which policies are out of scope (following 2 slides)
3. which policies are in scope (slide after those 3)
4. Policies: some EPOS Examples (following slides)

Creating Policies from Policy Statements


International and National Legal Frameworks
RIa cooperating organisations
RIb cooperating organisations
ENVRI RIa
ENVRI RIb
ENVRI
ENVRI-HUb
Standards Organisations
EOSC
Other clusters
Other RIs outside ENVRI
Other International Organisations

EPOS Policies out of scope (for now)

#1

- **1. Applicable Legal Jurisdiction**
- ***2. Personal (Human rights)***
  - Equality of opportunity / respect
  - Racial (race, colour, nationality); gender; religious/belief
  - Health and Safety
  - Code of Conduct
  - Education & Training
- **3. Business**
  - Mission, Principles
  - Purpose, general principles
  - Stakeholders
  - Customer community, supplier community, external communities (customer and supplier)
  - Objectives
  - Targets to be achieved; timeline; resources
  - Contracts and Agreements
  - Ownership

•Responsibility (management)
•Open competition / tendering
•Contract
•MoU
•Financial Management
•Financial Policy
•Responsibility and delegated authoroty
•Financial reporting
•Audit
•Intellectual property (assets)
•IP Policy (relates to licensing and citation/acknowledgement)
•Branding
•Risk
•Risk, Severity, Probability, Risk Factor, Mitigation

ENVRI FAIR

EPOS Policies out of scope (for now)

#2

- **4 Environment**
  - Reduced energy consumption / carbon footprint
- **5 External Activities**
  - Business
  - Responsibility (management)
  - Code of Conduct
  - Cooperative

6 Communication

- General External Policy
  - Branding, channels, information, feedback
- Customer community policy
  - Branding, channels, information, feedback
- RI community policy
  - Branding, channels, information, feedback

ENVRI FAIR

Policies in scope (proposed)

- Physical Security
- Disaster Recovery
- Privacy
- Authentication
- Authorisation
- Terms and Conditions
- Cookies
- Metadata
- Identifiers
- Licensing
- Curation
- Provenance
- Quality Assurance
- Acknowledgement
- Responsible Research and Innovation (RRI)

Note: there is always some intersection between some of the policies. For example, RRI includes open science which in turn relates to policies on metadata and others. Similarly, licensing relates to authorisation. Terms and conditions relates to many other policies. Those in red were needed urgently for legal reasons and do not follow the current EPOS template.

Pause

- Audience comments on list of policies in scope
  - Are these relevant for your RI?
  - Do you have them documented already?
  - Are they relevant for ENVRI-Hub?
  - Are they useful in integrating your RI with ENVRI-Hub?

Policies: Some Existing Policies using Licensing as an example

Atmosphere subdomain

ICOS licence

- **You are free to:**
- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material for any purpose, even commercially
- **Under the following terms:**
- **Attribution** — You must give appropriate credit, provide a link to the licence, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use
- **No additional restrictions** — You may not apply legal terms or technological measures that legally restrict others from doing anything the licence permits
- The licensor cannot revoke these freedoms as long as you follow the licence terms.
- (the actual licence is CC BY 4.0)

Ocean subdomain

SeaDatanet Licence

- The Licensor grants to the Licensee a non-exclusive and non-transferable license to retrieve and use data sets and products from the SeaDatanet service in accordance with this license.
- 2. Retrieval, by electronic download, and the use of Data Sets is free of charge, unless otherwise stipulated.
- 3. Regardless of whether the data are quality controlled or not, SeaDataNet and the data source do not accept any liability for the correctness and/or appropriate interpretation of the data. Interpretation should follow scientific rules and is always the user?s responsibility. Correct and appropriate data interpretation is solely the responsibility of data users.
- 4. Users must acknowledge data sources. It is not ethical to publish data without proper attribution or co-authorship. Any person making substantial use of data must communicate with the data source prior to publication, and should possibly consider the data source(s) for co-authorship of published results.
- 5. Data Users should not give to third parties any SeaDataNet data or product without prior consent from the source Data Centre.
- 6. Data Users must respect any and all restrictions on the use or reproduction of data. The use or reproduction of data for commercial purpose might require prior written permission from the data source.
- 7. Users are requested to inform SeaDataNet of any problems encountered with SeaDataNet-provided data. A timely and easy-to-use feedback procedure is available (sdn-userdesk@seadatanet.org), aimed at correcting data at the data source. This feedback will increase the quality of the data.

