

# EOSC-ENTRUST First Evaluation & Adoption Workshop

24-25 September 2024, Helsinki

Local Organisers: Miikka Kallberg (CSC) Stefanie Kirschenmann  
(CSC), Susanna Repo (CSC)









Funded by  
the European Union

# The venue: Paasitorni

- Paasitorni was built to be a Helsinki Workers' House. The oldest part of Paasitorni was completed in 1908, and extensions in 1925, 1995 and 2012.
- The granite used was facade excavated on site
- Paasitorni is one of 7 workers' assembly halls that are aiming for UNESCO World Heritage List



# Welcome to the 1st EOSC-ENTRUST Evaluations & Adoptions Workshop

-  Please remain muted unless you are invited to speak by the Chair
-  Please use the “hand-raising function” to indicate you would like to contribute directly
-  Attendees are encouraged to have their camera on when appropriate (bandwidth and circumstances allowing)
-  Please use “Chat” for further comments or discussions.
-  The meeting will start at the top of the hour
-  This meeting will be run in line with the ELIXIR Code of Conduct  
If you have any concerns, please refer to the Code of Conduct on the ELIXIR website

Adapted from [ELIXIR housekeeping slides](#)



# ELIXIR's Code of Conduct – the principles



The Code of Conduct pertains to ELIXIR organised or funded events



**We value**  
each other's perspectives

**We adopt**  
a zero-tolerance approach to harassment and discrimination

**We maintain**  
high ethical standards

**We'll apply**  
honesty and integrity in the dealing of any transgressions against the Code.

**We're committed**  
to making ELIXIR events collaborative, supportive and enjoyable

**We'll ensure**  
a respectful and inclusive environment

Source: [ELIXIR housekeeping slides](#)



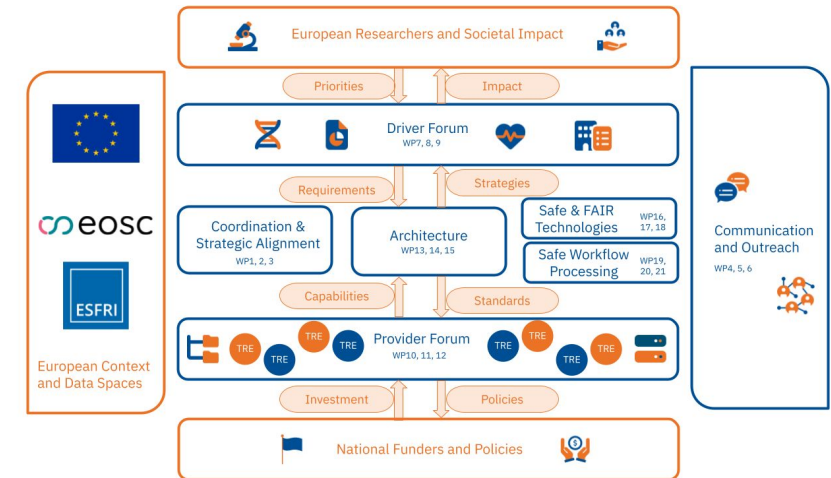


# Opening and Welcome

- Words of welcome and Housekeeping, Objectives of this workshop  
– *Miikka Kallberg*
- EOSC-ENTRUST: WP1 view and links to EOSC, EHDS and Data Spaces  
– *Peter Maccallum*
- Round-table of introductions – *Miikka Kallberg*

# Workshop objectives

- ★ Facilitating alignment between the different EOSC-ENTRUST work packages
- ★ Mapping results from the Drivers and Providers WPs to the Architecture WP
- ★ Providing input for the related deliverables regarding the blueprint architecture and the provider catalogue



# Agenda 24 September

[Link to Agenda](#)

[Link to collaborative minutes](#)

Time	Session	Presenter
13:00-13:15	<b>Opening</b> <ul style="list-style-type: none"><li>Words of welcome and Housekeeping, Objectives of the workshop</li><li>The Blueprint in context - the view from WP1</li><li>Round-table of introductions</li></ul>	Miikka Kallberg Peter Maccallum Miikka Kallberg
13:45-15:00	<b>Session 1 - Input from Drivers and Providers</b> <ul style="list-style-type: none"><li>WP7: Evaluating driver requirements for the TRE blueprint</li><li>TRE Inventory &amp; Capabilities</li><li>Requirements gathering framework and gap analysis</li></ul>	Anne van der Kant Heidi Laine Abdulrahman Azab
15:00-15:30	<b>Break</b>	
15:15-16:45	<b>Session 2 - Cross-WP Alignment</b> <ul style="list-style-type: none"><li>Update from WP16 (Technologies)</li><li>WP19: Digital Transformation to support FAIR, workflows and federated analytics</li><li>Discussion: Cross-WP alignment</li></ul>	Peter Balcirak, Martin Kuba Stian Soiland-Reyes
16:45-17:00	<b>Closing Day 1</b>	
18:00-	<b>Working dinner</b>	

# Agenda 25 September

Time	Session	Presenter
08:00–09:00	<b>Breakfast</b>	
09:00–10:30	<b>Session 3 - Architecture and Blueprint</b> <ul style="list-style-type: none"> <li>Short summary from DARE UK report</li> <li>Architecture WP: Introduction and Status updates on the upcoming deliverables / milestones <ul style="list-style-type: none"> <li>D13.2 - Training package for EOSC-ENTRUST Year one Blueprint &amp; Interoperability Framework</li> <li>D13.3 - Machine-readable First Edition of the EOSC-ENTRUST TRE Provider Catalogue</li> <li>D13.4 - Year one version of EOSC-ENTRUST Blueprint &amp; Interoperability Framework</li> <li>M15 - Key selected interoperability challenge demonstrations implemented</li> </ul> </li> <li>Discussion</li> </ul>	Rob Baxter  Christine Stansberg  Miikka Kallberg  Pål Sætrom  Per Kulseth Dahl
10:30–12:00	<b>Breakout Rooms (3 hybrid rooms)</b> <u>Main focus:</u> Year one version of EOSC-ENTRUST Blueprint	
	Subtopic: <i>Interoperability</i>	Subtopic: <i>Capabilities</i>  Subtopic: <i>Governance</i>
12:00–12:45	<b>Lunch</b>	
12:45–14:30	<b>Results from the Breakout sessions and closing of the Workshop</b> <ul style="list-style-type: none"> <li>Plenary: Wrap-up from the breakout rooms</li> <li>Closing</li> </ul>	Miikka Kallberg, Pål Sætrom
14:30–15:00	<b>Coffee and Leaving</b>	

[Link to Agenda](#)

[Link to collaborative minutes](#)

## **Next**

EOSC-ENTRUST: WP1 view and links to EOSC, EHDS and Data Spaces

– *Peter Maccallum*



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union





# The Blueprint in context - the view from WP1

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Peter Maccallum, ELIXIR/EOSC-ENTRUST Coordination



Funded by  
the European Union

# EOSC-ENTRUST Objectives

Objective 1: Create a European network of Trusted Research Environments, linked to EOSC and EuroHPC, to enable transnational collaborative research on sensitive or restricted data.

Objective 2: Trusted Research Environment providers implement, validate, and promote their capabilities through a European framework using common standards and shared legal, operational and technical language.

Objective 3: National funders and governments understand the network of TRE capabilities serving their needs, and how TREs support their national priorities and their contributions to selected transnational programmes.

**Objective 4: The European Network of Trusted Research Environments (ENTRUST) is embedded in the European Open Science Cloud and the European Data Spaces and fosters an ecosystem of public, private and joint-venture providers of TRE services.**

# Blueprint & Interoperability Framework in context

*'There was a star danced, and under that was I born...'*

There is a lot of activity in the TRE/SPE space, and the Data Spaces in general.

This leads to two possible interpretations of where we stand (Sep 2024)

- **Pessimistic:** there is so much going on, we will never be able to track it all and keep up
- **Optimistic:** there is so much going on, Europe (and therefore the World) needs a more robust framework to make sense of it all

We will (of course!) make the case for the second view

# Data Spaces and TRE/SPE specifications

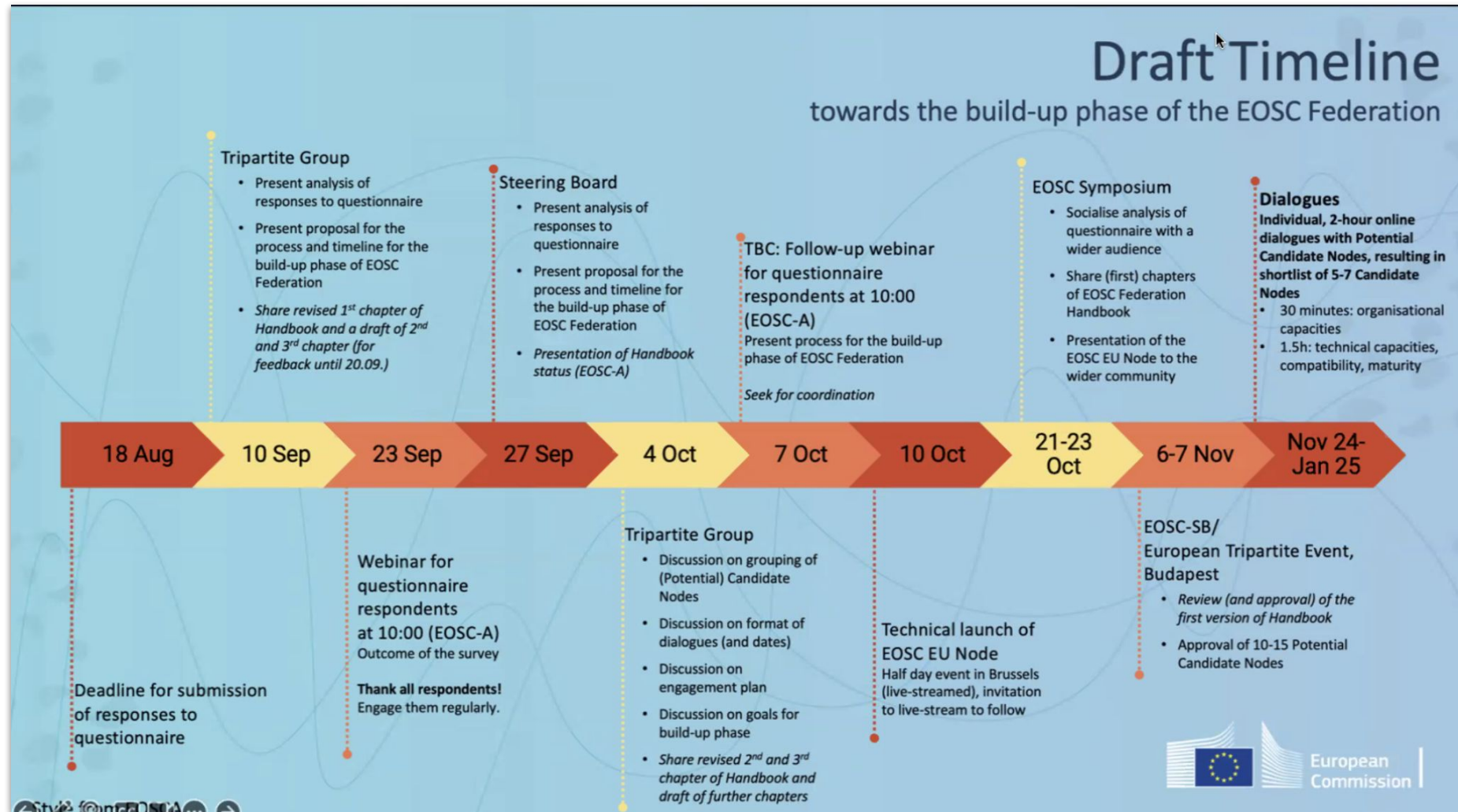
Key developments ongoing now:

- EOSC Association Handbook and the EOSC Node Concept
- Adoption of the EHDS regulation and TEHDAS2
- Data Spaces standardisation approaches
- Activities outside the EU, and outside Europe

# EOSC is developing its operational model

The EOSC Association is finishing the development of its operating model.

This will include the context of 'EOSC Nodes' through which TRE and other services will be delivered.



# The **EOSC EU Node**

The EOSC EU Node has been procured as a single entity.

It will take the form of a Cloud hosting environment and proof-of-concept.

TRE/SPE is not part of the initial specification.

**European Open Science Cloud - EU Node**

Home | About | Services | Resource Hub | Support | Contributors | News & Events

## **EOSC EU Node**

A European platform and information gateway to explore, engage, and enrich your research collaborations.

[Explore our services >](#)

### **Upcoming Services**

The EOSC EU Node will offer the following services (currently under development):

<b>File Sync &amp; Share</b> Enable automatic file syncing and secure sharing across locations and teams.	<b>Interactive Notebooks</b> Create and share documents with real-time code execution.	<b>Large File Transfer</b> Streamline large file transfers online with added security and integrity.
<b>Virtual Machines</b> Design and conduct experiments with flexibility while ensuring reproducibility.	<b>Cloud Container Platform</b> Deploy cloud-native containerised applications that can easily scale.	<b>Bulk Data Transfer</b> Move data effortlessly to data-intensive execution environments.



# The EOSC Catalogue revisited

The EOSC-Future 'EOSC Catalogue' is present in reduced form. Most of the resources listed are harvested from OpenAIRE and Zenodo.

We can expect that RDF will be the 'language' of the catalogue.

The screenshot displays the 'European Open Science Cloud - EU Node' website. The header includes the European Commission logo and a navigation menu with links to Home, About, Services, Resource Hub, Support, Contributors, and News & Events. The 'Resource hub' section features a search bar and a list of resource categories: All resources, Publications, Data, Software, Other Products, Services, Data Sources, Training, and Interoperability Guidelines. A sidebar on the left lists various scientific domains and horizontal services. The main content area shows a list of resources, with the first entry highlighted by a yellow circle. This entry is titled 'EOSC Interoperability Guidelines for Data Sources to onboard Research Products' and is provided by OpenAIRE. The text below the title describes the guidelines for hosting data and mentions the use of descriptive metadata. The second entry, also highlighted by a yellow circle, is titled 'Guidelines for the evaluation and combination of the assurance of external identities (AARC-G031)' and is provided by the GÉANT Association. The text below this title describes the AARC Blueprint Architecture and the use of external Identity Providers.

European Commission

European Open Science Cloud - EU Node

Home | Home | About | Services | Resource Hub | Support | Contributors | News & Events

Home > Resource hub

Resource hub

Search resources

All resources | Publications | Data | Software | Other Products | Services | Data Sources | Training | Interoperability Guidelines

Showing 1 to 20 of 5,169,055 resources

No filters applied

Relevance

INTEROPERABILITY GUIDELINE

Year: 2023 | License: CC-BY-4.0

**EOSC Interoperability Guidelines for Data Sources to onboard Research Products**

Interoperability guidelines are intended for adoption by EOSC Data source managers/developers (personnel acting on behalf of Data Source providers). An EOSC Data Source is an EOSC Service intended for hosting data (in the sense of digital objects, such as research publications, research data, research software) and associated descriptive metadata (e.g., bibliographic, attribution, provenance, quality, disciplinary). Data Sources typically enable...

Provider: OpenAIRE

INTEROPERABILITY GUIDELINE

Year: 2016 | License: CC-BY-4.0

**Guidelines for the evaluation and combination of the assurance of external identities (AARC-G031)**

The Research Infrastructures (from now on just Infrastructures) that follow the AARC Blueprint Architecture set up their own AAI to grant access to their services. The AAI is typically based on a central IdP-SP proxy that act as a gateway for the Infrastructure services and resources. In order to assign an identity to the users of the research collaboration or the community they serve, Infrastructures rely on external Identity Providers and employ identity...

Provider: GÉANT Association

# The **EHDS** Regulation

The EHDS regulation has been adopted as a proposal.

There are a few steps to get it ratified by the Parliament and revised by the Commission. It will likely come in to force late 2025, with implementation over 5 years.

Brussels, 18 March 2024  
(OR. en)

7553/24

LIMITE

SAN 139  
PHARM 41  
COMPET 293  
MI 279  
DATAPROTECT 134  
CODEC 741  
IA 81

## NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
No. Cion doc.:	8571/22 ADD1-8
Subject:	Proposal for a Regulation on the European Health Data Space - Analysis of the final compromise text with a view to agreement

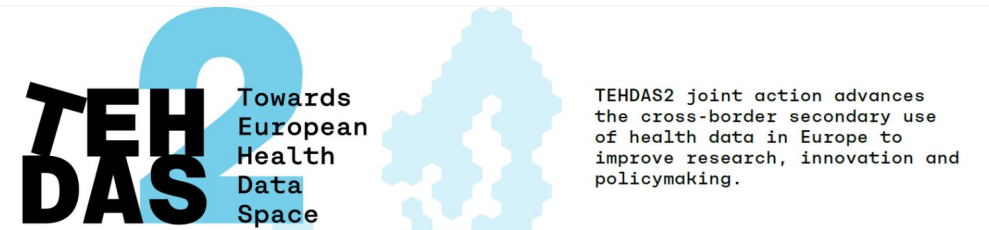
## I. INTRODUCTION

1. On 3 May 2022, the Commission submitted to the Council and the European Parliament a proposal for a Regulation on the European Health Data Space<sup>1</sup> (EHDS), which was accompanied by an impact assessment and a communication. The proposal is based on Articles 16 and 114 of the Treaty on the Functioning of the European Union (TFEU) (ordinary legislative procedure). The EHDS is the first of the European common data spaces proposed in the 2020 communication 'A European strategy for data'<sup>2</sup>, which announced the creation of nine sector- and domain-specific data spaces, and is considered a key pillar of the European Health Union.
2. The proposal aims to improve individuals' access to and control over their personal electronic health data (primary use of data), at both national and EU levels, and to facilitate data reuse (secondary use of data) for research, innovation, regulatory and public policy purposes across

# EHDS specification: **TEHDAS2**

The TEHDAS joint actions are developing the technical specifications.

TEHDAS2 has just started.  
WP7 will define the 'SPE' technology to be adopted.



## **What is our goal?**

Our goal is to develop common guidelines and technical specifications to facilitate smooth access to health data and strengthen European collaboration in using data efficiently. Secondary use of health data enhances competitiveness of European research and innovation in the health sector.

## **What are we doing?**

TEHDAS2 produces concrete guidelines and technical specifications for the European Commission and member states to ensure a harmonised implementation of the European Health Data Space (EHDS) regulation. Member states can use TEHDAS2 results to support their implementation efforts at the national level, while at the same time, the work will support the European Commission, for instance, in the drafting of the implementing acts defined in the EHDS regulation.

## **What are the benefits?**

The benefits include harmonised rules and procedures for secondary use of health data to boost research, innovation, and policymaking, ultimately improving public health in Europe.

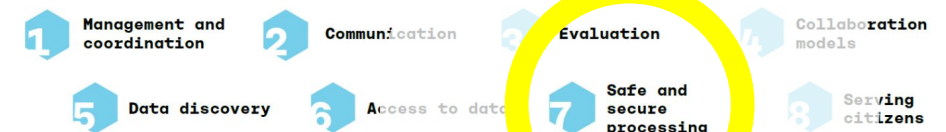
## **Who is involved?**

The project is being carried out by 30 European countries. Stakeholders across Europe are invited to provide input to the work through public consultations. TEHDAS2 builds on the work of previous TEHDAS joint action and other European projects such as the HealthData@EU Pilot project, and it will be implemented in close collaboration with other ongoing projects and initiatives.

## **How to follow the project and connect?**

All results, consultations and events will be published on the [tehdas.eu](https://tehdas.eu) website and social media. The TEHDAS2 coordination team can be reached by email at [tehdascoordination@sitra.fi](mailto:tehdascoordination@sitra.fi).

## **The work is divided into eight work packages:**



# EHDS mandated standards

The Data Spaces, and the EHDS in particular, have a recent history of mandating standards when faced with competition and diversity.

For example EHDS have selected DCAT-AP for dataset catalogue metadata.