ENVRI FAIR

Solid Earth subdomain

EPOS Licensing

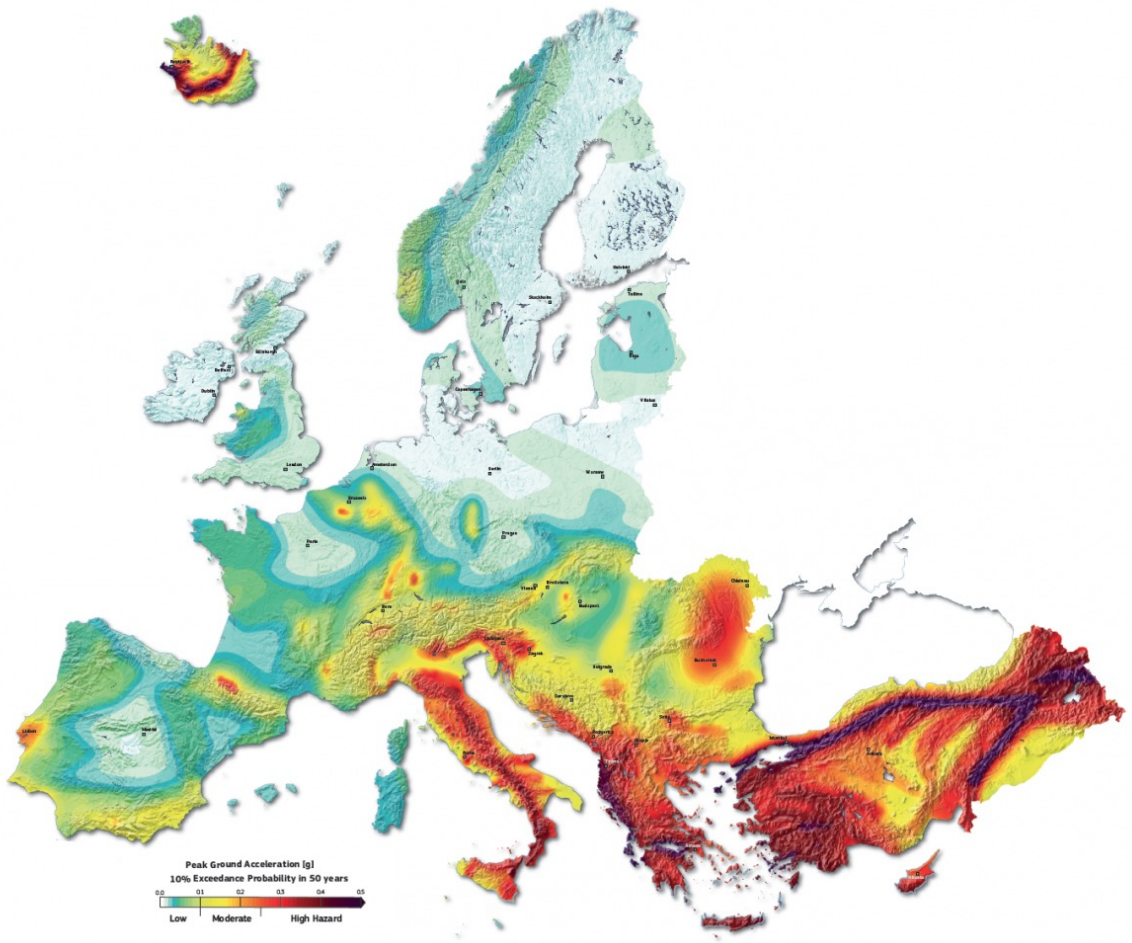
- 5.2.1 DDSS licensing
- To facilitate effective rights/ownership management, EPOS shall only redistribute DDSS after 2021 to which a licence has been applied/affixed. EPOS aims to grant one default licence set for EPOS-managed DDSS, Creative Commons 4.0. Within the Creative Commons permitted licence scheme, two licences will be adopted, CC:BY and CC:BY:NC. SP(s) have the possibility, provided it is agreed with Suppliers, where no licence type is identified to apply/affix a licence on unlicensed data on the Supplier's behalf.
- 5.2.2 Metadata licensing
- To ensure the widest dissemination and publicity for EPOS managed DDSS, it is essential that metadata are easily and freely accessible at any time, with as few restrictions as possible. In order to achieve this, Suppliers will be encouraged to affix open licenses, preferably Creative Commons 4.0 CC:BY, to their metadata. The machine-readable version of this licence will allow User(s) to identify the relevant datasets through search engines licences filters.

ENVRI FAIR

Biosphere subdomain

Lifewatch in ECOPortal Terms

- **Use of Semantic Resources** In general, any semantic resource submitted to EcoPortal will be freely available for public use, unless the content is marked as private (in which case it will not be shared via EcoPortal) or the Licensing Attribute is defined in the metadata for that ontology. If an end user re-uses semantic resources with a Licensing attribute defined, EcoPortal considers it the end user's responsibility to acquire appropriate licenses for that re-use. Only the submitter of the semantic resource (either an individual or organization that is the authorized owner of the resource content or a designated representative) will be able to modify it or submit new versions, except when semantic resources which are configured for automatic ingest/update by EcoPortal are changed at their source location on the web by anyone with that authority. All submitted semantic resource content will be indexed and made available for search and visualization to all users of EcoPortal worldwide.
- (more detailed T&Cs at https://www.lifewatch.eu/terms-and-conditions/)



Policies: Some EPOS Examples of current work

← Earthquake Map Europe

EPOS Policy Renewal

- EPOS has policies on data, privacy, terms and conditions and cookies.
- There are some intersections, and the data policy includes elements of policy relating to e.g. licensing
- EPOS decided to do a revision of policy documents:
  - Having modular, atomic policies that can be combined into one cohesive document;
  - Examples are licensing, authorization (which are clearly related)
- EPOS created a policy group to do the work
  - Policies proposed by the group and then discussed by representatives of the 10 sub-domains of EPOS
  - Progressive refinement

EPOS Policy Template Document

- Why? Do we have a policy and what does it cover
- Who? – target
- Who? – Authors
- When? Is the policy applicable (version, dates)
- Where? Is the policy applicable (countries, regions)
- What?... Is the policy
- How? Is the policy implemented (i.e. relates to which guidelines)

Physical Security

- Why? Do we have a policy and what does it cover
- The purpose of the Physical Security Policy is to:
  - establish the rules for granting, control, monitoring, and removal of physical access to office premises;
  - identify sensitive areas within the organization;
  - to define and restrict access to the same.
- What? Is the policy
- The Physical Security policy protects and preserves information, physical assets, and human assets.
- How? Is the policy implemented (i.e. relates to which guidelines)

- Physical access to the server rooms/areas shall completely be controlled and servers shall be kept in the server racks under lock and key.
- Access to the servers shall be restricted only to designated Systems and Operations Personnel. Besides them, if any other person wants to work on the servers from the development area then he/she shall be able to connect to the servers only through Remote Desktop Connection with a Restricted User Account.
- Critical backup media shall be kept in a fireproof off-site location in a vault.

Disaster Recovery

- Why? Do we have a policy and what does it cover
- The purpose of this policy is to ensure that IT resource investments made by EPOS are protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of disaster recovery plans. Furthermore, that IT resource investments made by EPOS are protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of disaster recovery plans.
- What? Is the policy
- The Disaster recovery policy is to respond to a major incident or disaster by implementing a plan to restore EPOS mission critical functions.
- How? Is the policy implemented (i.e. relates to which guidelines)

- Plans for disaster recovery shall be developed by IT management.
- Disaster recovery plans shall be updated at least annually and following any significant changes to computing or telecommunications environment of EPOS.
- IT staff of EPOS shall be trained to execute the disaster recovery plan.
- Annual testing of the disaster recovery plan shall be done.
- An external auditor shall audit disaster recovery plans.

Authentication

- Why? Do we have a policy and what does it cover

- A security/authentication policy is needed to define the governance of persons accessing or providing EPOS assets within the EPOS Delivery Framework (EDF) and to record their usage of assets if/when required. In particular, authentication ensures that a person is who they claim to be. It is part of the security policy, the other parts being authorisation, physical security and disaster recovery.

- What? Is the policy

- The security/authentication policy is that all users and suppliers of EPOS assets must be authenticated at the appropriate stage of access. EPOS will implement appropriate authentication wherever required either from a supplier or user perspective. EPOS will use any information about users gained through authentication mechanisms according to the privacy policy.

- How? Is the policy implemented (i.e. relates to which guidelines)

- The security/authentication policy relates to the security guideline. The policies related to this guideline are security (including authentication, authorisation, physical security and disaster recovery), privacy, licensing.
- The policy is implemented by a check of a person's identity with respect to EPOS declared by a responsible person.
- The implementation requires that mechanisms are in place to allow users to authenticate themselves using EPOS approved Identity Providers (IdPs). (the approved IdPs are listed in the guidelines).
- The implementation (guidelines) includes checking that the user is not barred from accessing EPOS due to any legal restrictions.

ENVRI FAIR

Authorisation

- Why? Do we have a policy and what does it cover

- A security/authorisation policy is needed to define the governance of persons supplying or accessing EPOS assets within the EPOS Delivery Framework (EDF). In particular, authorisation defines the assets (or asset classes) a person may access, in what role (e.g. user, manager), in what modality (**C**reate; **R**ead; **U**pdate; **D**elete; **E**xecute; down**L**oad) and within what time period. Authorisation balances the rights of the user (such as open access) against the rights associated with the asset (such as a licence). A prerequisite is user authentication. It is part of the security policy, the other parts being authentication, physical security and disaster recovery.

- What? Is the policy

- The security/authorisation policy is that all users of EPOS assets must be authorised to access assets in the appropriate role, modality, time period either explicitly (permissions linked to authenticated identity) or by default (where the asset is not so protected). The latter is so-called anonymous use, although the user identity (authentication) and relevant attributes may be utilised for recording usage.

- How? Is the policy implemented (i.e. relates to which guidelines)

- The authorisation policy relates to the security guideline. The policies related to this guideline are security (including authentication, authorisation, physical security and disaster recovery), privacy, licensing.
- The policy is implemented by a record of a person's rights to access EPOS assets in the appropriate role, modality, time period declared by a responsible person.
- The implementation requires that, for any EPOS asset that requires authorisation a process exists for a defined, authorised person to declare that a given user has a right to access a specific EPOS asset in the appropriate role, modality, time period, and that the person (user) is registered at a node of the EPOS delivery framework with appropriate details in the associated Identify Provider (IdP).