## DCAT-AP 3.0

14 June 2024



### ▼ More details about this document

#### Latest published version:

<https://github.com/SEMICeu/DCAT-AP/tree/master/releases/2.1.1>

#### Latest editor's draft:

<https://semiceu.github.io/DCAT-AP/releases/3.0.0>

#### History:

[Commit history](#)

#### Editors:

Jitse De Cock (PwC EU Services)  
Makx Dekkers  
Pavlina Fragkou (DG DIGIT)  
Arthur Schiltz (PwC EU Services)  
Anastasia Sofou (Trasys International)

#### Author:

[Bert Van Nuffelen](#) (Digitaal Vlaanderen)

#### Feedback:

[GitHub SEMICeu/DCAT-AP](#) ([pull requests](#), [new issue](#), [open issues](#))

#### Owners:

[SEMIC](#)  
Pavlina Fragkou (DG DIGIT)

Copyright © 2024

## Abstract

DCAT-AP is a DCAT profile for sharing information about Catalogues containing Datasets and Data Services descriptions in Europe, under maintenance by the SEMIC action, Interoperable Europe.

This Application Profile provides a minimal common basis within Europe to share Datasets and Data Services cross-border and cross-domain.



# Mandated standards 2 - **SIMPL?**

One intention, across the Data Spaces but led by EHDS, is adoption of the SIMPL middleware.

This has been procured, from scratch - we don't yet have reference implementations to evaluate.

The image shows a screenshot of the Simpl Programme website, which is part of the European Commission's initiatives. The website features a blue header with the European Commission logo and a navigation menu including Home, Community, Development, Publications, and About. A prominent banner highlights 'On the spotlight | New Requirements Updated!' with a link to 'To the requirements'. Below this, there are sections for 'About Simpl' and 'Upcoming Events'. The 'About Simpl' section describes it as an open source, secure middleware platform. The 'Upcoming Events' section lists the 'Simpl Annual Event' and the 'European Big Data Value Forum'. A diagram in the foreground illustrates the SIMPL ecosystem, showing the core product (SIMPL-Open) and its deployment in various environments (SIMPL-Labs, SIMPL-Live) for sectoral data spaces.

European Commission

## Simpl Programme

Home Community Development Publications About

**On the spotlight | New Requirements Updated!**  
How Can Simpl-Open Enhance Logging and Monitoring?  
[To the requirements](#)

**About Simpl**  
Simpl is an open source, secure middleware platform that supports data access and interoperability in European data initiatives. It provides multiple compatible components, free to use, that adhere to a common standard of data quality and data sharing. A future where reliable, updated data are available across industries is possible with Simpl.  
[Read more](#)

**Upcoming Events**

- Simpl Annual Event**  
30 Jan '25 08:30 - 17:30 (CEST)
- European Big Data Value Forum**  
2 Oct '24 08:30 - 4 Oct '24 15:30

**How to participate**  
At its core, Simpl is an open source project, which a large network of contributors. Simpl allows anyone to contribute to the project, which increases transparency and customisation. Beyond code development: there are many ways to get involved in the project.  
[Read more](#)

**SIMPL-Open**  
The core product of SIMPL  
An open-source software stack that powers data spaces and other cloud-to-edge federations initiatives.

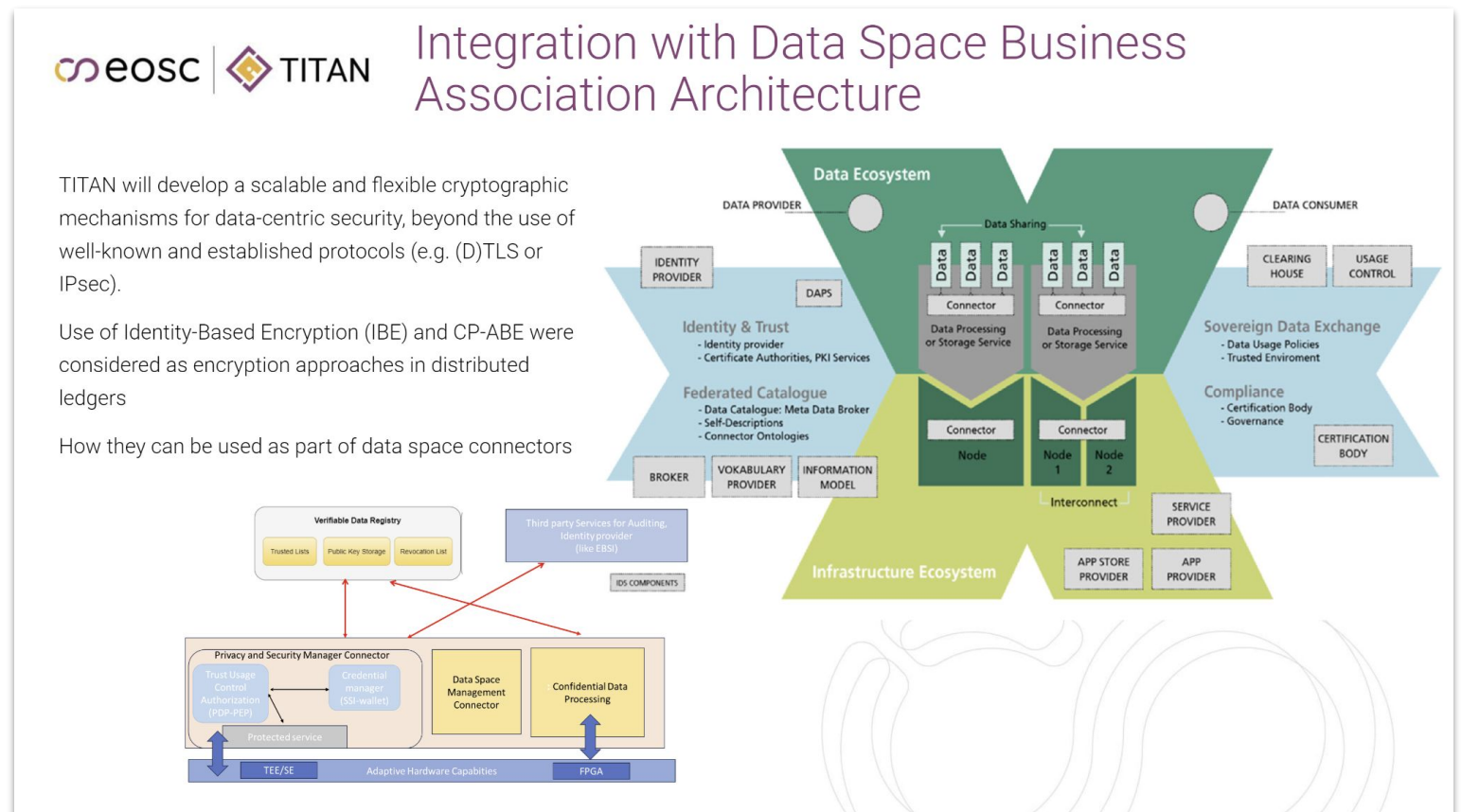
**SIMPL-Labs**  
Playground and demonstration environment for SIMPL-Open  
An environment for data spaces to experiment with the open-source software and assess their level of interoperability with Simpl.

**SIMPL-Live**  
Instances of SIMPL-Open for sectoral data spaces  
The deployment of SIMPL-Open for selected Data Spaces.

# TITAN Data Space connector technology

Our EOSC TRE sister project plans a workstream on Data Space connectors.

We should connect this work at an early stage, and see how their future developments would be represented in the current blueprint.





# 'Outside' the EU United Kingdom

The DARE programme, which funded SATRE and TRE-FX, has been renewed by the UK government.

While the focus will be to support UK research needs, the funding to develop capabilities is significant (more than 5MGBP/year)

## DARE UK

News September 18, 2024

### **£18 million for DARE UK to support secure research on sensitive data**

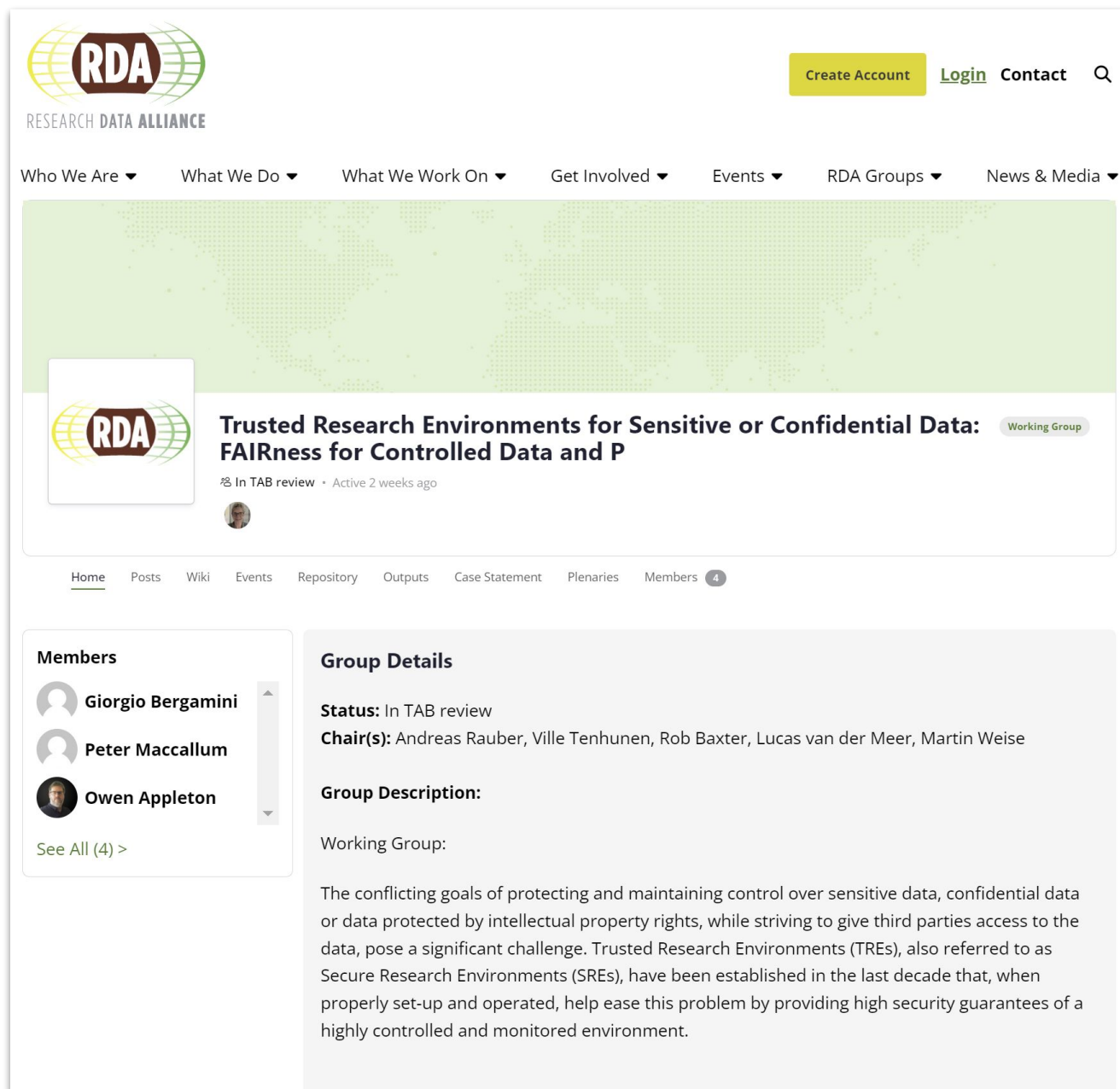
UK Research and Innovation (UKRI), the UK's largest public funder of research, has confirmed funding for a new phase of the DARE UK (Data and Analytics Research Environments UK) programme with up to £18.2 million made available over 2.5 years.

Starting this month, Phase 2 of the DARE UK programme will bring together Trusted Research Environments (TREs) across the UK to test and build new capabilities for a connected national network of secure data research infrastructures for better, faster, and safer research on sensitive data. TREs are highly secure computing environments that provide remote access to sensitive data (such as education, tax and benefits, and health datasets) for approved researchers to generate new understanding for public benefit and to improve people's lives.

The investment will support researchers using TREs to do faster and safer research with sensitive data, for example, through new capabilities in federated analysis and safe training of AI models. The DARE UK programme will continue to work with and convene stakeholders across the research ecosystem to deliver this in Phase 2.

# 'Outside' the EU Worldwide/RDA

A new WG on TREs is being convened by the RDA - this will work for 18 months towards published recommendations.



The screenshot displays the RDA Research Data Alliance website. At the top, the RDA logo is on the left, and navigation links for 'Create Account', 'Login', and 'Contact' are on the right. A secondary navigation bar includes links for 'Who We Are', 'What We Do', 'What We Work On', 'Get Involved', 'Events', 'RDA Groups', and 'News & Media'. The main content area features a large green banner with a world map pattern. Below this, a white box contains the RDA logo and the title 'Trusted Research Environments for Sensitive or Confidential Data: FAIRness for Controlled Data and P', with a 'Working Group' tag. It also indicates the group is 'In TAB review' and 'Active 2 weeks ago'. A horizontal menu below the banner lists 'Home', 'Posts', 'Wiki', 'Events', 'Repository', 'Outputs', 'Case Statement', 'Plenaries', and 'Members' (with a count of 4). The 'Members' section on the left lists Giorgio Bergamini, Peter MacCallum, and Owen Appleton, with a 'See All (4) >' link. The 'Group Details' section on the right shows the status as 'In TAB review', lists the chairs (Andreas Rauber, Ville Tenhunen, Rob Baxter, Lucas van der Meer, Martin Weise), and provides a description of the working group's goals and the challenges of Trusted Research Environments (TREs).

**RDA**  
RESEARCH DATA ALLIANCE

Create Account Login Contact

Who We Are What We Do What We Work On Get Involved Events RDA Groups News & Media

**Trusted Research Environments for Sensitive or Confidential Data: FAIRness for Controlled Data and P** Working Group

In TAB review · Active 2 weeks ago

Home Posts Wiki Events Repository Outputs Case Statement Plenaries Members 4

**Members**

- Giorgio Bergamini
- Peter MacCallum
- Owen Appleton

See All (4) >

**Group Details**

**Status:** In TAB review

**Chair(s):** Andreas Rauber, Ville Tenhunen, Rob Baxter, Lucas van der Meer, Martin Weise

**Group Description:**

Working Group:

The conflicting goals of protecting and maintaining control over sensitive data, confidential data or data protected by intellectual property rights, while striving to give third parties access to the data, pose a significant challenge. Trusted Research Environments (TREs), also referred to as Secure Research Environments (SREs), have been established in the last decade that, when properly set-up and operated, help ease this problem by providing high security guarantees of a highly controlled and monitored environment.

# For this workshop

Some constraints:

- The Data Spaces will require flexibility as business models develop
- There may be technical standards imposed by the Commission such as SIMPL
- EOSC will preferentially consume RDF
- There are programmes beyond EOSC with their own objectives

Some opportunities:

- We have the UK blueprints as a baseline
- We already have a network of TREs with varying capabilities and user communities
- We have already started!

Most importantly - most of these other programmes will consume whatever high quality reference is available, as their starting point.



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# Evaluating driver requirements for the TRE blueprint

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Anne van der Kant - Health-RI (NL)



Funded by  
the European Union

# WP 7-8-9: Drivers

## Aim

- Inform Blueprint from the perspective of representative TRE users
- Evaluate Blueprint through real-world use cases (“Drivers”)

## How?

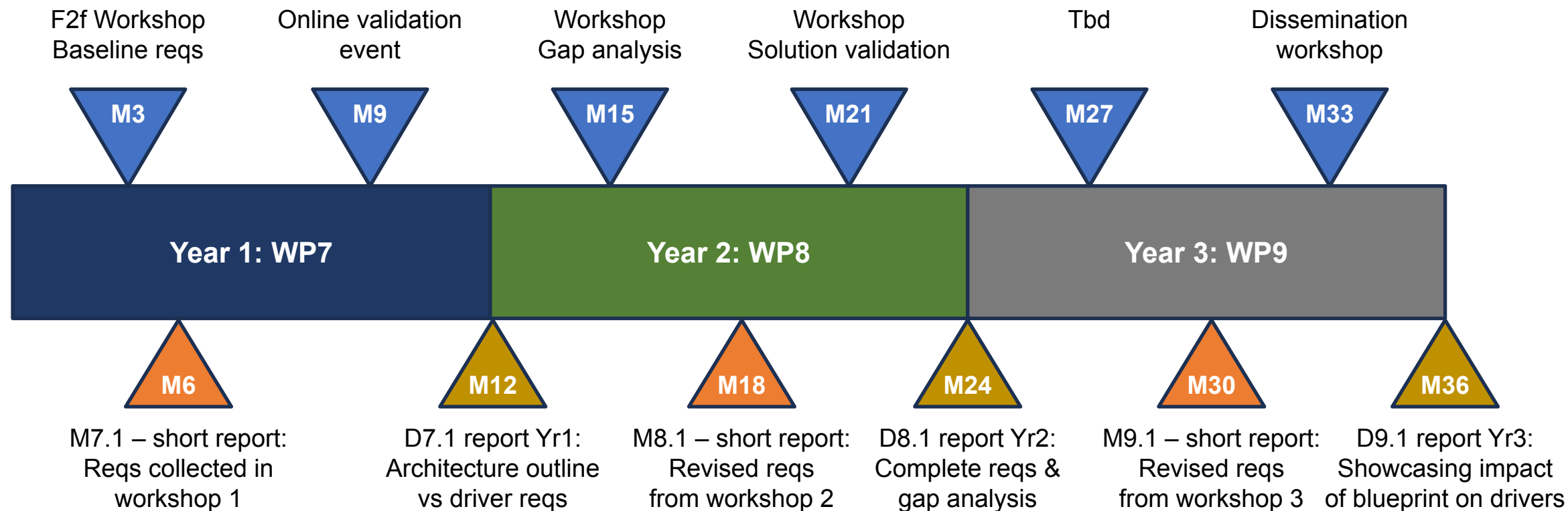
- Gather Driver requirements and harmonize these using a common framework (where possible)
- Evaluate architectural concepts and proposed technical solutions (WP13) against requirements
  - Workshops
  - Validation report



# Four Drivers

- Federated Human Genomics as a catalyst for European TRE provision (EMBL, CRG, BSC)
- Common standards to enable trans-national sharing of administrative and social science data (CESSDA, GESIS, UKDS, TARKI)
- Enabling the re-use of clinical trials data for research purposes across Europe (ECRIN, UiO, HDR UK, UNIVDUN)
- Public-Private interactions between TRE in health and environmental data (Turku UAS, CSC, Sigma2)

# Structure of WP7-9



# Status

- Initial Driver requirements have been gathered:
  - [M7.1 Milestone Report](#)
  - [M7.1 Drivers List of requirements](#)
  - [M7.1 Drivers mapping](#), containing analysis
- Drivers participate in D13.4 Blueprint meetings to help align Blueprint with requirements
- Preparing next steps towards D7.1: Driver validation report
  - Barriers to adoption
  - Gaps between blueprint & requirements
  - Follow-up in-person workshop to be planned

# Process towards requirements: design thinking

## Leading questions

- What problem is the Driver trying to solve?
- Who are the users?
- What is the (expected) user journey?
- Which key capabilities and requirements can be identified?