ENVRI FAIR

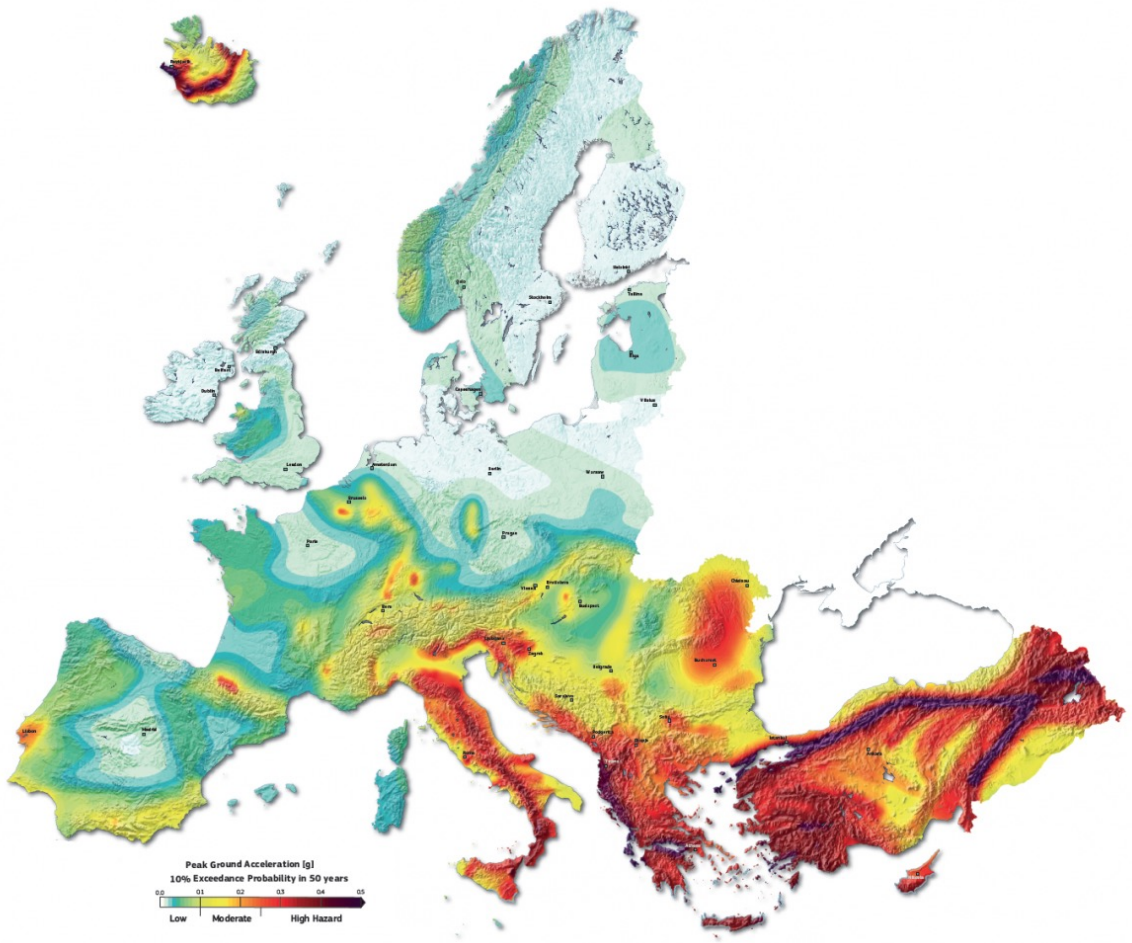
Metadata

- Why? Do we have a policy and what does it cover
- A metadata policy is needed to align with the FAIR principles: metadata provide the information to utilise digital assets.
- What? Is the policy
- The metadata policy is that all providers of EPOS assets (asset suppliers within the TCS and the ICS-C system) must ensure rich metadata describing each digital asset at the appropriate level of granularity. Rich metadata is metadata sufficient for the purpose: discovery, contextualisation (relevance/quality), access (appropriate information to control access including licensing), (re-)use (including any changeable parameters to control the asset). The metadata must be in the current EPOS standard for the metadata catalog (CERIF) to be recognised as an asset within the EPOS Delivery Framework.
- How? Is the policy implemented (i.e. relates to which guidelines)
- The metadata policy relates to the asset provision and asset access guidelines. The policies related to these guidelines – and to metadata - are security (including authentication, authorisation, physical security and disaster recovery), privacy, licensing, citation/acknowledgement and curation.
- The policy is realised by providing appropriate procedures to assign rich metadata to an asset. It relates also to the pre-existing EPOS Data Policy.

ENVRI FAIR

Pause

- Audience comments on policy template and examples
  - Do you like the template (allows policy documents to be compared and checked easily)?
  - Are the examples useful?



Guidelines: Some EPOS Examples of current work

← Earthquake Map Europe

Guidelines

Asset Provision Data,
Asset Provision Services,
Asset Provision Software,
Asset Provision Documentation
Asset Provision Publication
Asset Access Data
Asset Access Services
Asset Access Software
Asset Access Documentation
Asset Access Publication
Personal Data Privacy
Security: Physical Security
Security: Disaster Recovery
Security: Authentication
Security: Authorisation
RRI

ENVRI FAIR

EPOS Guidelines Template

- Why? Do we have a guideline and what does it cover
- Explain here the purpose of the guideline and list the policies to which it relates and which influence it.

- Who? – target of the guideline
- The audience

- Who? – Authors of the guideline
- The authors

- When? Is the guideline applicable (version, dates)
- Version n yyyymmdd

- Where? Is the guideline applicable (countries, regions)
- Geographical regions

What? Is the Guideline

Here explain the guideline and its purpose e.g. in guideline for asset provision something like:
"The guideline for asset provision consists of a checklist of actions that should be taken before an asset is accepted into the EPOS delivery framework. This list includes (a) ensuring the metadata is provided in accordance with the current EPOS-DCAT_AP standard; (b) ensuring ownership is recorded in the metadata; (c) ensuring management is recorded in the metadata; (d) ensuring licensing is recorded in the metadata. Reference should be made to the pre-existing EPOS Data Policy."

How? Is the Guideline implemented in desk instructions and in IT systems

Here document the procedures associated with implementing the guideline e.g. in guideline for asset provision something like:
"(a) Ensure relevant staff have been trained in the metadata ingestion pipeline; (b) utilise the procedure to convert metadata from local asset provider standard to EPOS-DCAT-AP; (c) validate the metadata using SHACL within the metadata pipeline; (d) upload the metadata using the metadata pipeline process; (e) check the metadata in the CERIF catalog is correct by running standard queries to ensure the metadata is all recorded and available."

ENVRI FAIR

Guideline Security

- Why? Do we have a guideline and what does it cover

- The security guideline addresses the challenges related to the protection of EPOS assets from physical or cyber attack.
- It relates to policies on:

1. Physical security and disaster recovery (to prevent damage to assets)
2. Security: Authentication (to ensure legitimate use of the EPOS system and its assets)
3. Security: Authorisation (to protect against unauthorised use of assets)
4. Curation: to ensure availability of the asset
5. Provenance: to track activity associated with the asset allowing – with any system logs – audit of activity and potentially recovery of state after an attack

Guideline Security

What? Is the Guideline

The major threats to the availability of EPOS assets are as follows:

1. Physical damage to the assets at ICS-C, ICS-D, asset supplier servers, sensor networks and laboratory equipment servers, national or regional portals, TCS portals and other nodes caused by natural disaster, act of war or protest, criminal forced entry;
2. Digital damage to the assets at ICS-C, ICS-D, asset supplier servers, sensor networks and laboratory equipment servers, national or regional portals, TCS portals and other nodes caused by unauthorised access;
3. Denial of service to access assets at ICS-C, ICS-D, asset supplier servers, sensor networks and laboratory equipment servers, national or regional portals, TCS portals and other nodes caused by cyberattack, failure of utilities (electricity, water, air conditioning, specialised gases)

The guidelines to mitigate the threats are as follows:

1.
    1. Replicated offsite backup system;
    2. Physical access control including entry to restricted areas only with validated identity and appropriate physical barriers;
2.
    1. Authentication and authorisation implemented;
    2. Robust authentication based on password or biometrics;
    3. Authorisation based on well-defined rules linked to (i) licensing of the asset; (ii) role and status of the user (or software on behalf of the user);
    4. Users educated in cyberthreats such as phishing and methods to mitigate;
3.
    1. A multi-layer firewall to prevent unauthorised access;
    2. Replicated provision of utilities;

The actions to recover the assets and the delivery framework are as follows:

1.
    1. Invocation of offsite backup system (ideally with automated network switching);
    2. Reviewing the security arrangements at the affected node and implementing the guidelines;
2.
    1. Restore asset based on log files/provenance information (i.e. rollback/recovery through transactions or compensating transactions) and local backup;
    2. Restore asset using offsite backup and roll forward based on log files/provenance information to restore state;
    3. Through curation and provenance information check for replicates/fragments of the assets and if necessary take restorative action (a) or (b);
3.
    1. Switch to any replicated offsite system;
    2. Restore utilities if necessary;
    3. Restore firewall (if necessary strengthened);
    4. Restore service utilising local or offsite backups of affected assets;