## How

- Initial Drivers requirements workshop
- Individual Driver focus workshops



# Results: Users

## **Data providers**

- Data managers
- Data custodians
- PIs
- Trial sponsors
- Healthcare professionals
- Public health institutes

## **Infrastructure providers**

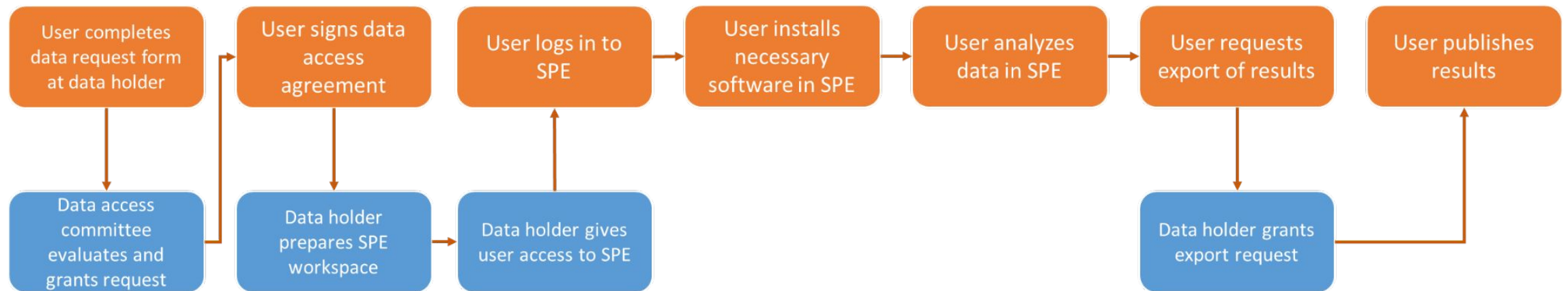
## **Regulatory bodies**

## **Data users**

- Researchers
- Policy makers
- Patients
- Citizens
- Developers

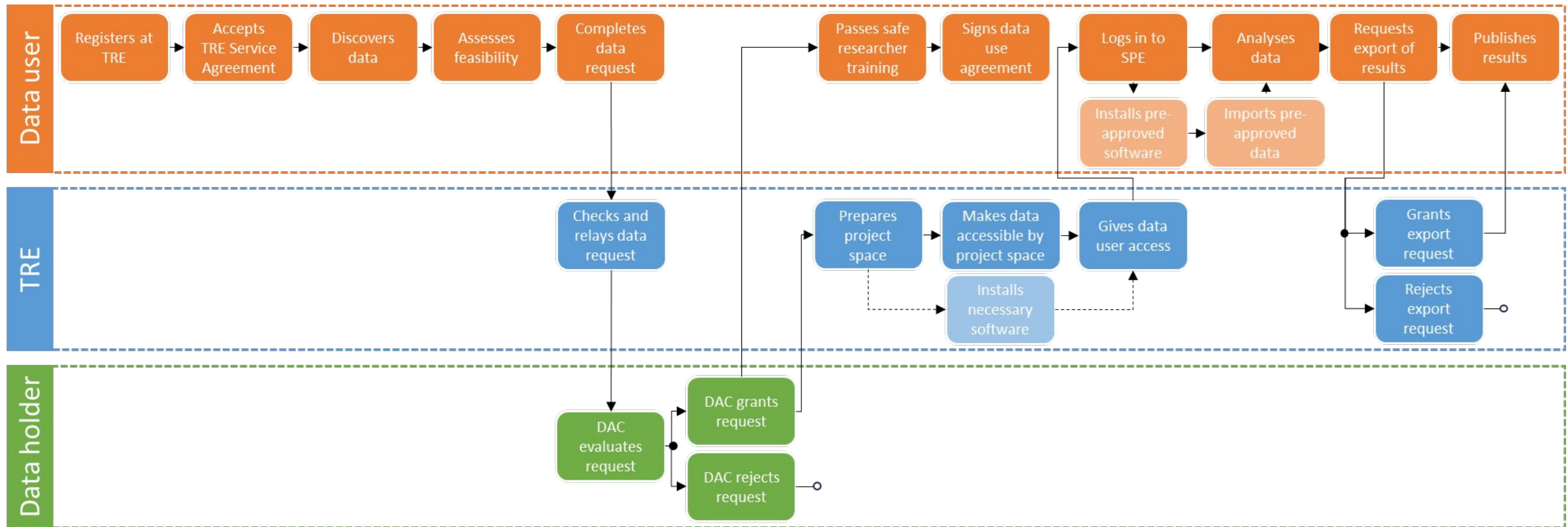
# Results: User journey

## Initial (example journey provided to Drivers)



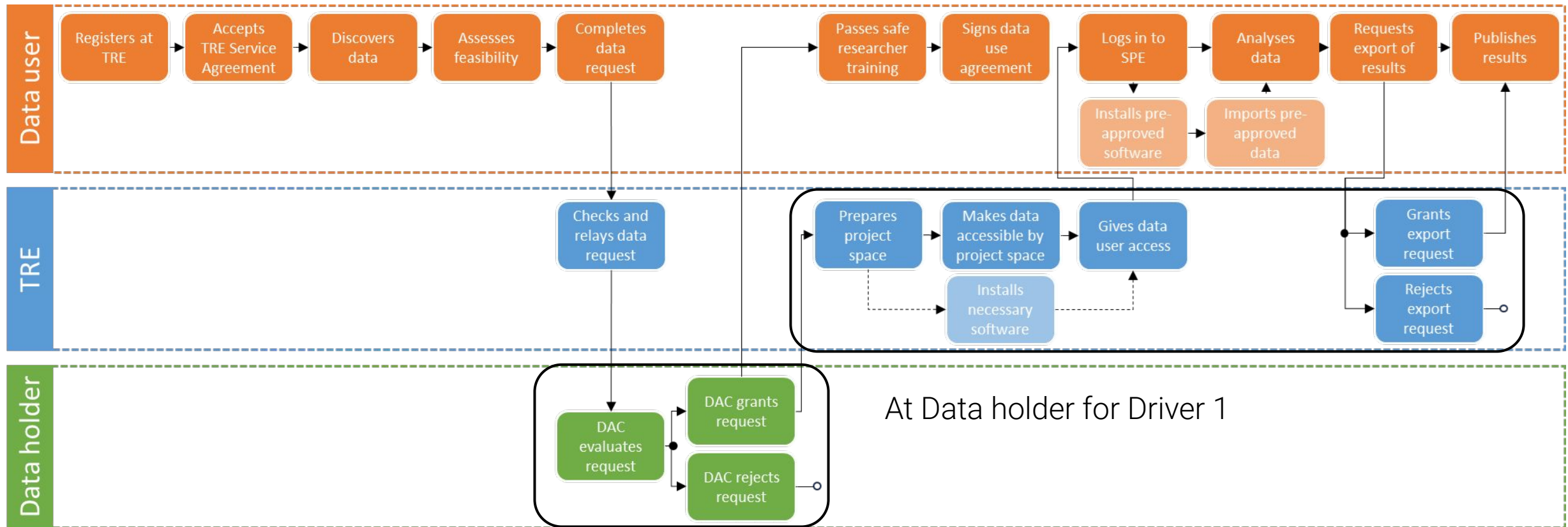
# Results: User journey

## Updated



# Results: User journey

## Updated



Can take place  
at TRE



# Drivers Requirements

Gathered in [M7.1 List of Requirements](#)

## **Most agreed-upon (3 or 4 Drivers)**

- Data Sharing Agreement
- Data encryption in transit
- Data Use Agreement
- Usability

## **Varying between Drivers**

- Internet connection from within TRE
- Retrieving output from TRE (more a question of: under which conditions)

# Mapping on SATRE

Key capabilities (indicated by 3 or 4 Drivers)

<b>Information Governance</b>	
Governance Requirements	4 Drivers
<b>Computing technology and Information Security</b>	
End user computing	4 Drivers
Infrastructure management	3 Drivers
Information security	4 Drivers
<b>Data Management</b>	
Data lifecycle management	3 Drivers
Identity and access management	3 Drivers
Output management	3 Drivers
Security Levels and Tiering	3 Drivers
<b>Supporting Capabilities</b>	
Business continuity management	3 Drivers
Legal services	3 Drivers

# Mapping on SATRE

Missing Capabilities	Driver 1	Driver 2	Driver 3	Driver 4
Anonymization	x		x	
Internet Connection from Within TRE	x			
Scalable Infrastructure	x			
data standardisation/ common data models			x	
Data transfer between environments		x		
Service design				x
Ethical guidance				x
Backup				x

# Alignment with DARE-UK

## Federation

- Driver 3 states *Data discovery*, possibly in a federated way, as a requirement (could-have), should-have for Driver 2
- Federation is not explicitly stated as a requirement or important capability by the Drivers
- However..

# Alignment with DARE-UK

**A federated network with shared services** (as in DARE-UK architecture) provides a possible solution for multiple requirements:

- Data transfer between environments
- Data discovery
- Internet connection from within TRE (Drivers 1 & 4: should-have, Driver 2: won't have) - functional requirement: using data from outside TRE, Examples: annotation of genomes, reference sequences for sequence alignment, usage of ontologies and other open resources
- Scalable infrastructure
- Publishing and re-using code and workflows

# Identified issues

- All Drivers use at least one mature TRE, which puts the focus on existing solutions. It is important to keep the perspective of the user in mind when gathering requirements
- Definition and scope of TRE differs between Drivers: keep a broad scope to identify differences
- Conflation of roles of Data providers with TRE providers: roles can be fulfilled by the same organisations, but should be separable in the Blueprint architecture
- Each of the Drivers should explicitly consider the perspective of the data contributor next to that of the user

# Next steps

**Drivers 1, 3 and 4 propose to design surveys, where the scope differs based on the aims of the Drivers:**

- Driver 1 aims to gather specific data holders' requirements, subsequently to be mapped to the SATRE framework
- Driver 3 aims to gather specific requirements from clinical trial sponsors and PIs on requirements for data sharing, including via the use of TREs
- Driver 4 aims to gather requirements from (potential) data users

Where possible we would like to align with other EOSC-ENTRUST surveys





---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# TRE Inventory & Capabilities

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Heidi Laine



Funded by  
the European Union

# TRE Survey

- WP10 (Provider Forum) conducted a survey among partner (and affiliated) TRE's for the inventory
- Survey was based on survey conducted by HDRUK
- Questions were organised around 5 safes
- Responses were collected over the summer
- 18 TRE's either in production or in development were reported (+ 1 directly to the inventory spreadsheet)
- Transcript of questions in Zenodo [here >](#)
- Raw survey results also available at the [project drive](#) (you might need to request authorization)

# Inventory

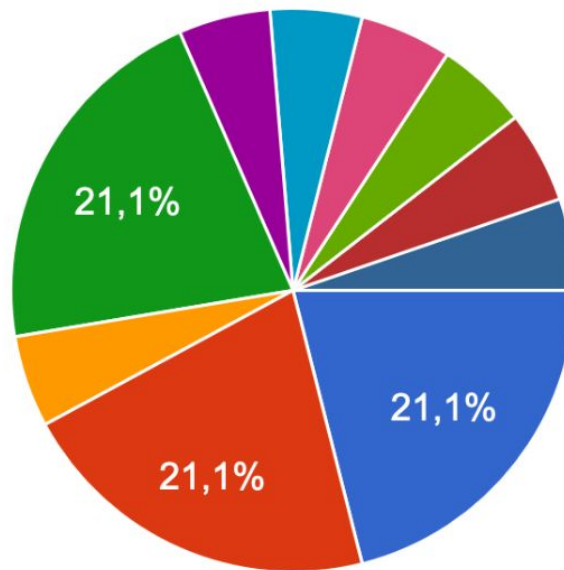
- First iteration of inventory (T4.1) covers TRE's operated by project partners or organisations affiliated with partners
- Inventory will be updated twice, by months 18 and 30 (and extended beyond original TRE's)
- First inventory internal to project, next versions will be public
- Final result the TRE service catalogue developed by WP Architecture in T5C.2?
- Inventory available for project participants [here>](#)
- Summary of TRE capabilities available [here>](#)

Some findings from the survey

# We need to define terminology

## 1.3 Primary term used to classify the environment

19 vastausta



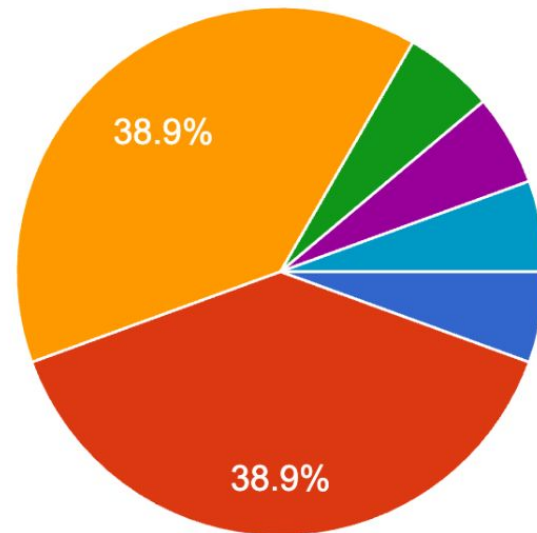
- Trusted Research Environment (TRE)
- Safe Processing Environment (SPE)
- Data Safe Haven
- HPC
- Remote access system
- My own TRE
- Data Archiving and Retrieval Environ...
- Federated IaaS, PaaS and SaaS clou...

▲ 1/2 ▼

# Some of us control data, others just process it

2.1 Is the organisation providing the environment also the data controller, or just a processor? Data controller = determines the purposes for which and t...ses sensitive data only on behalf of the controller

18 responses



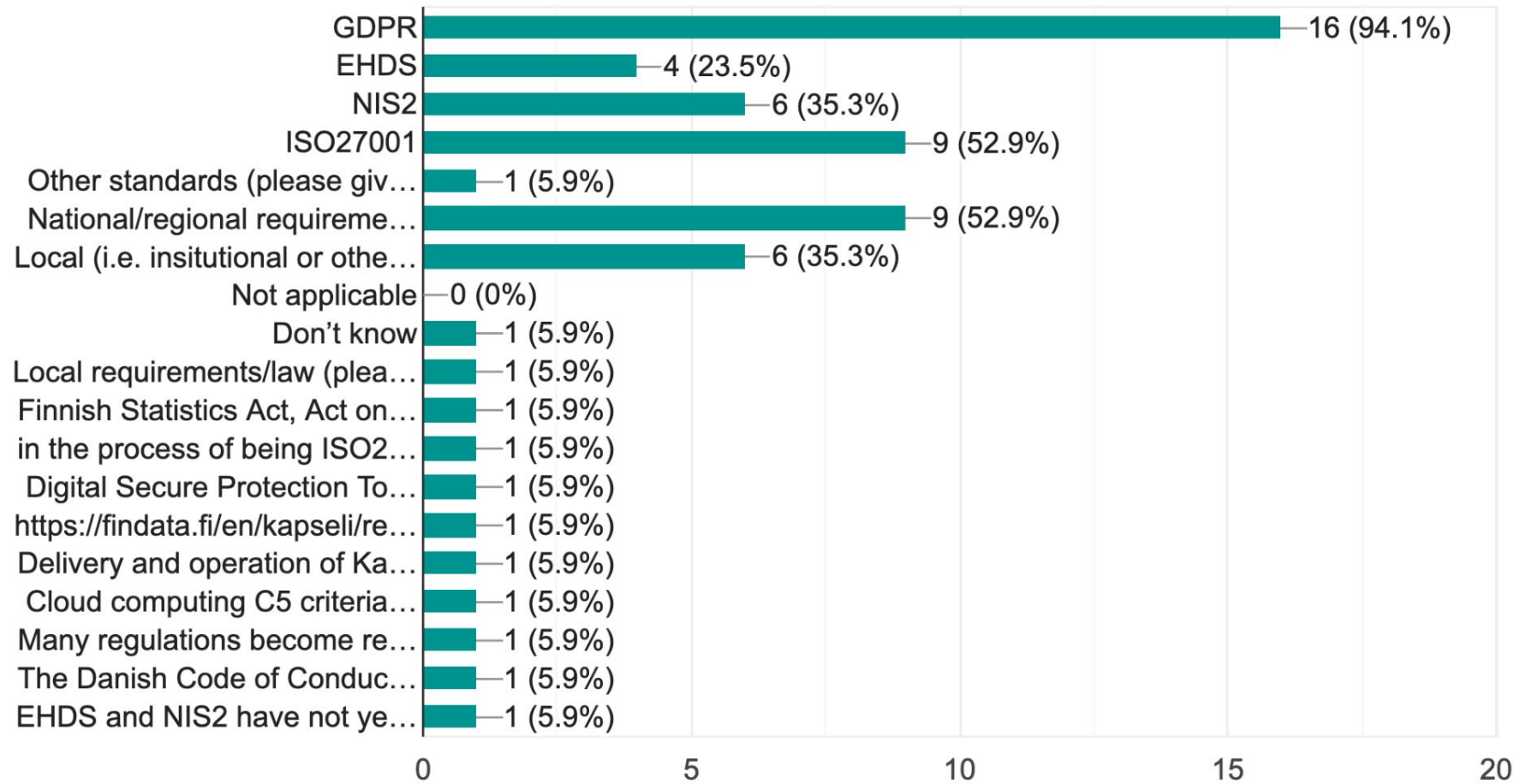
- The organization providing the environment is the data processor AN...
- The organization providing the environment is ONLY a processor
- The organization providing the environment can be the data controle...
- The organization providing the TRE is just a processor.
- The institution providing the environm...
- anDREa offers the ability to create Wo...



# There's a lot of red tape

2.2 What multinational, national, regional, or local legal or other binding requirements do you as the environment provider need to comply with?

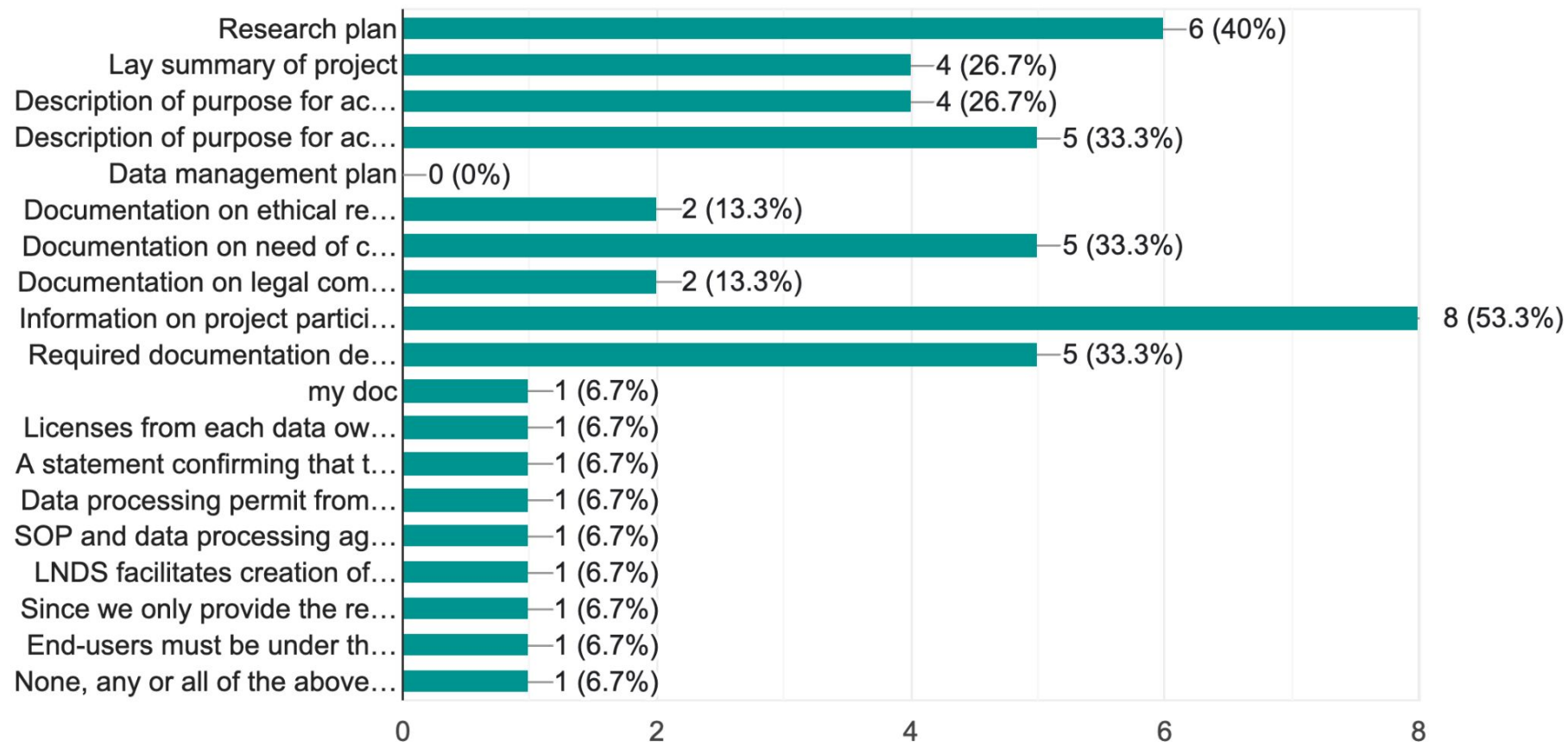
17 responses



# Also for users

## 2.3 What type of project documentation is required from end-users/projects to be granted access to the environments?

15 responses



# TRE capabilities based on the inventory

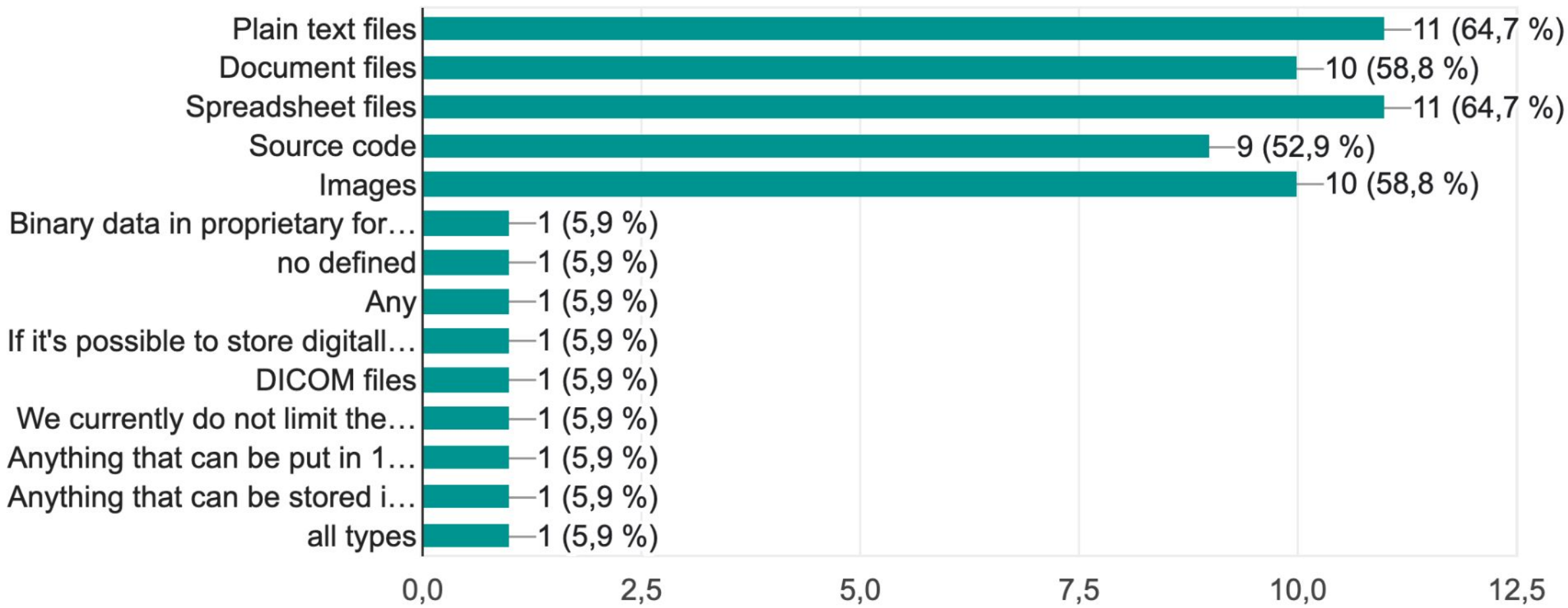
**A capability is the ability to execute a specified course of action or to achieve a desired outcome.**

## TRE capabilities covered in the survey

- Ability to support different data formats in the environment and upon export
- Ability to support secure access
- Ability to support international access
- Ability to prevent unauthorized access
- Ability to mitigate data loss
- Ability to mitigate misuse by users
- Ability to offer HPC in/through the environment
- Ability to allow users to import code/software/libraries
- Ability to prevent malicious code execution
- Ability to support external federated queries of metadata/data
- Ability to support AI/machine learning methods

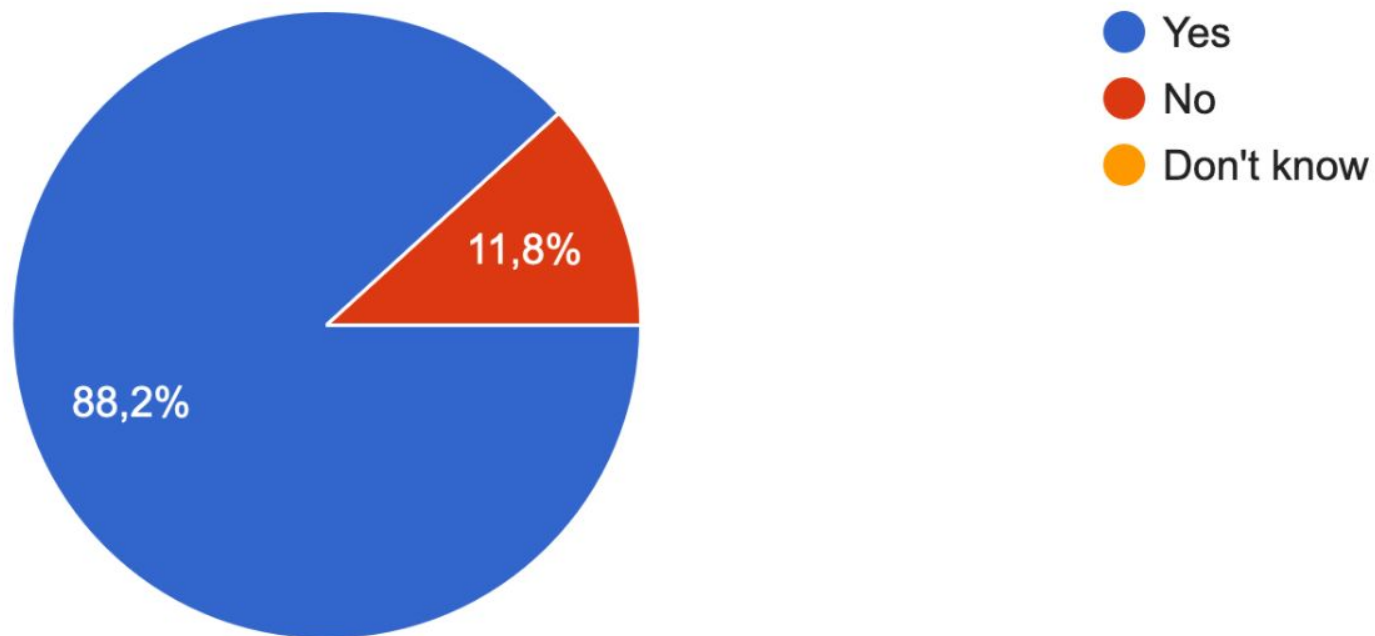
## 6.1 What types of data can a user export from your environment?

17 vastausta



### 3.6 Can the environment be accessed internationally? Please specify below.

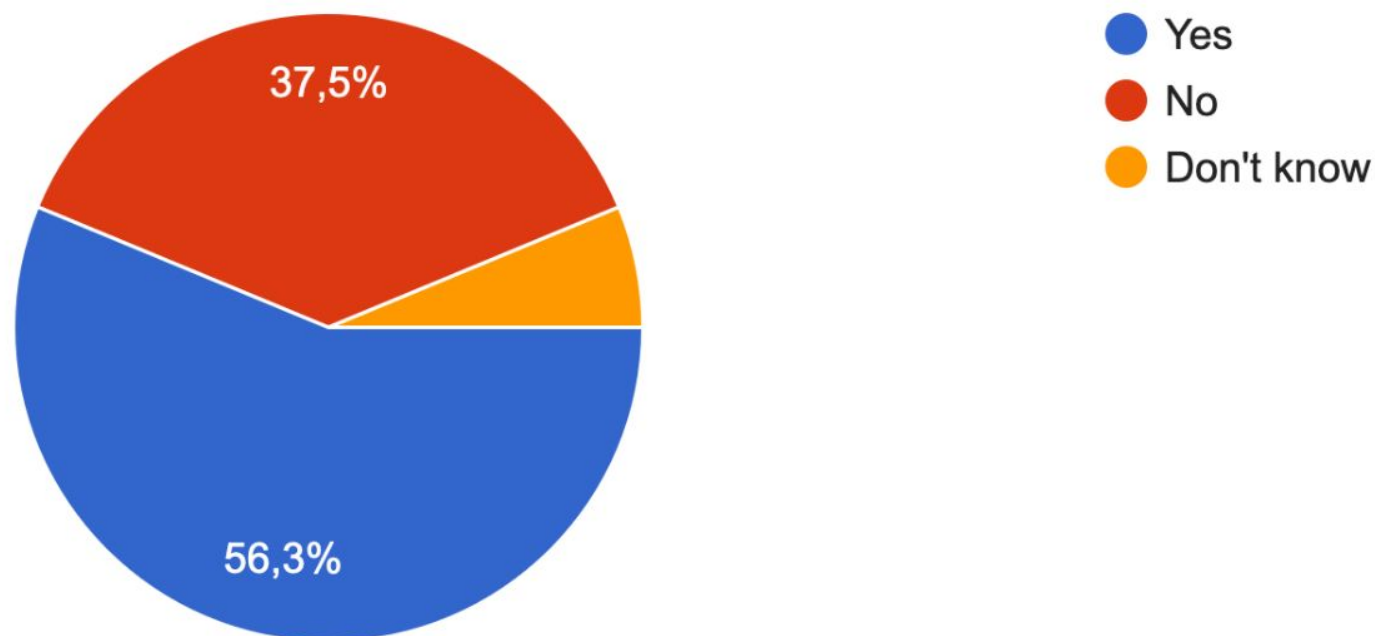
17 vastausta



## 5.2.2 Do you provide access to high performance computing (HPC) in/through your environment?

Please give details below

16 vastausta



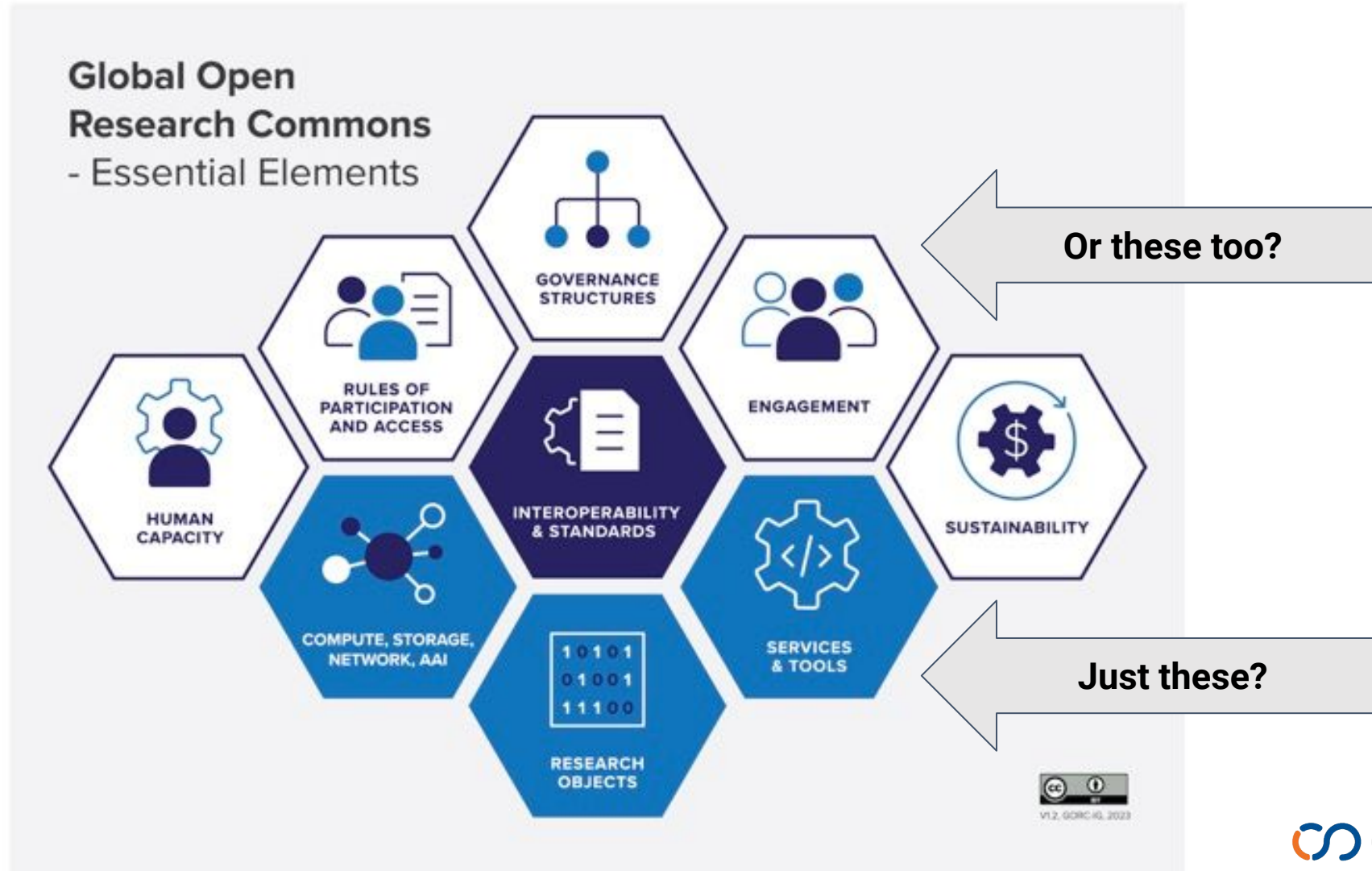
# Next generations capabilities

Question: Do you have plans for next generation capabilities?

- 10 responded in affirmative, 2 negative
- 4 answered just yes
- Rest were planning to include these capabilities
  - GPU and super computing resources capabilities.
  - HPC and GPU -capabilities
  - Quantum computing infrastructure, AI specialized systems, LEXIS platform extensions and more.
  - HPC access, containerisation and setting up an analytics platform on top.
  - Secure Computing cluster to provide larger computational resources and improve the efficiency of their use.
  - 1) Integrating SANE in scientific workflows, 2) supercomputer offloading, 3) better internal collaboration tooling



# How to capture all relevant capabilities?



May all your problems be  
technical ones



# Ecosystem update for EOSC-ENTRUST

Date: 8 October

Time: 10-11 CEST

## Agenda

- Short update on Common European Data Spaces, Heidi Laine
- RDA TRE WG & EGI TRE WG, Ville Tenhunen
  - Includes results from the EGI TRE WG's landscape analysis work



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# Requirement gathering framework and gap analysis

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Abdulrahman Azab (Sigma2), Provider Forum (WP10)



Funded by  
the European Union

# Drivers

A portfolio of Multidisciplinary Drivers informs and validates the blueprint.

- Driver 1: **Federated Human Genomics** as a catalyst for European TRE provision
- Driver 2: Common standards to enable trans-national sharing of **administrative/register and social science data**
- Driver 3: Enabling secure transnational re-use of **clinical research data** in a legally and ethically compliant manner
- Driver 4: **Public-Private interactions** between TRE in health and environmental data

# Provider forum

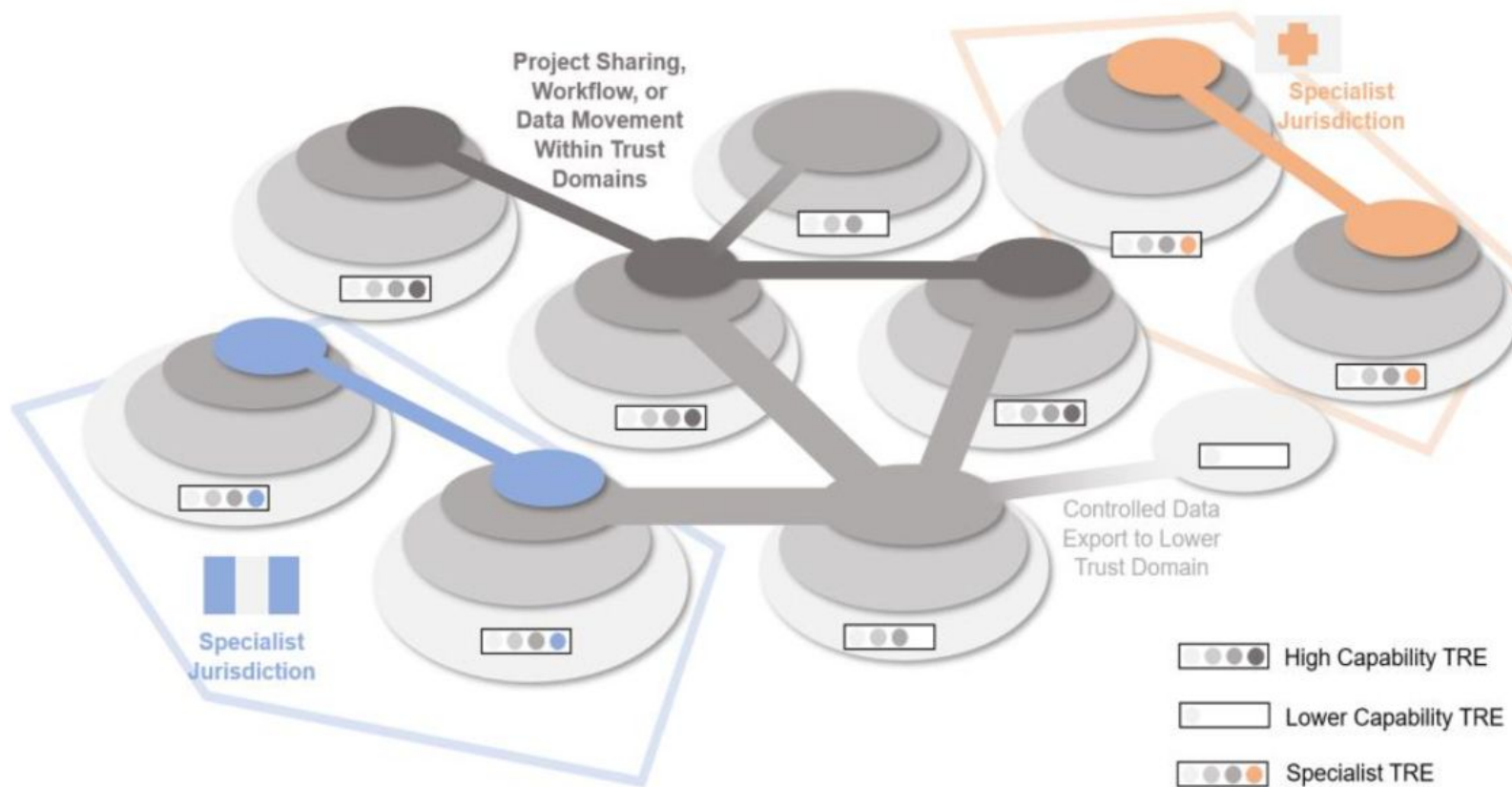
The Provider Forum is an open platform for convergence of TREs including co-development of composable services and common processes (where the national requirements are visible to users and other providers).

- The Provider Forum collects requirements, challenges and opportunities for making TREs part of the EOSC offering. Its wide participation is a unique opportunity to give input for further development of the EOSC itself.
- To be sustained as a platform for knowledge sharing, collaboration and discussion beyond the EOSC-ENTRUST project.



# Provider Forum

TRE Providers Forum consolidate existing expertise and good practices for the common interoperability blueprint.