Guideline Security

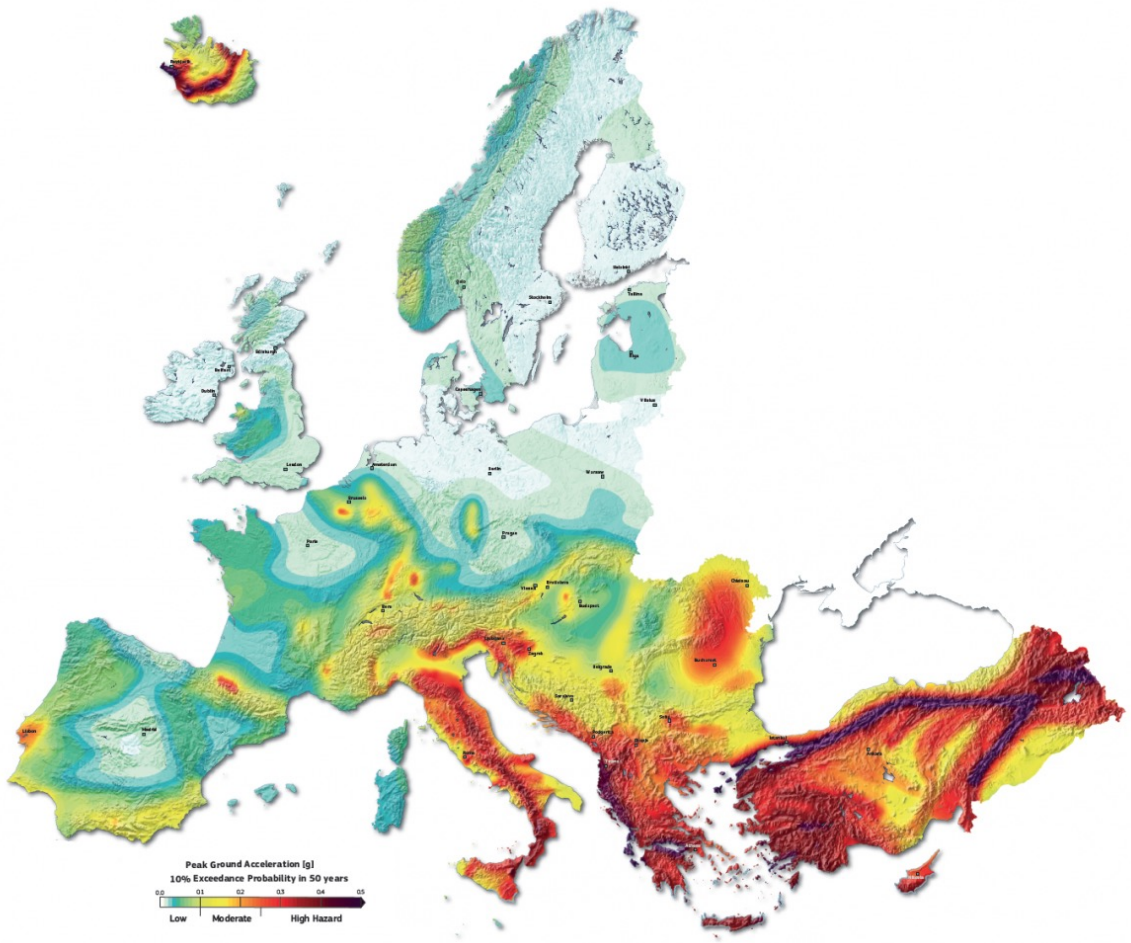
- How? Is the Guideline implemented in desk instructions and in IT systems

- The guideline is implemented through clear procedural instructions and associated IT implementation. These cover the following:

1. Replicated offsite system;
2. Physical barriers and personal identity systems for access;
3. Onsite and offsite backup arrangements to assist in restoration;
4. Replicated utilities;
5. Multilayer firewall;
6. Authentication;
7. Authorisation;
8. Log files, curation and provenance to assist in audit and restoration;
9. User education in cyberattack and mitigations;