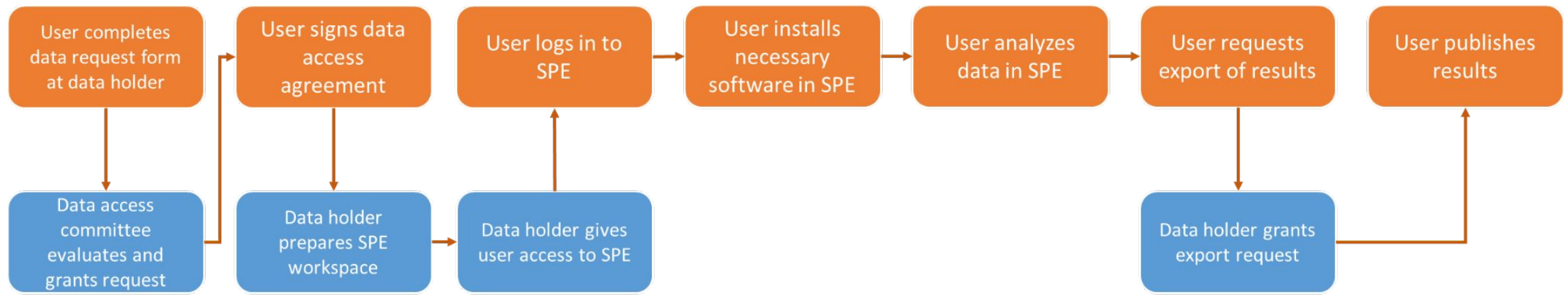


# TRE state-of the art capability mapping and gap analysis (T4.2)

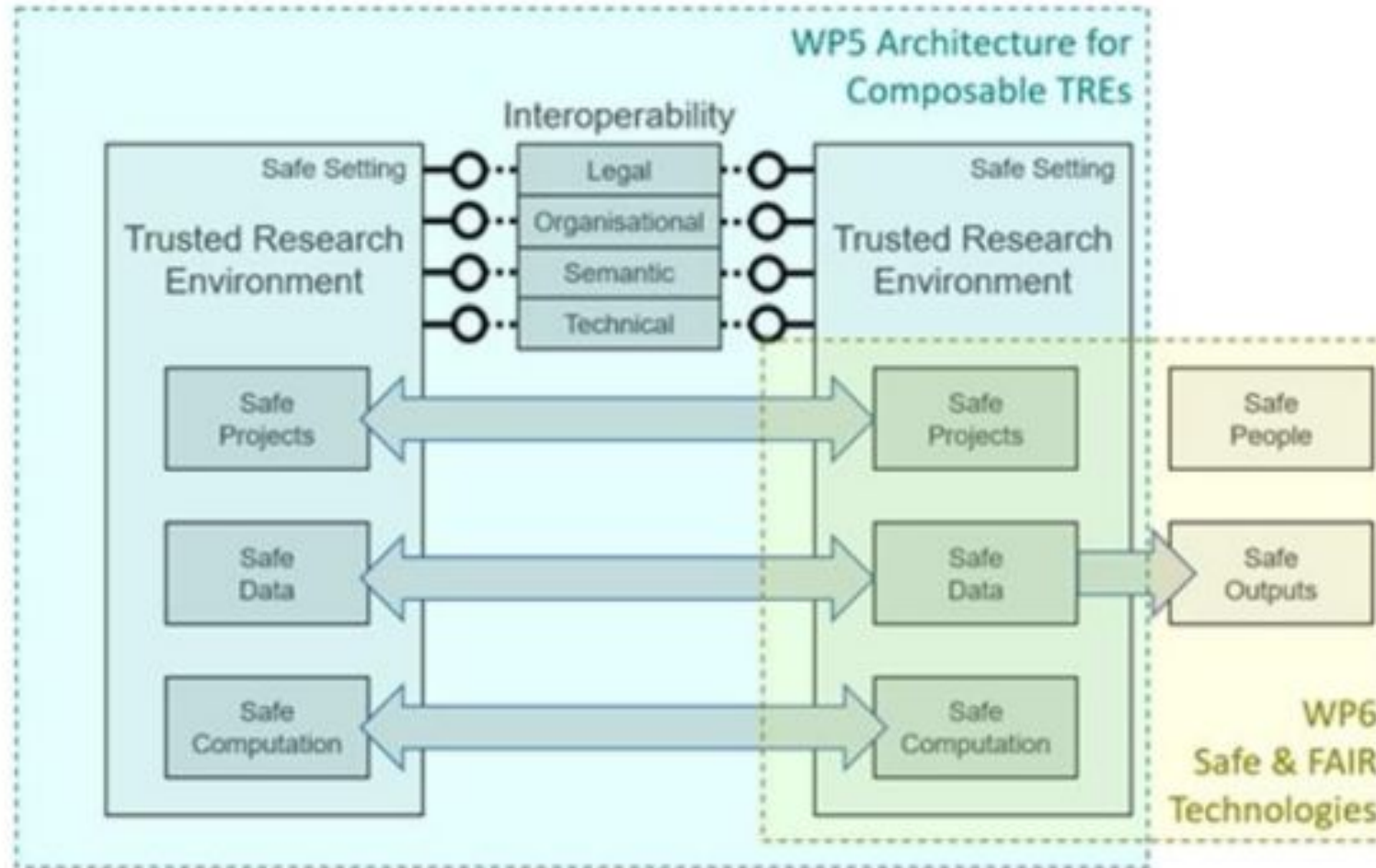
Capability mapping of the TREs enhancing the inventory of TREs.

- Includes a listing of used reference architectures.
- Establish a requirements management framework and identify gaps in the existing services.
- The outcomes are delivered as input for the blueprint architecture and discussed in the first Evaluation and Adoption Workshop.

# Scope and framework of the requirements



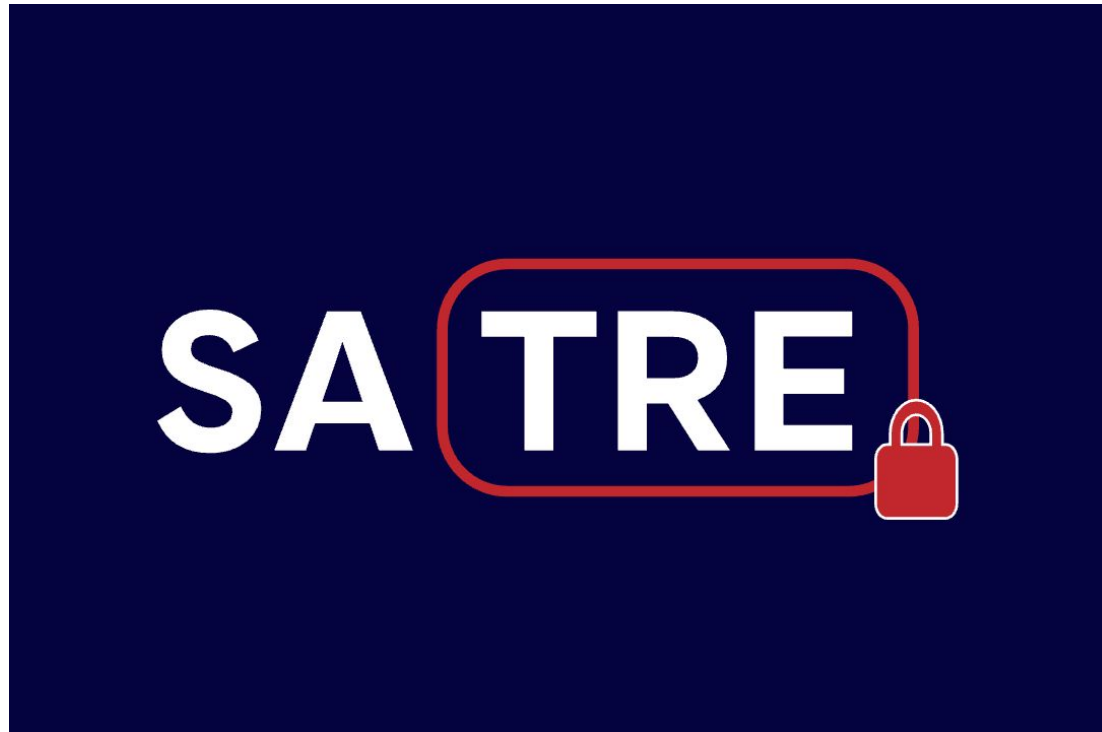
# EOSC-ENTRUST Blueprint



# Listing of used reference architectures

- SATRE
- DARE UK

# Standard Architecture for Trusted Research Environments



Health  
Informatics  
Centre

UCL ADVANCED RESEARCH  
COMPUTING CENTRE



UCL

The  
Alan Turing  
Institute

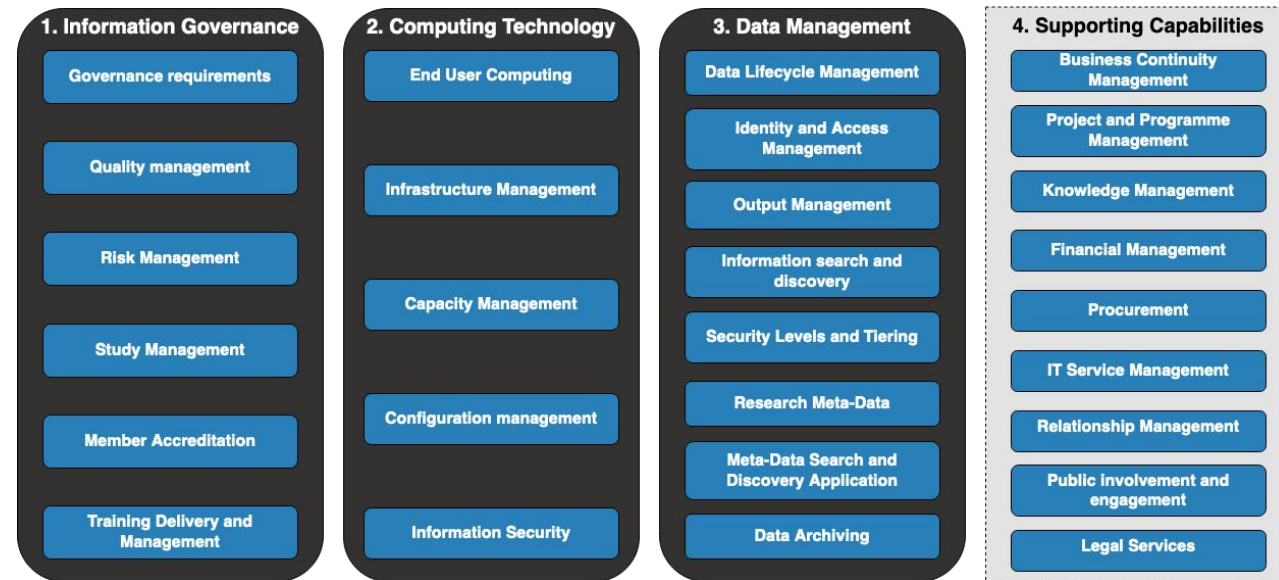
U  
Ulster  
University

Research  
Data  
Scotland

Source: [SATRE Presentation](#)

# What is it?

- A guide on how to build and run a TRE
- Four Pillars
  - Information Governance
  - Computing Technology
  - Data Management
  - Supporting Capabilities
- 29 Capabilities
  - 160 statements
    - 75 mandatory
- Applicable to almost all UK TREs

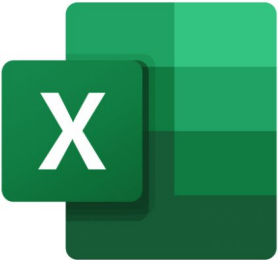


Source: [SATRE Presentation](#)

<https://satre-specification.readthedocs.io>



	A	B	C	D	E	F	
1	Section	Item	Statement	Guidance	Importance	Score	Response
2	Information governance	1.1.1.	You must gather and monitor the information governance requirements needed to fulfil any legal, regulatory and ethical standards.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
3	Information governance	1.1.2.	You must ensure controls are implemented to ensure the requirements are met.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
4	Information governance	1.1.3.	You must ensure there are adequate resources to meet information governance requirements.		Mandatory	1	ISO 27001, Scottish Safe Haven charter, DSPT
5	Information governance	1.2.1.	You must ensure that changes to policies and standard operating procedures can only be made by trusted individuals.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
6	Information governance	1.2.2.	You must use versioning and a codified change procedure for all policies and standard operating procedures.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
7	Information governance	1.2.3.	You should measure the performance of information governance within the TRE with regular reporting available to your TRE organisation's management team.		Recommended	1	
8	Information governance	1.2.4.	You must audit your TRE organisation against relevant requirements and standards.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
9	Information governance	1.2.5.	You must report on and share outcomes of each audit of your TRE organisation with the required bodies.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
10	Information governance	1.2.6.	You must ensure that suppliers, contractors and sub-contractors with access to your TRE align with your security requirements.		Mandatory	1	
11	Information governance	1.2.7.	You must monitor compliance of your suppliers with the terms of the contracts.		Mandatory	1	
12	Information governance	1.2.8.	You must track and maintain any physical assets used by your TRE.		Mandatory (where physical assets are in scope)	2	ISO 27001, Scottish Safe Haven charter, DSPT
13	Information governance	1.2.9.	You must log, track and resolve any issues resulting from deviations from processes, incidents and audit findings.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
14	Information governance	1.2.10.	You must use reported issues to inform changes, such as for process improvement and risk management.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
15	Information governance	1.2.11.	You should collect and maintain quality management data for measuring the effectiveness of a TRE.		Recommended	1	Regularly ask users for feedback. Monitor technical performance.
16	Information governance	1.2.12.	You could use a QMS (Quality Management System) to standardise and automate quality management tasks and workflows, and to generate quality data and reports auto		Optional	2	ISO 27001, Scottish Safe Haven charter, DSPT
17	Information governance	1.3.1.	You must have a way to score risk to understand the underlying severity.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
18	Information governance	1.3.2.	You must carry out a data processing assessment for all projects requiring a TRE.		Mandatory	2	DPIA, etc
19	Information governance	1.3.3.	You must have a process for designing, implementing and recording risk mitigations where indicated by a risk assessment.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
20	Information governance	1.3.4.	You must have a clear set of roles and responsibilities relating to risk including who owns risks and how they are escalated and delegated.		Mandatory	2	
21	Information governance	1.3.5.	You must understand the risk appetite of your TRE organisation.		Mandatory	2	
22	Information governance	1.4.1.	You must have checks in place to ensure a project has the legal, financial and ethical requirements in place for the duration of the project.		Mandatory	2	
23	Information governance	1.4.2.	You must have checks in place to ensure that any time limited compliance requirements are maintained.		Mandatory	2	Managed through JIRA assets
24	Information governance	1.4.3.	You must have checks in place to ensure that changes in regulations are met for a project.		Mandatory	1	Yes for legal regulations
25	Information governance	1.4.4.	You must have standard processes in place for the end of a project, that follow all legal requirements and data security best practice.		Mandatory	1	Have processes
26	Information governance	1.4.5.	You could implement a portal that can provide a workflow engine and database which automates the processes within this capability.		Optional	1	Implemented ISMS that abides by the above. E.g. forms to create new project, governance, JIRA workflows, etc
27	Information governance	1.4.6.	You must keep a complete record of all the data assets held within the system.		Mandatory	1	ISO 27001, Scottish Safe Haven charter, DSPT
28	Information governance	1.4.7.	You should keep a complete record of all the research studies and projects within the TRE current and past.		Recommended	2	JIRA, sharepoint/folios
29	Information governance	1.5.1.	You must have a robust method for identifying accredited members of your TRE organisation, prior to their accessing of sensitive data.		Mandatory	2	Data use declaration, confidentiality agreements, MRC training
30	Information governance	1.5.2.	You must have clear onboarding processes in place for all roles within your TRE organisation.		Mandatory	1	Have processes
31	Information governance	1.5.3.	You must have a set of services to manage access to resources based on identity.		Mandatory	2	Identity management, Active Directory, Keycloak
32	Information governance	1.5.4.	You must not give anyone access to datasets without agreement from the Data Controller.		Mandatory	2	ISO 27001, Scottish Safe Haven charter, DSPT
33	Information governance	1.5.5.	You must have robust and secure applications in place to authenticate users (and services) within the TRE.		Mandatory	2	Identity management, Active Directory, Keycloak
34	Information governance	1.5.6.	You must give each user of the TRE a unique logon with changes to any records strictly controlled.		Mandatory	2	Identity management, Active Directory, Keycloak
35	Information governance	1.6.1.	You must determine what training is relevant for all roles within the TRE organisation.		Mandatory	1	MRC training, in-house cyber security training
36	Information governance	1.6.2.	You must ensure that relevant training is available for all roles within the TRE organisation.		Mandatory	1	MRC training, in-house cyber security training
37	Information governance	1.6.3.	You must provide repeat or updated training where necessary to account for changes in competency requirements.		Mandatory	2	Annual
38	Information governance	1.6.4.	You must maintain accurate training records that are directly tied to the role and access levels within the TRE.		Mandatory	2	JIRA Asset management
39	Information governance	1.6.5.	You should accept proof of relevant training certifications from trusted third parties.		Recommended	1	Accept some (e.g. MRC) but not ONS
40	Information governance	1.6.6.	You could have a training platform capable of delivering online training in a variety of formats.		Optional	0	
41	Information governance	1.6.7.	You could implement a learning management system (LMS) to manage courses and deliver training as required.		Optional	0	
42	Information governance	1.6.8.	You could ensure that any courses you use are available in standard, transferable formats.		Optional	0	
43	Information governance	1.6.9.	You could keep historical copies of courses in order to demonstrate competency at a given point in time.		Optional	0	
44	Computing technology and	2.1.1.	You must not allow users to copy data out of your TRE via the system clipboard.		Mandatory	2	Blocked by TRE
45	Computing technology and	2.1.2.	Your TRE workspace should provide an environment familiar to your users.		Recommended	2	Windows and Linux desktops, typical software or equivalent available
46	Computing technology and	2.1.3.	A TRE could restrict data access from data consumers entirely and provide an interface for submitting code.		Optional	0	Desktop TRE, we're not OpenSAFELY
47	Computing technology and	2.1.4.	Your TRE should be accessed via a user interface accessible using commonly available applications.		Recommended	2	Web browser
48	Computing technology and	2.1.5.	Your TRE must provide clear guidance on how to use software tools and work with data in the TRE.		Mandatory	1	
49	Computing technology and	2.1.6.	Your TRE should, where possible, automatically apply security related updates for user software.		Recommended	0	Currently don't do it, TRE workspaces are firewalled
50	Computing technology and	2.1.7.	Your TRE could provide shared services that are accessible to users in the same project.		Optional	1	We have some shared services e.g. MSSQL server
51	Computing technology and	2.1.8.	Your TRE must ensure that any shared services are only available to users working on the same project.		Mandatory	2	User access controls on shared services
52	Computing technology and	2.1.9.	You must mitigate and record any risks introduced by the use in your TRE of software that requires telemetry to function.		Mandatory	1	Improvement in recording required
53	Computing technology and	2.1.10.	Your TRE must provide software applications that are relevant to working with the data in the TRE.		Mandatory	2	We provide requested open-source packages, and commercial applications where licensed
54	Computing technology and	2.1.11.	Your TRE should provide tools to encourage best-practice in reproducibly analysing data.		Recommended	2	R, Python, and standard libraries are available
55	Computing technology and	2.1.12.	Your TRE could provide access to some public software repositories or container registries.		Optional	1	We provide limited access to some package repositories
56	Computing technology and	2.1.13.	Your TRE could tightly control which packages are available.		Optional	1	We limit which package repositories can be accessed
57	Computing technology and	2.1.14.	Your TRE must maintain segregation of users and data from different projects when using non-standard compute.		Mandatory	2	Flexibility of cloud compute means non-standard compute resources aren't shared
58	Computing technology and	2.1.15.	Your TRE should be able to provide access to high performance computing or other scalable compute resource if required by users.		Recommended	2	Available where required and funded
59	Computing technology and	2.1.16.	Your TRE should be able to provide access to accelerators such as GPUs if required by users.		Recommended	2	Available where required and funded
60	Computing technology and	2.1.17.	Your TRE could make data available to data consumers using common database systems such as PostgreSQL, MSSQL or MongoDB.		Optional	2	MSSQL is required by many users
61	Computing technology and	2.1.18.	Your TRE could integrate with large-scale data analytics tools for working with large datasets.		Optional	1	Offer HPC
62	Computing technology and	2.2.1.	You must have a documented procedure for deploying infrastructure.		Mandatory	2	GitHub workflows, ISO documentation
63	Computing technology and	2.2.2.	You should, where possible, automate any repeatable aspects of your deployment		Recommended	2	GitHub workflows



Source: SATRE Presentation

Response example: [NORTRE \(National Federation\)](#)



# Pan-UKRI infrastructure programme for secure, cross-domain sensitive data research



*“Enable a step-change in the UKRI’s/national research capability for secure sharing, linkage and analysis of sensitive data for research and innovation, timely and at scale for public benefit.”*

## DARE UK



Source: [DARE UK Presentation](#)

# Federation: Joining The Dots

- We have to federate TREs, and we have to start from where we are
  - Landscape version 0 is not a throwaway prototype!
- We need to connect existing services in a way that's
  - Secure and trustworthy
  - Governed and managed
  - Standardised and non-proprietary
  - Secure and trustworthy
- We need to do this in ways which cause the least disruption...
- ...support both remote query and data pooling...
- ...and are open to new participants

Source: [DARE UK Presentation](#)

# Driver Projects Key Results

- Defining TRE capabilities
  - **SATRE** developed a specification that gives us the first answer to “what is a TRE anyway?”
- (Semi-) automation of data risk assessment at TRE boundaries
  - **SARA** and **SACRO** demonstrated approaches to reducing frictions of data in and results out
- Federated query patterns
  - **TRE-FX** federated indirect queries via job submission
  - **TELEPORT** federated direct queries via polystore presentation
- Pop-up TREs
  - **TELEPORT** demonstrated dynamic provisioning with ongoing “approved state” sync using GitOps CI/CD
- Registry services
  - **TRE-FX** and **TELEPORT** demonstrated common researcher identities & project registration
- Common technologies
  - RO-Crates as an object exchange format (**TRE-FX**, **TELEPORT**, **SACRO**)
  - GA4GH Passports (OIDC JWT) as common researcher identity/authZ (**TRE-FX**, **TELEPORT**)
  - Docker and Kubernetes (everywhere)

Source: [DARE UK Presentation](#)

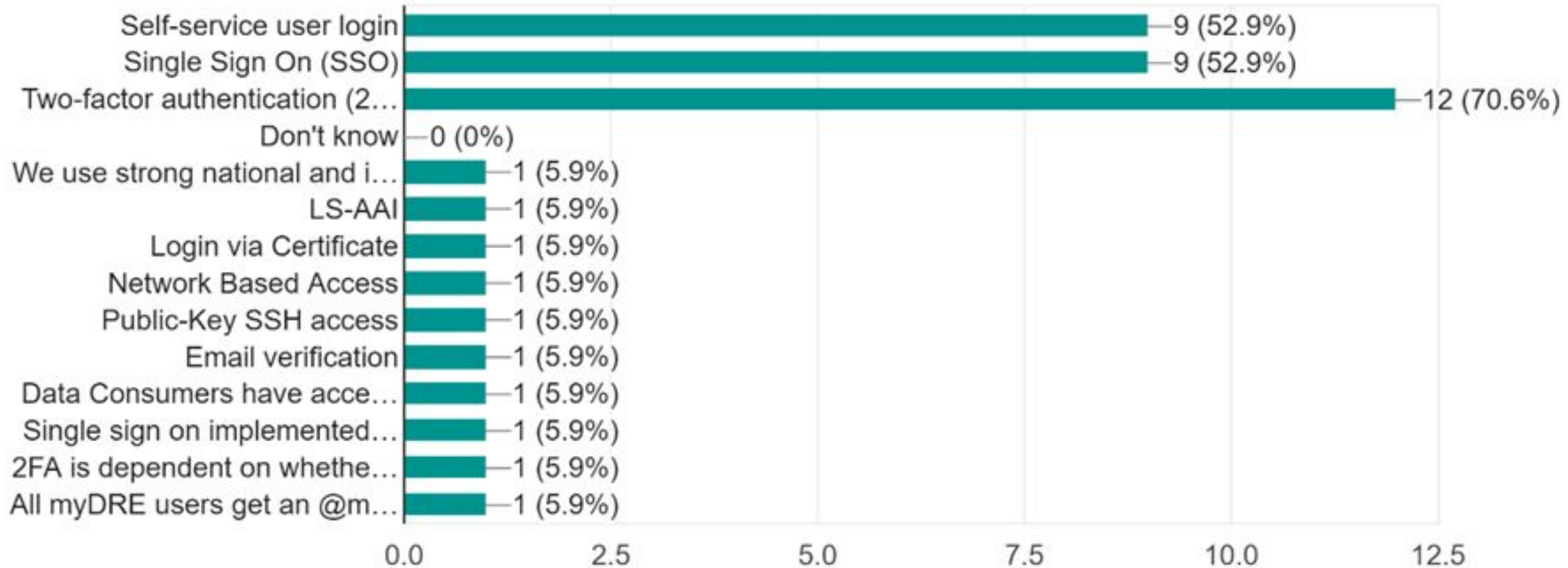
# Interoperability requirements from Drivers

1. Data transfer between environments
  - Different data from distinct environments
  - Encryption during transfer mandatory
  - Efficient data transfer protocols
2. User identity and access management
  - Verify user and role
  - Categorised data access levels (e.g. role-based access)
3. Data lifecycle management
  - Mechanisms for timely deletion of data
  - Integration and management of diverse sensitive data
4. Governance and compliance
  - Tailored governance models (e.g. private companies vs. public research org.)
  - Domestic and international standards and certification of compliance
  - Legal frameworks for data sharing
  - Allow diverse TREs (technical or resource constraints)
5. User training and standardisation
  - Researcher training compliant with access requirements
  - General training on curating and handling data in varied domains
  - Standardization of statistical disclosure control

# Driver requirements evaluation: Data Access

Driver 1	Data Encryption in transit	All data within the Trusted Research Environment must be encrypted in transit. This requirement aims to ensure that data is protected from unauthorized access or breaches.
Driver 1	Data Encryption at rest	All data within the Trusted Research Environment must be encrypted at rest. This requirement aims to ensure that data is protected from unauthorized access or breaches.
Driver 3	2-factor authentication for TRE users	2-factor authentication is a critical security measure in TREs to ensure that only authorized individuals can access sensitive data. E.g. username and password + OTP.

# TRE Capabilities: Data Access



NB! Encryption is mentioned as a requirement by some TREs



# Driver requirements evaluation: Policies 1

Driver 1	Data Sharing Agreement	Establish a formal data-sharing agreement among participating institutions. This agreement should outline the terms and conditions for sharing data, including licensing, access controls, and data use limitations.
Driver 1	Anonymization Agreement	Establish anonymization guidelines among participating institutions. This agreement should outline the set of techniques - and their use-cases - that best assure the privacy of the patient is respected
Driver 1	Technology agreement	The current landscape of available TREs makes quite difficult - if not directly impossible - to provide a single, comprehensive list of possible hardware or technologies to use.
Driver 3	Data Transfer Agreement	A TRE that wants to cover datasets from a specific data type needs to provide to potential data providers a <b>Data Transfer Agreement (DTA)</b> template that covers necessary requirements specific to the data type. DTAs at least per data type should be standardised but some flexibility should be provided to cover the different legal obligations of the data controllers (data providers).
Driver 3	Data Use Agreement	A TRE that wants to cover datasets from a specific data type needs to provide a model <b>Data Use Agreement (DUA)</b> that covers necessary requirements specific to the data type. DUAs should include access prerequisites, requirements and obligations.
Driver 3	Data Sharing Policy	A <b>Data Sharing Policy</b> / <b>Data Access Policy</b> is a common element needed for TREs operating with clinical trial data.

# Driver requirements evaluation: Policies 2

Driver 1	ISO 27001 Accreditation	
Driver 3	Certification	Demonstrate good information management and security via certifications: e.g., ISO/IEC 27001 - Information Security Management, ISO/IEC 27701 -Privacy Information Management

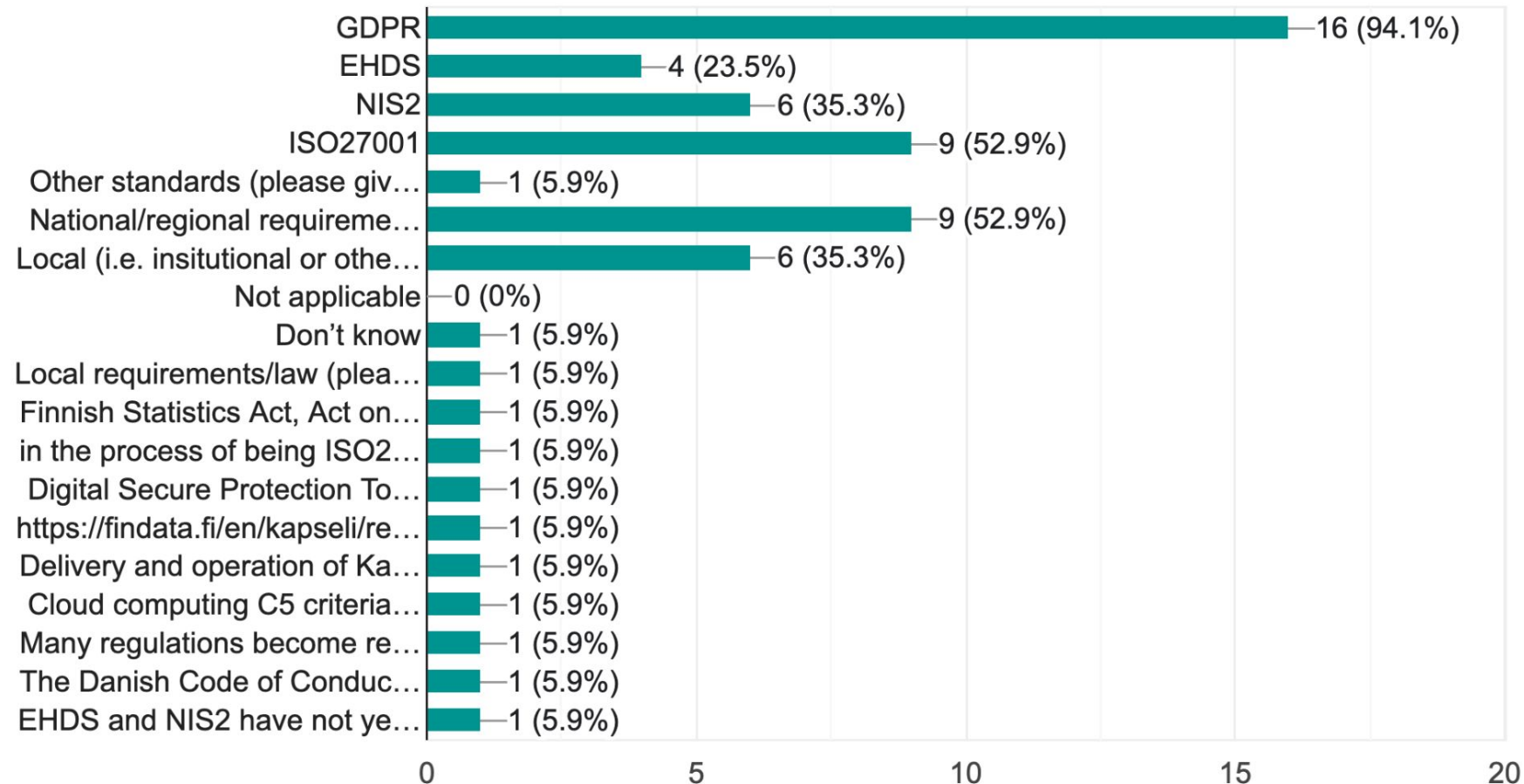
Metadata	Metadata available in one language (English)
Findability	Central Portal for research data discovery (improved CESSDA portal?, New portal, harvesting info of existing ones?)



# TRE Capabilities: Policies

2.2 What multinational, national, regional, or local legal or other binding requirements do you as the environment provider need to comply with?

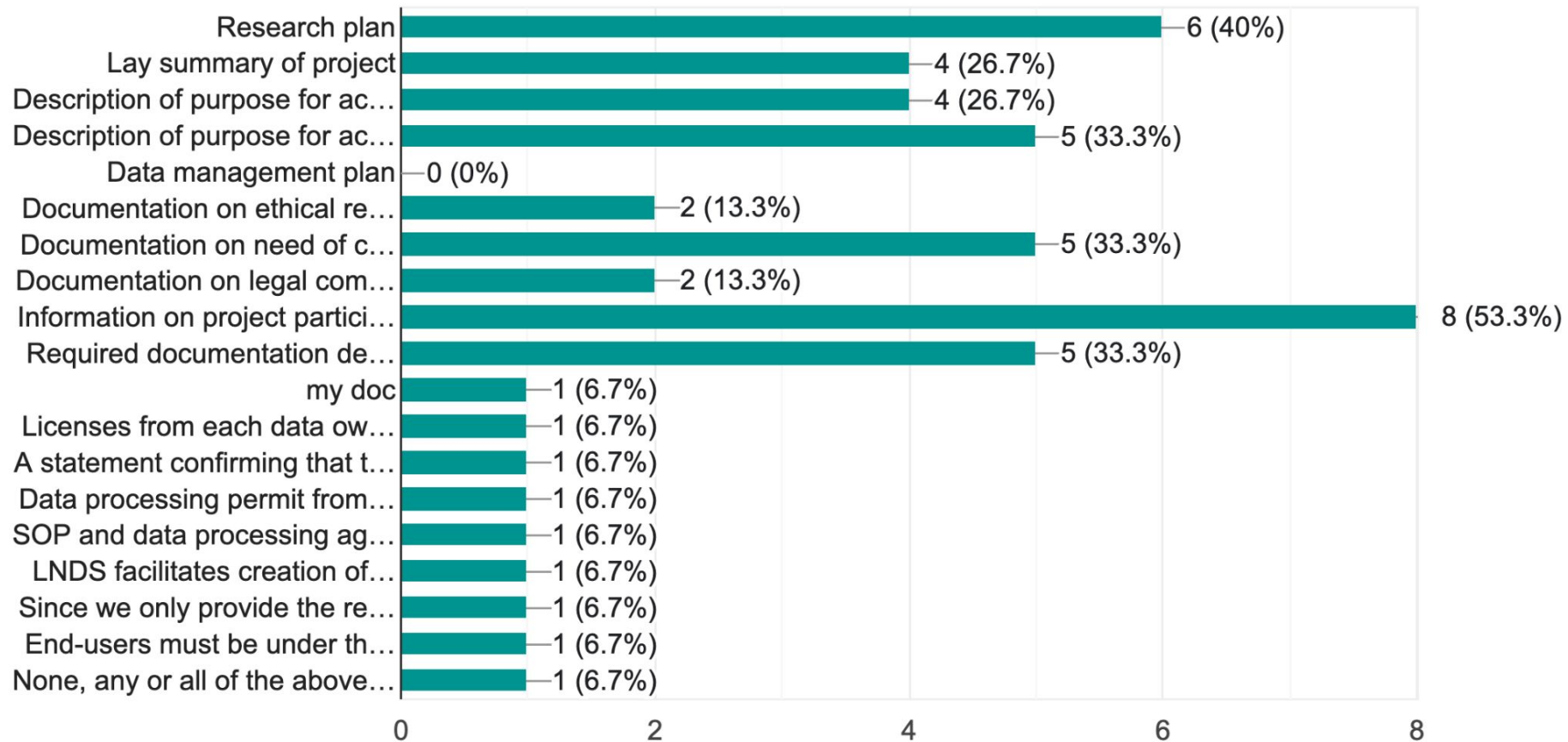
17 responses



# TRE Capabilities: Policies

## 2.3 What type of project documentation is required from end-users/projects to be granted access to the environments?

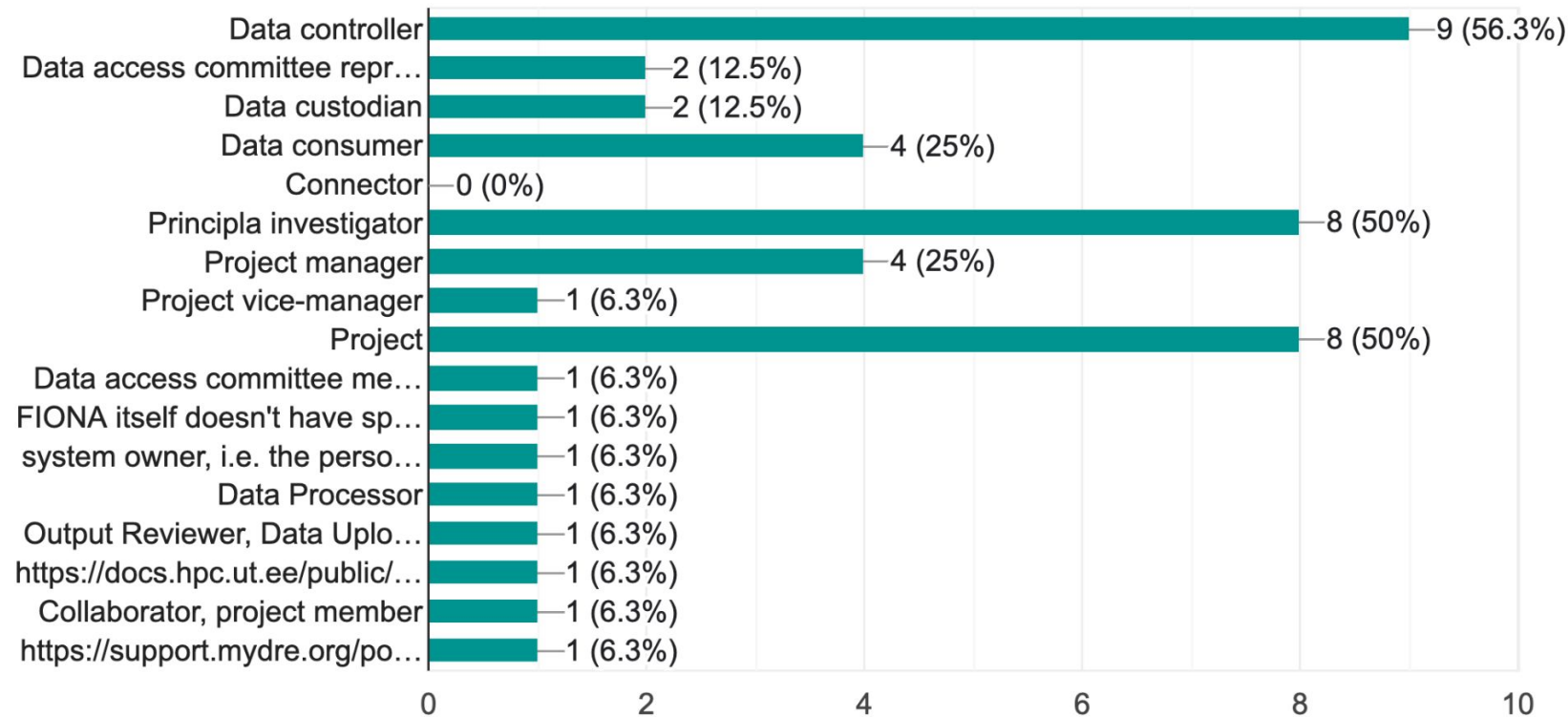
15 responses



# TRE Capabilities: Policies

3.1 Does the environment have a list of defined roles? If there's a public listing available, please provide a link in the open answer ("other")

16 responses



# Ethical Assessment and legal frameworks

## TREs

- Internal projects
- ***Federation?***

# Ethical Assessment for NORTRE Projects

Before starting a project in NORTRE, it is mandatory to obtain **ethical approval** for handling personal data in your research. This approval must come from one of the following authorized entities:

- REK (Regional Committees for Medical and Health Research Ethics): Primarily responsible for medical and health-related research involving sensitive personal data.
- SIKT (Norwegian Agency for Shared Services in Education and Research): Focuses on research across various fields, ensuring proper data handling in compliance with privacy laws.
- Datatilsynet (The Norwegian Data Protection Authority): Monitors and enforces compliance with privacy regulations, including GDPR, ensuring the protection of personal data.
- Data Protection Officer/Official: Provides guidance and approval for personal data management in accordance with institutional and legal frameworks.
- Additionally, a Data Protection Impact Assessment (DPIA) is required for projects involving high-risk processing of personal data. The DPIA ensures that risks to privacy and data security are evaluated and mitigated before the research begins.