Pause

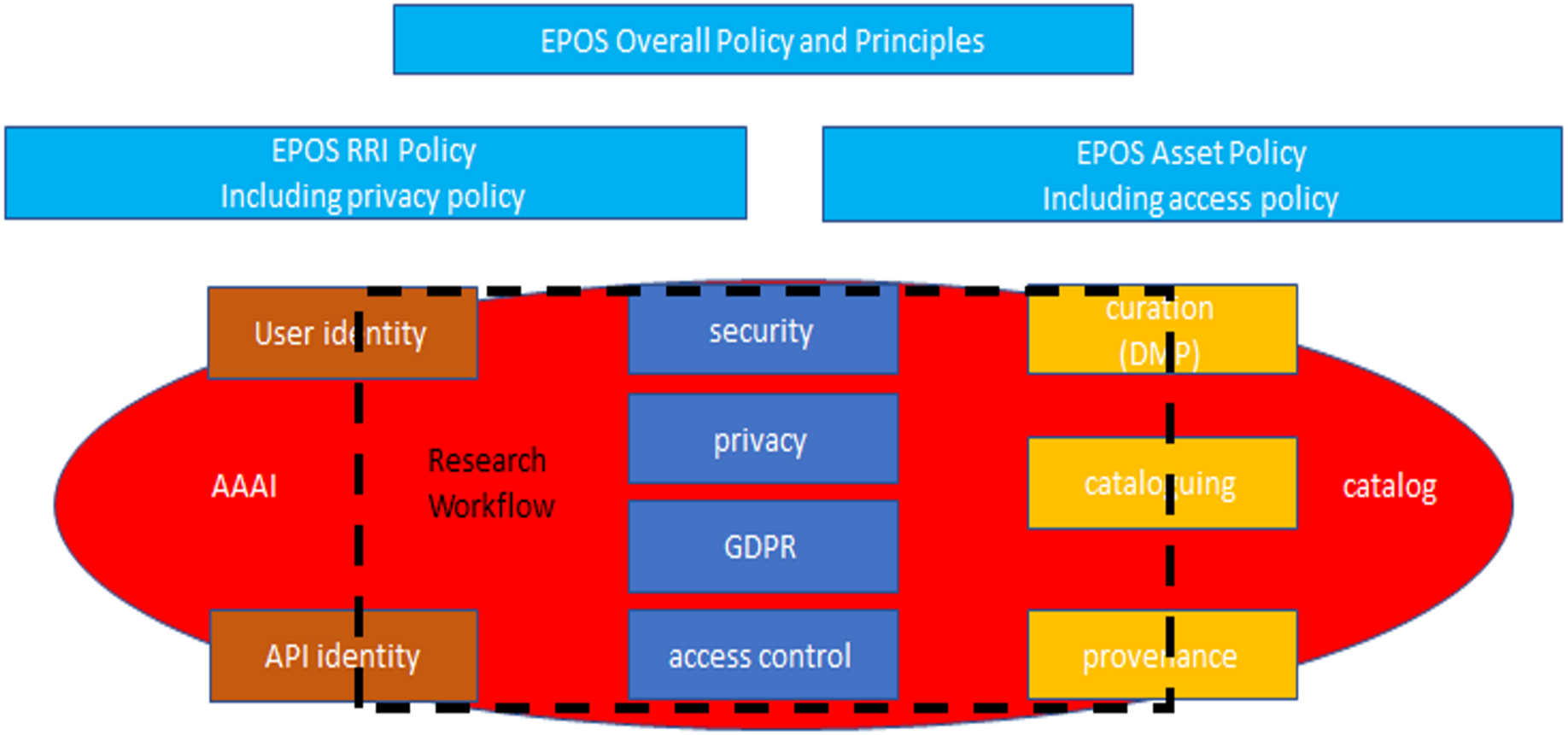
- Audience comments on guideline template and examples
  - Do you like the template (allows guidelines documents to be compared and checked easily)?
  - Is the example useful?



IT Implementation: EPOS Example

← Earthquake Map Europe

How it all links together (EPOS example)



The Three Special Ones

- Privacy
- Terms and Conditions
- Cookies

These are special because they are documenting to what the user has to consent to use the system

User Consent

EPOS POLICIES

☐ **I consent to Terms and Conditions**

Here you will find the conditions under which you use the EPOS ICS-C portal. This includes acceptable use and liability disclaimer. If you do not consent to such use of the portal, further access to the portal is denied.

☐ **I understand and acknowledge the Privacy Policy document**

The Privacy policy explains how EPOS-ERIC manages and protects personal data, particularly in the sense of GDPR (General Data Protection Regulation). If you do not consent to such use of your personal data, further access to the portal is denied.

○ **COOKIES**

Websites utilise cookies to store certain information. EPOS-ERIC ICS-C portal uses cookies only to monitor performance anonymously, information used in improving the portal. You may choose to allow these cookies or not. Either choice does not prevent use of the portal.

ENVRI FAIR

Privacy (relates to GDPR)

https://www.epos-eu.org/epos-eric-privacy-policy

Information about us and this policy

- Policy
- Data Controller
- DPO contact details

Information we may collect about you

- Categories of personal data
  - How is your personal data collected?
  - How we use your personal data
  - Communications
  - Cookies
  - International transfers
  - Data security
  - Data retention

Your legal rights

Glossary

Terms and Conditions

https://www.epos-eu.org/sites/default/files/Terms_and_Conditions.pdf

Your responsibility

- By using our Portal, you accept these terms.
- You must keep your account details safe

We may change the Portal

- We may make changes to these terms
- We may make changes to our Portal
- We may suspend or withdraw our Portal
- We may transfer this agreement to someone else

Use of material on Portal

- How you may use material on our Portal....
- Permitted uses
- Do not rely on information on our Portal
- We are not responsible for Portals we link to
- Rules about linking to our Portal.

Breach of these Terms

Which country's laws apply to any disputes

EPOS ICS-C Terms and Conditions If you disagree with any part of these terms and conditions, please do not use our website.

By accepting these Terms and Conditions, you enter into an agreement with EPOS ERIC, an international organisation with registered offices at EPOS ERIC, in Via di Vigna Murata 605 - 00143 Rome Italy - FISCAL CODE 96409510581 - VAT N° IT15152381008 ("EPOS ERIC "), made up by the contents of these Terms, in order to regulate the user's access and use of the Portal.