# Ensuring Legal Compliance: IT4Innovations' Requirements for Project Work and Data Analysis

## HPC Resources Use

- **Purpose:** HPC (High-Performance Computing) resources provided by IT4I should align with the approved project scope.
- **Access Controls:** Users must not alter or bypass access controls to perform unauthorized actions.
- **Account Security:** Promptly report compromised accounts to IT4I via support@it4i.cz.
- **Vulnerabilities:** Users are obligated to report any detected vulnerabilities or data security threats.
- **Misuse Reporting:** IT4I personnel and users must address and report misuse, abuse, and criminal activities related to HPC technologies.

## Data Handling

- **Data Categorization:** Authors/owners must correctly categorize data as sensitive or non-sensitive.
- **Secure Handling:** Owners of sensitive information are responsible for secure handling, transmission, processing, storage, and disposal.
- **Unauthorized Access:** Users are prohibited from attempting unauthorized data access or modifications.
- **IT4I's Right:** IT4I reserves the right to deny access to its infrastructure based on legal or international restrictions.

Within our **ISO 27001 framework**, there is a requirement to establish a specialized contract with external institutions.

We have shared services as **part of e-INFRA CZ, including a unified AAI (Authentication and Authorization Infrastructure), where there is also a contract defining precise access roles to data, among other things.**

# Legal Framework for TRE at LNDS (LU)

The following **legal framework** is used to inform LNDS SPE service requirements:

## EU Legislation:

- Data Governance Act (DGA);
- General Data Protection Regulation (GDPR)  
including Data Processing Agreements as per Article 28 / role of Data Processors;
- EU Health Data Space (EHDS) - *not yet adopted into EU law.*

## Standards:

- ISO 27001, 27001, 27701

## Guidance:

- FinData [Annex 1, Regulation 1/2022](#)

## Documentation:

- (a) Terms of Service, (b) contracts with 3rd party subprocessors & (c) data processing agreements (as per GDPR data processor obligations).

**\*\*Ethical requirements will more so be assessed by the Data Holders, Data Users, and Researchers, in the preliminary steps before uploading data to the SPE platform, etc.**

# Ethical/Legal Framework and Requirements of ARIS HPC (GRNET)

## ARIS HPC:

- **EU Legislation and Standards:**

- GDPR, NIS2
- ISO27001

- **Documentation:**

- Research plan
- Description of purpose for accessing and using the environment
- Documentation on need of computational capacity
- Information on project participants (i.e. environment end-users)

- **Specific Legal/Ethical Requirements:**

- **Only for Academia/Research users – no access granted to SMEs/Industry**
- Publication of research results is included in the eligibility criteria
- Users must acknowledge the use of GRNET resources in all publications related to their production/development project
- Users indicate the level of Confidentiality required for their project
- Access to GRNET's HPC facilities is granted on an individual basis (personal account) - no sharing of accounts allowed



# Ethical/Legal Framework and Requirements of **HARMONI:** Harmoni (GRNET)

- **EU Legislation and Standards:**

- GDPR, NIS2,
- ISO27001,
- National/regional requirements

- **Documentation:**

- MoU between GRNET and the Ministry of Health (Hospitals are the users)

- **Specific Legal/Ethical Requirements:**

- **The institutions included as users must be hospitals, already having medical imaging archiving system (LOCAL PACS), appropriately configured to automatically send and retrieve exams through the Gateway Server to/from the diagnostic imaging archive solution (DIAS); if they don't, the transmission will be carried out via diagnostic units using the DICOM standard**
- Controlled access to the server is required and equipment provided by GRNET (Gateway server) must be protected from physical damage - also online UPS system for the Gateway is mandatory, as well as alternative generators

# Ethical/Legal Framework and Requirements of de.NBI Cloud (UNIBI)

## de.NBI Cloud:

- **EU Legislation and Standards:**

- GDPR, (NIS2, KRITIS: critical infrastructures, application unclear ATM)
- ISO 27001, 27017, BSI C5 (Cloud Computing Compliance Criteria Catalogue)

- **Documentation:**

- Research Data Management Plan
- Approval of ethics committee or similar authority
- Description of purpose for accessing and using the environment
- Justification for computational capacity and special resources (e.g. high RAM / CPU or GPUs)
- Information on project participants (rights and roles)
- Data Processing Agreement between legally responsible PI and hosting location with inclusion of resp. data protection officers, procedural directory & TOMs (for mutual audits between data holder and data processor), data protection impact assessment (for highly sensitive data)
- [Terms of Use](#) (detailing rights and obligations, responsibilities etc.)

- **Specific Legal/Ethical Requirements:**

- **Only for academic research use**
- PI is required to work for a public German research institution – no access granted to SMEs/Industry, unless cooperation with PI
- PIs can select which information details to release about their project (e.g. nothing, title only, description, down to requested resources)
- Publication of research results must acknowledge de.NBI Cloud funding statement.

# Driver requirements evaluation: Federation

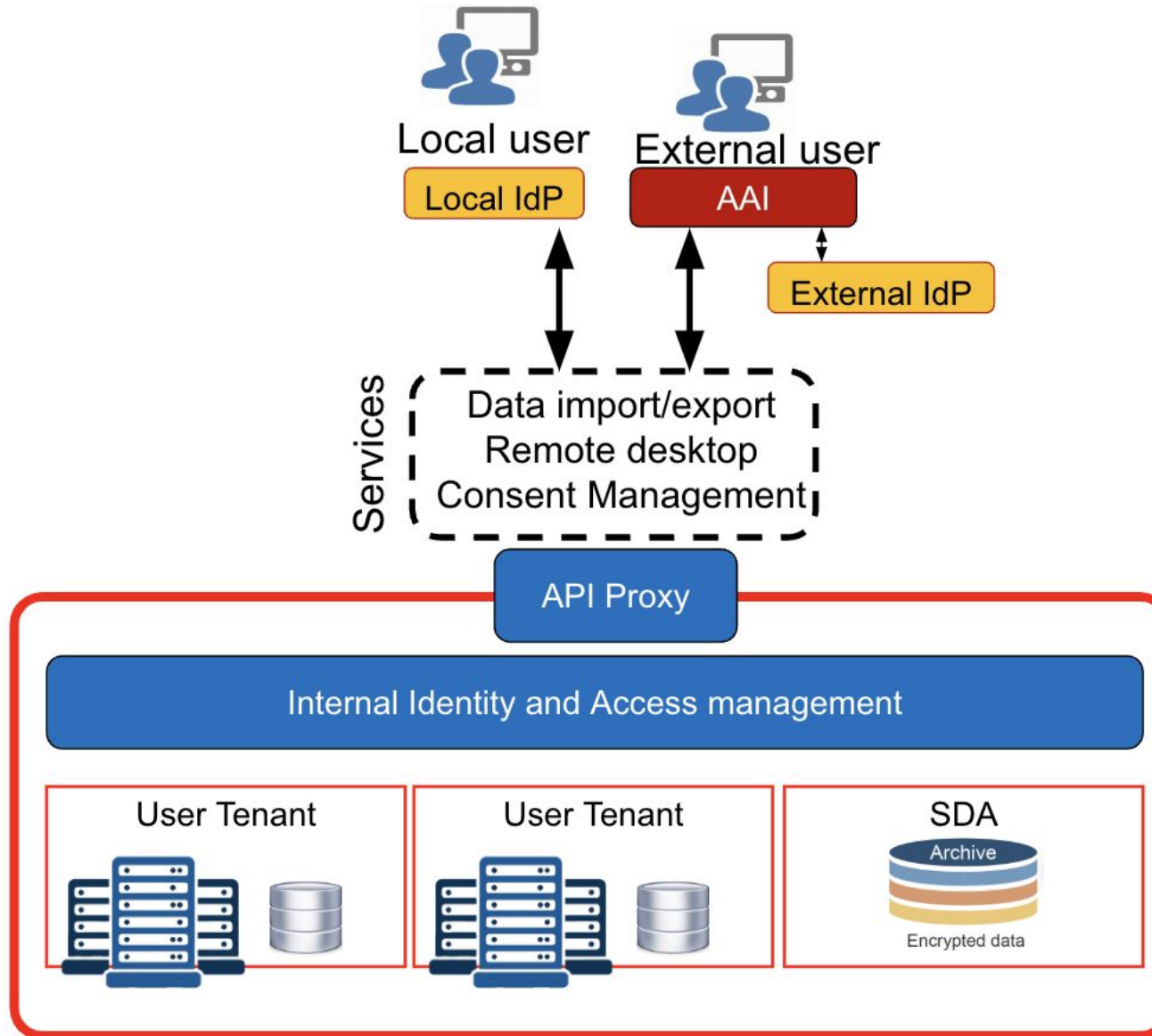
## Anne's presentation

### Alignment with DARE-UK

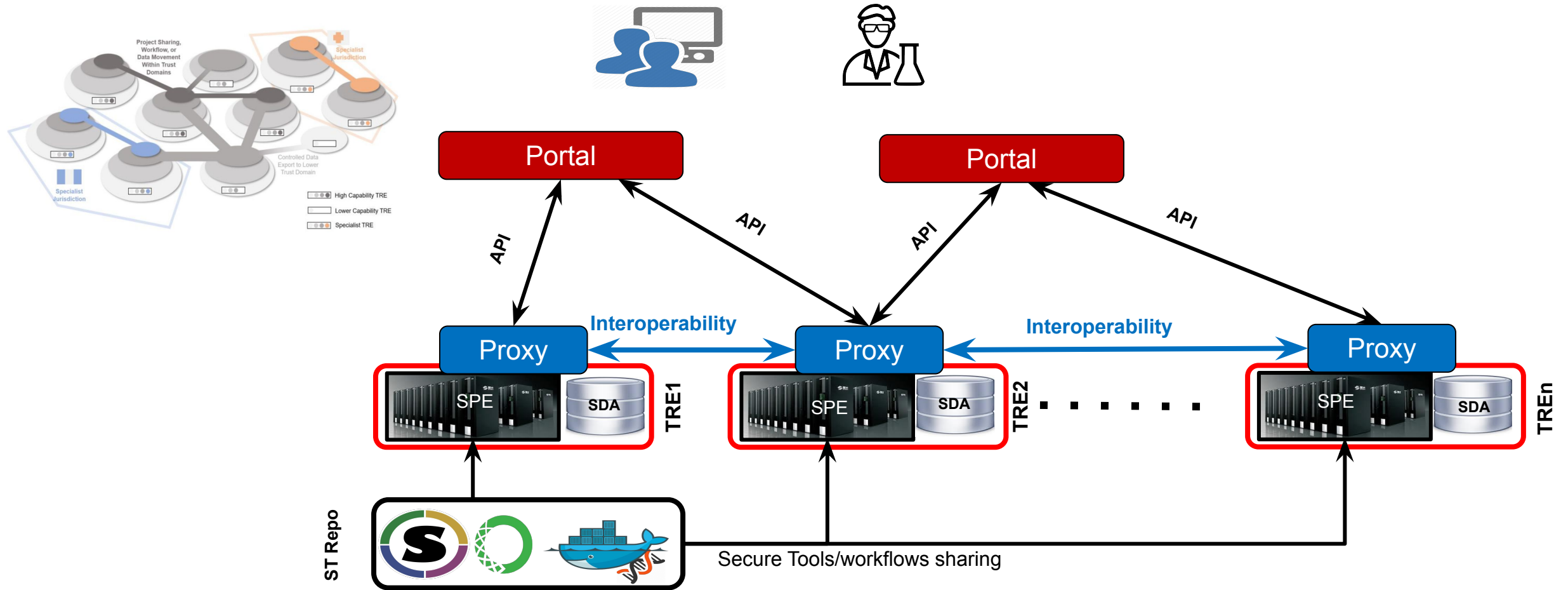
**A federated network with shared services** (as in DARE-UK architecture) provides a possible solution for multiple requirements:

- Data transfer between environments
- Data discovery
- Internet connection from within TRE (Drivers 1 & 4: should-have, Driver 2: won't have) - functional requirement: using data from outside TRE, Examples: annotation of genomes, reference sequences for sequence alignment, usage of ontologies and other open resources
- Scalable infrastructure
- Publishing and re-using code and workflows

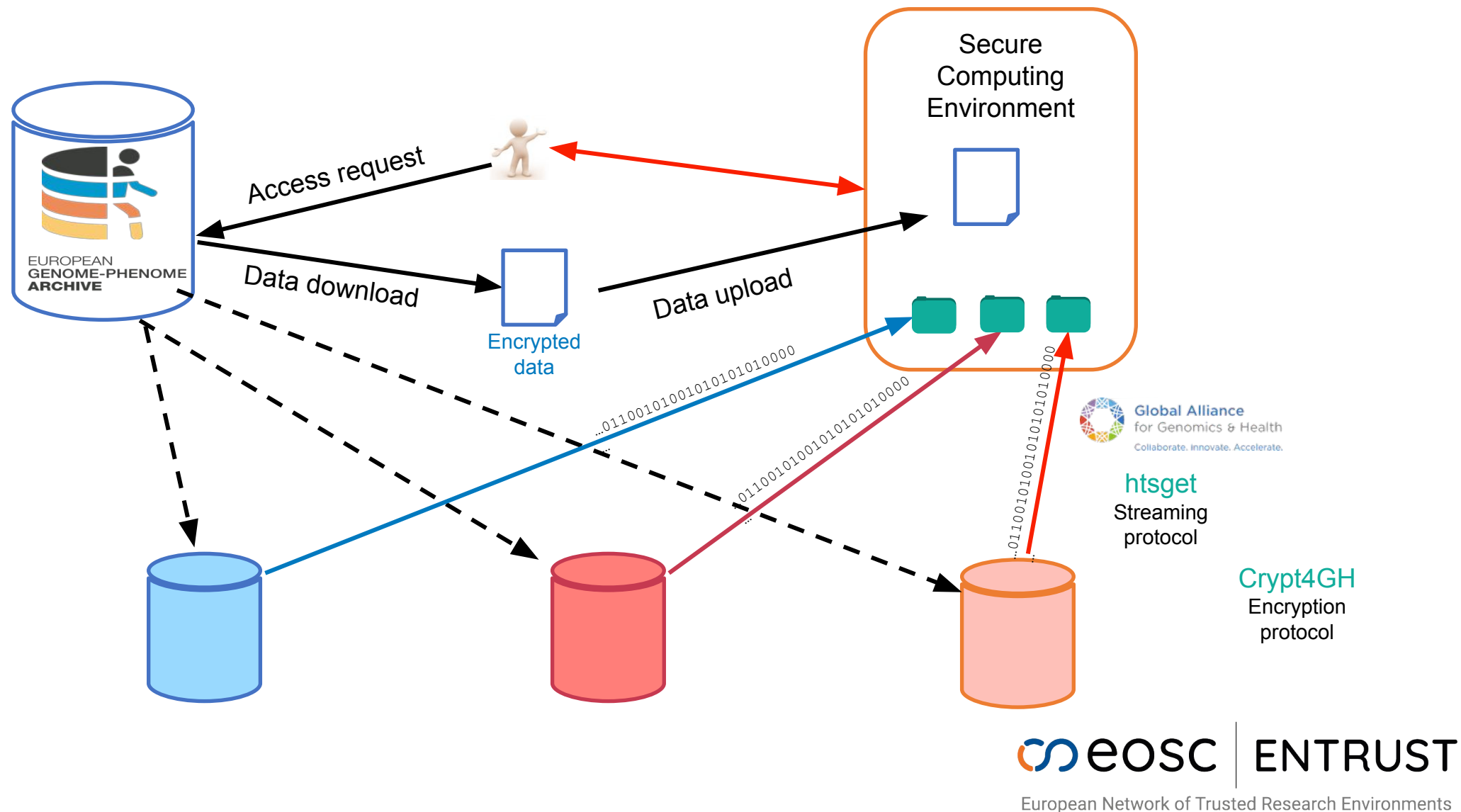
# Can we establish a complete federation?



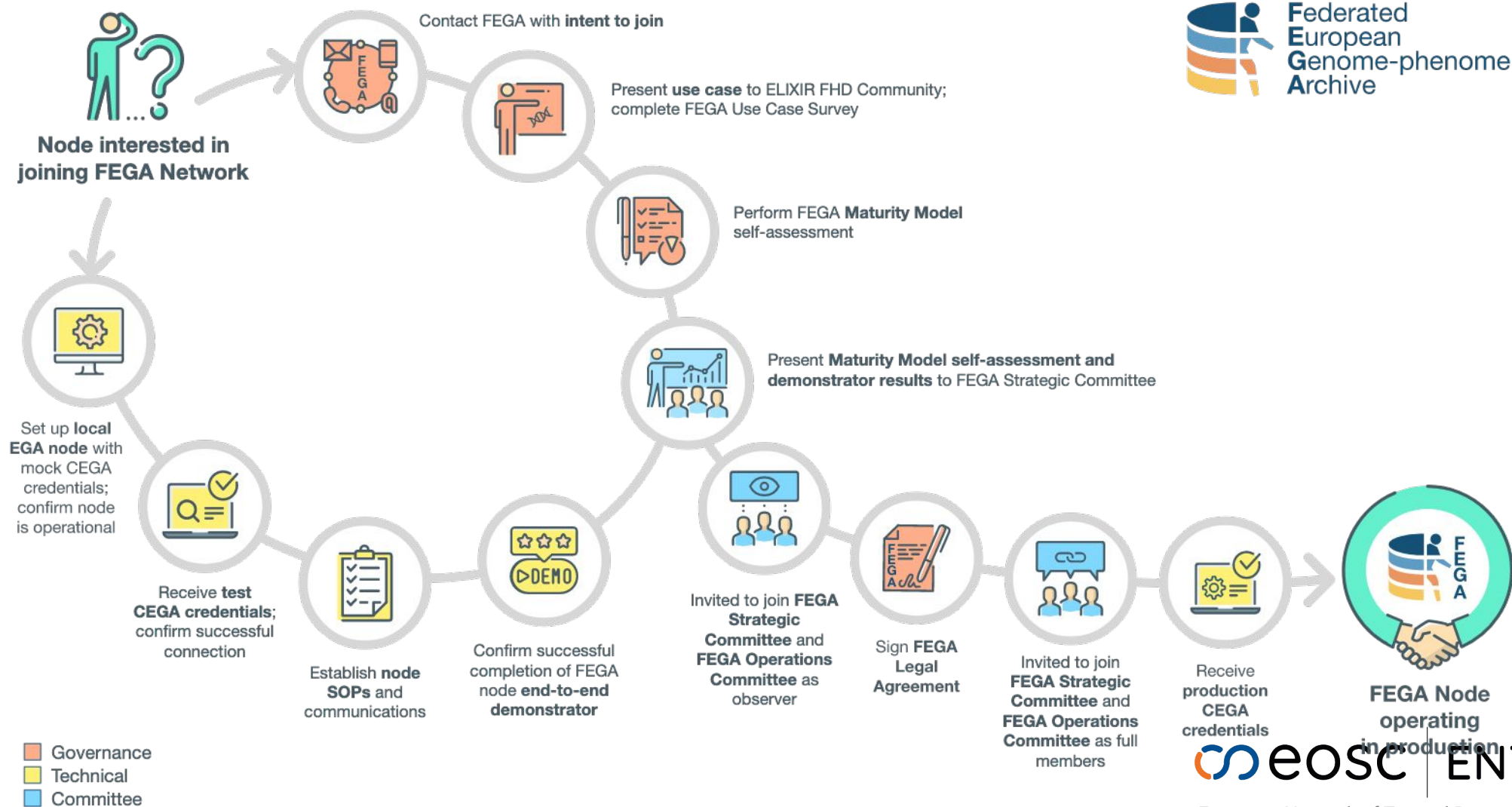
# Can we establish a complete federation?



# Federation Example: Federated European Genome-Phenome Archive (FEGA)



# Federation Example: Federated European Genome-Phenome Archive (FEGA)







---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc-entrust](https://twitter.com/eosc-entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# Survey on TREs - Providers

Create an inventory of TREs operated by the TRE provider forum members.