Cookies

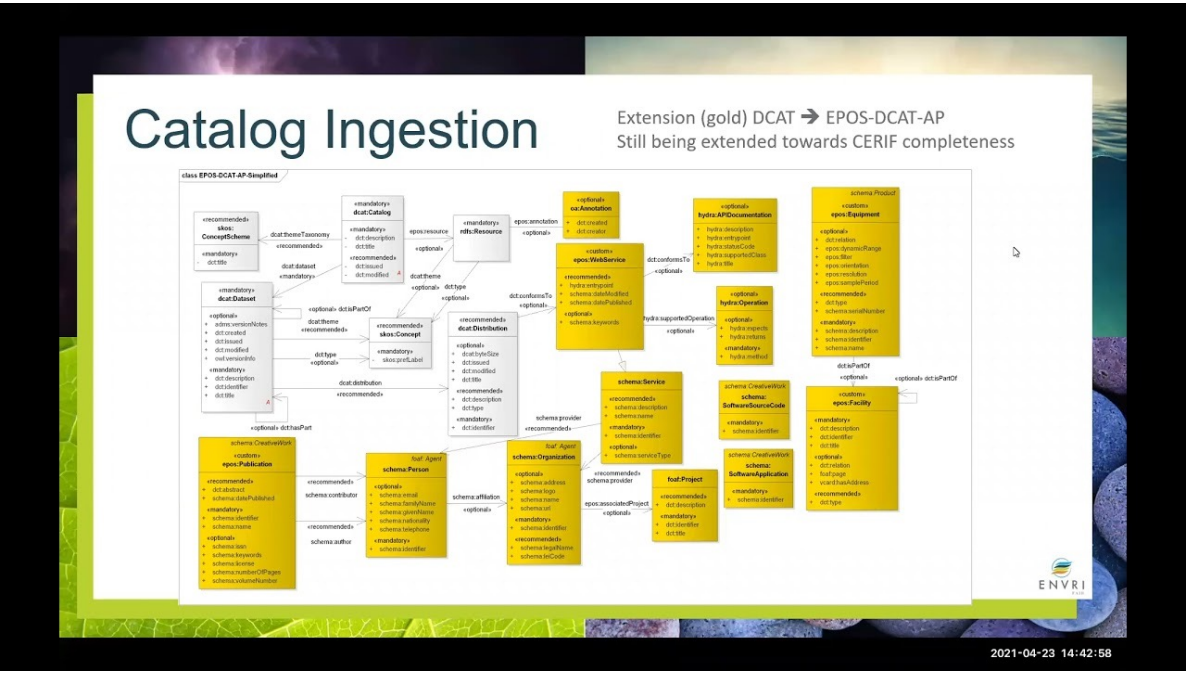
https://www.epos-eu.org/sites/default/files/Cookie_Policy.pdf

- What are cookies?
- Why we use cookies?
- Are all cookies the same?
- How to manage cookies using our website To give you the best experience on the cookie management side, we classify cookies

Pause

- Audience comments on the three special ones
  - Do you have these and the consent pop-up already implemented?
  - Are the EPOS examples useful?

Policies Related to ENVRI Catalog



Policies Related to ENVRI Catalog

- Most policies concerned with: (a) the rights and responsibilities of humans; (b) the rights and protection of digital assets; (c) the interaction between (a) and (b)

- The purposes of the catalog related to policy:

(a) Curation: Availability of digital assets) and FAIR

(b) Security (protection of digital assets)

(c) Privacy (personal data)

(d) Authorisation of access (protection of digital assets and recording for provenance, citation and usage: requires authentication)

(e) Licensing (protection of digital assets: name of licence and authorisation parameters)

(f) Provenance: (tracking of asset evolution and use for privacy)

(g) Citation (tracking for accreditation of researcher)

(h) Usage tracking (for statistics indicating popularity and usage of personal data)

The catalog

(a) Metadata: representation of policy elements: syntax and semantics, integrity

(b) API

(c) GUI / query interface

How well does the catalog support policy?

(a) Sufficient information in the metadata, consistency

(b) Sufficient processes/procedures (IT implementation) utilising the metadata to support/enforce policy as defined in guidelines

The catalog provides a mechanism for TECHNICAL interoperability.

However, we also need interoperability of IT implementations based on conforming policies and guidelines

POLICY Interoperation

How do we achieve this in ENVRI: ENVRI-Hub / RI –RI / interface to EOSC

- Terms and Conditions
- Cookies
- Privacy
- Authentication
- Authorisation
- Metadata (FAIR)
  - Curation
  - Provenance
- Licensing
  - Acknowledgement
  - Citation

T&C: Liability, respect terms

Cookies: For certain functions (maintaining state) and collecting usage data

Privacy: GDPR conformance

Authentication: Valid user

Authorisation: Permission to access asset in appropriate modality

Metadata: discovery, contextualization, workflow orchestration including curation and provenance

Licensing: usage conditions, attribution/citation/acknowledgement

All Require SUFFICIENT conformity for interoperation

Policy Interoperation / Conformance

- To be discussed when a quorum of RIs have their policies, guidelines and IT implementations defined
- A new landscape analysis at that time to identify any non-conformances / inconsistencies with the recommendations of the WP5 TFs and individual RI governance
- A plan to finalise evolutionary convergence of policies of ENVRI RIs, ENVRI-Hub and EOSC

These are the next steps

General Discussion

ENVRI

FAIR

envri.eu/envri-fair

@envri_fair

company/envri-fair

facebook.com/ENVRIcomm