- The survey serves the purpose of the inventory, as well as capability mapping and gap analysis.
- Collect an initial set of high-level requirements and best practices on TREs from the provider forum members.
- Give input for the TRE blueprint, to be developed by the work package on architecture.

# Survey on TREs - Providers

The survey is divided into six parts:

1. **Administrative information**
2. **Safe Projects** - Is the data being used appropriately?
3. **Safe People** - Who is going to be accessing the data?
4. **Safe Data** - How will the data be accessed?
5. **Safe Settings** - What computing/analytics services does the environment provide?
6. **Safe Outputs** - How do users export data from your environment?

# TRE Survey Responses

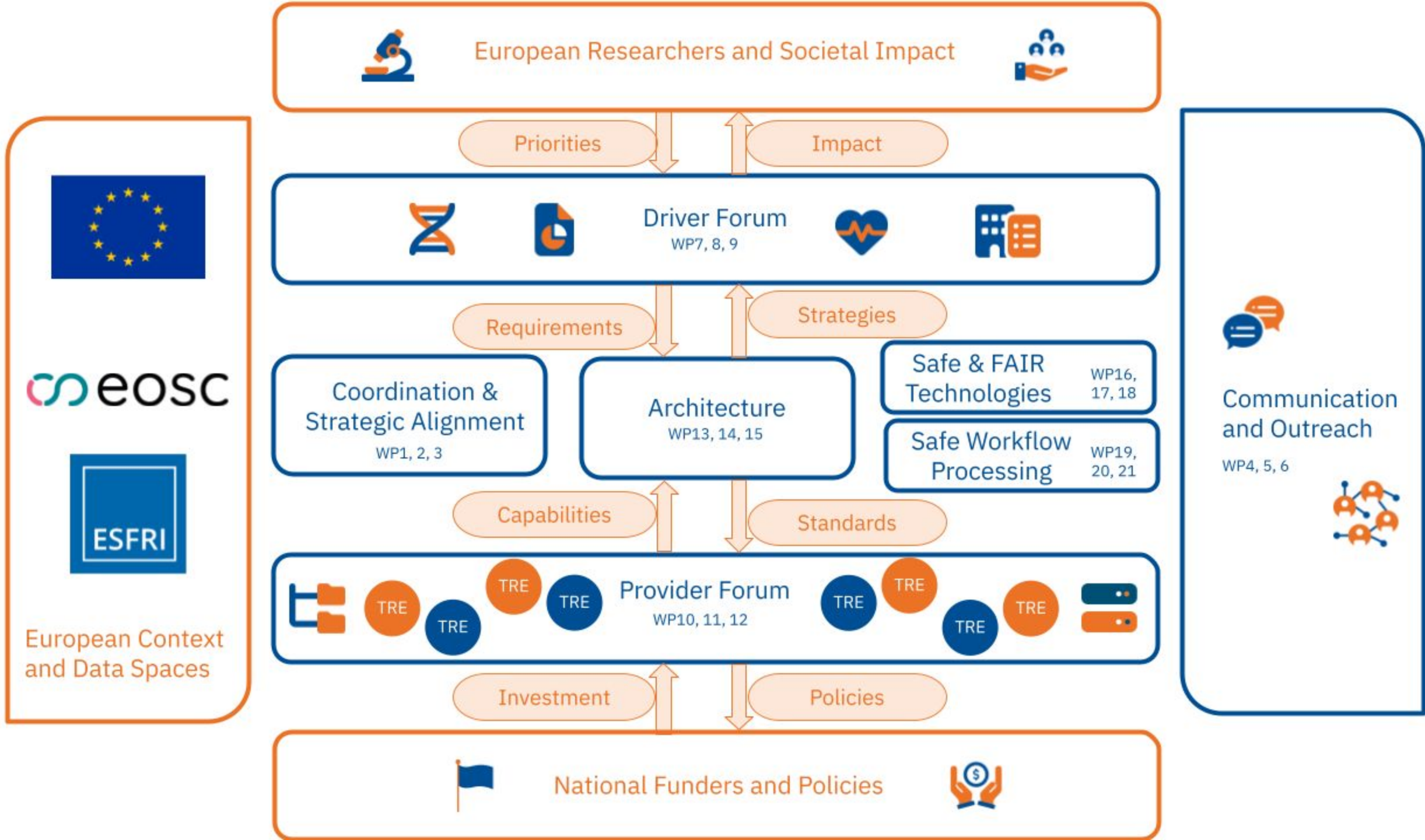
<https://docs.google.com/forms/d/1-EKxhbxwzLjRI7qCVyvmPiy1ZXxega80SNFbbkVtZYY/edit#responses>

# Requirements - Drivers

<b>Data Security</b>	Requirements related to data encryption, access controls, and secure data storage.
<b>Data Privacy</b>	Policies on personal data protection, compliance with privacy regulations (e.g., GDPR), and anonymization techniques.
<b>Data Governance</b>	Standards for data management, data stewardship, and data quality.
<b>Data Sharing and Collaboration</b>	Guidelines for sharing data among institutions, including licensing, data use agreements, and collaborative research frameworks.
<b>Compliance and Regulation</b>	Requirements to ensure compliance with legal and regulatory frameworks (e.g., GDPR, HIPAA).
<b>Audit and Monitoring</b>	Procedures for auditing data access and use, as well as monitoring for security incidents.
<b>Identity and Access Management</b>	Policies for user authentication, authorization, and role-based access controls.
<b>Data Integrity</b>	Mechanisms to ensure data accuracy, consistency, and reliability.
<b>Incident Response and Recovery</b>	Plans for responding to security incidents, data breaches, and disaster recovery.
<b>Infrastructure and Technology</b>	Requirements for the underlying technology, including cloud infrastructure, hardware, and software tools.

# Requirements - Drivers

<b>Infrastructure and Technology</b>	Requirements for the underlying technology, including cloud infrastructure, hardware, and software tools.
<b>Data Retention and Disposal</b>	Policies for data retention, archival, and secure data disposal.
<b>Training and Awareness</b>	Programs for training staff and raising awareness about data security and compliance.
<b>Ethics and Responsible Research</b>	Guidelines for conducting ethical research, including informed consent and ethical review processes.
<b>Performance and Scalability</b>	Requirements to ensure the TRE can handle the anticipated data load and user traffic.
<b>Interoperability and Standards</b>	Standards for ensuring data can be easily shared and used across different systems and platforms.





# Partners - as Drivers

<b>Barcelona Supercomputing Center - Centro Nacional de Supercomputacion</b>	<b>EMBL-EBI</b>	Sciensano	<b>University of Essex</b>
Bielefeld University	EUDAT Collaborative data infrastructure	<b>Sigma2 AS</b>	University of Ljubljana
BioData.pt	Finnish Institute for Health and Welfare (Terveyden ja hyvinvoinnin laitos)	<b>Stichting Health-RI</b>	University of Nottingham
<b>Centre for Genomic Regulation (CRG)</b>	<b>GESIS - Leibniz-Institut für Sozialwissenschaften</b>	SURF	<b>University of Oslo</b>
<b>CESSDA ERIC</b>	GRNET – National Infrastructures for Research and Technology	<b>Tárki Alapítvány</b>	University of Tartu
<b>CSC – Tieteen tietotekniikan keskus Oy</b>	<b>Health Data Research UK (HDR UK)</b>	The University of Manchester	Uppsala universitet
Danmarks Tekniske Universitet(DTU)	Luxembourg National Data Service (LNDS)	<b>Turku University of Applied Sciences (Turun ammattikorkeakoulu)</b>	Vlaams Instituut voor Biotechnologie (VIB)
<b>ECRIN (European Clinical Research Infrastructure Network)</b>	Masaryk University	<b>University of Bergen</b>	VSB - Technical University of Ostrava
ELIXIR	NTNU - Norwegian University of Science and Technology	<b>University of Dundee</b>	

# Partners - as Providers

<b>Barcelona Supercomputing Center - Centro Nacional de Supercomputacion</b>	EMBL-EBI	<b>Sciensano</b>	University of Essex
<b><u>Bielefeld University (de.NBI Cloud)</u></b>	EUDAT Collaborative data infrastructure	<b>Sigma2 AS</b>	<b>University of Ljubljana</b>
<b>BioData.pt</b>	<b>Finnish Institute for Health and Welfare (Terveystieteiden tutkimuskeskus)</b>	<b>Stichting Health-RI</b>	University of Nottingham
Centre for Genomic Regulation (CRG)	GESIS - Leibniz-Institut für Sozialwissenschaften	SURF	University of Oslo
CESSDA ERIC	<b>GRNET – National Infrastructures for Research and Technology</b>	Tárki Alapítvány	<b>University of Tartu</b>
<b>CSC – Tieteen tietotekniikan keskus Oy</b>	Health Data Research UK (HDR UK)	The University of Manchester	<b>Uppsala universitet</b>
<b>Danmarks Tekniske Universitet (DTU)</b>	<b>Luxembourg National Data Service (LNDS)</b>	Turku University of Applied Sciences (Turun ammattikorkeakoulu)	<b>Vlaams Instituut voor Biotechnologie (VIB)</b>
ECRIN (European Clinical Research Infrastructure Network)	Masaryk University	University of Bergen	<b>VSB - Technical University of Ostrava</b>
ELIXIR	NTNU - Norwegian University of Science and Technology	<b>University of Dundee</b>	

# Mail distribution lists

# WP16 Update (Technologies)

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Peter Balcirak  
Masaryk University, Brno, Czechia  
<[peter.balcirak@ics.muni.cz](mailto:peter.balcirak@ics.muni.cz)>



Funded by  
the European Union

- **What is the WP16 about?**

- **What is the WP16 about?**
  - Trusted researcher identities and data authorisation

- **What is the WP16 about?**
  - Trusted researcher identities and data authorisation
    - AAAI for TREs Blueprint



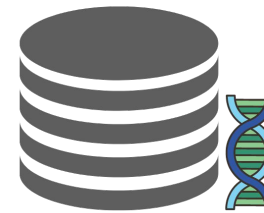
- **What is the WP16 about?**
  - Trusted researcher identities and data authorisation
    - AAAI for TREs Blueprint



# Motivation



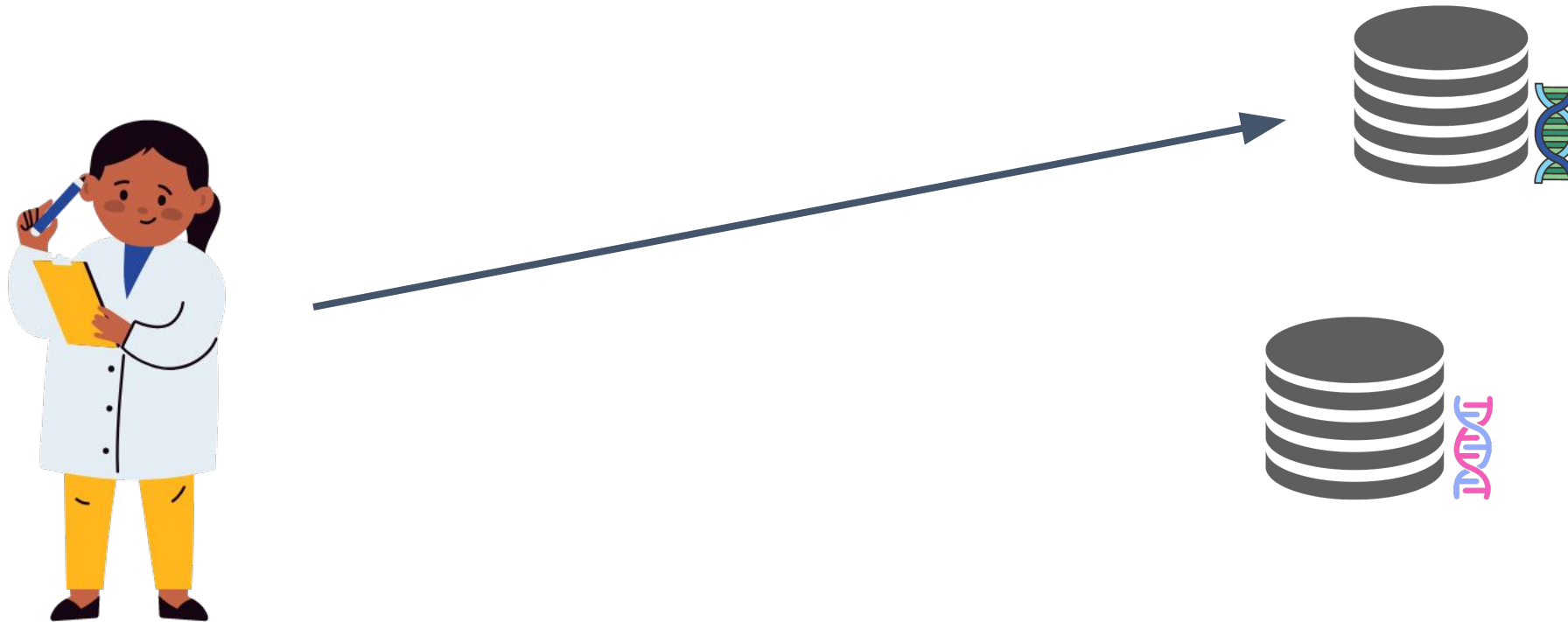
# Motivation



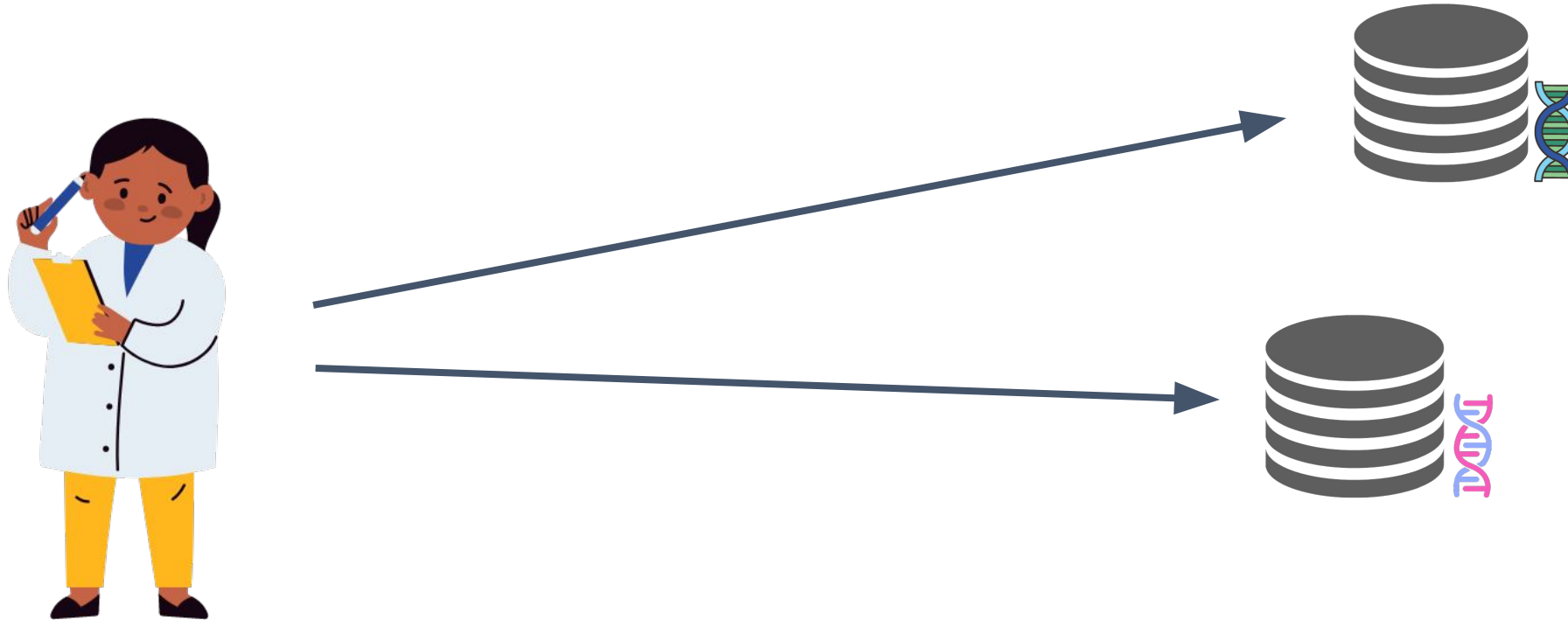
# Motivation



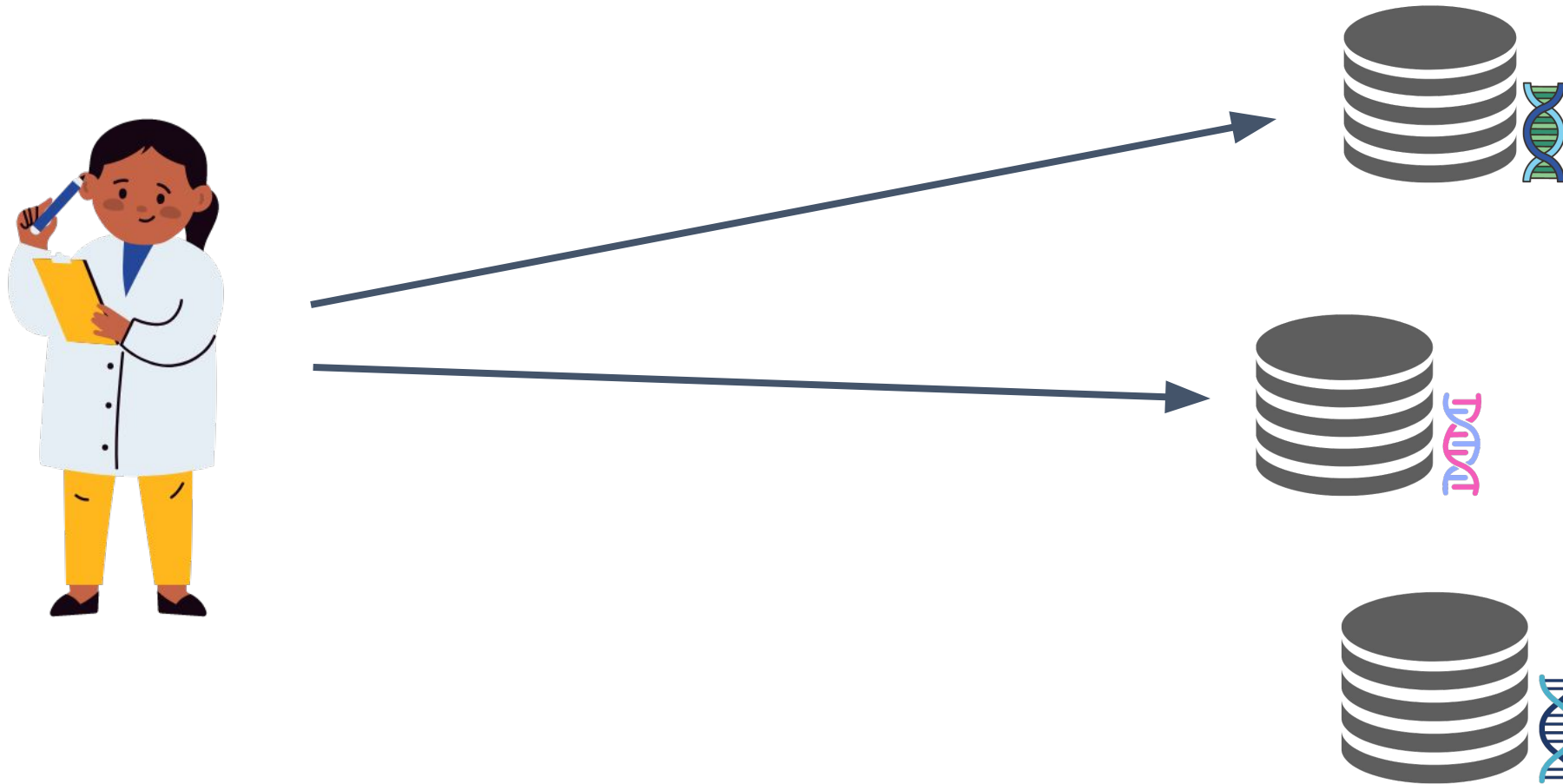
# Motivation



# Motivation

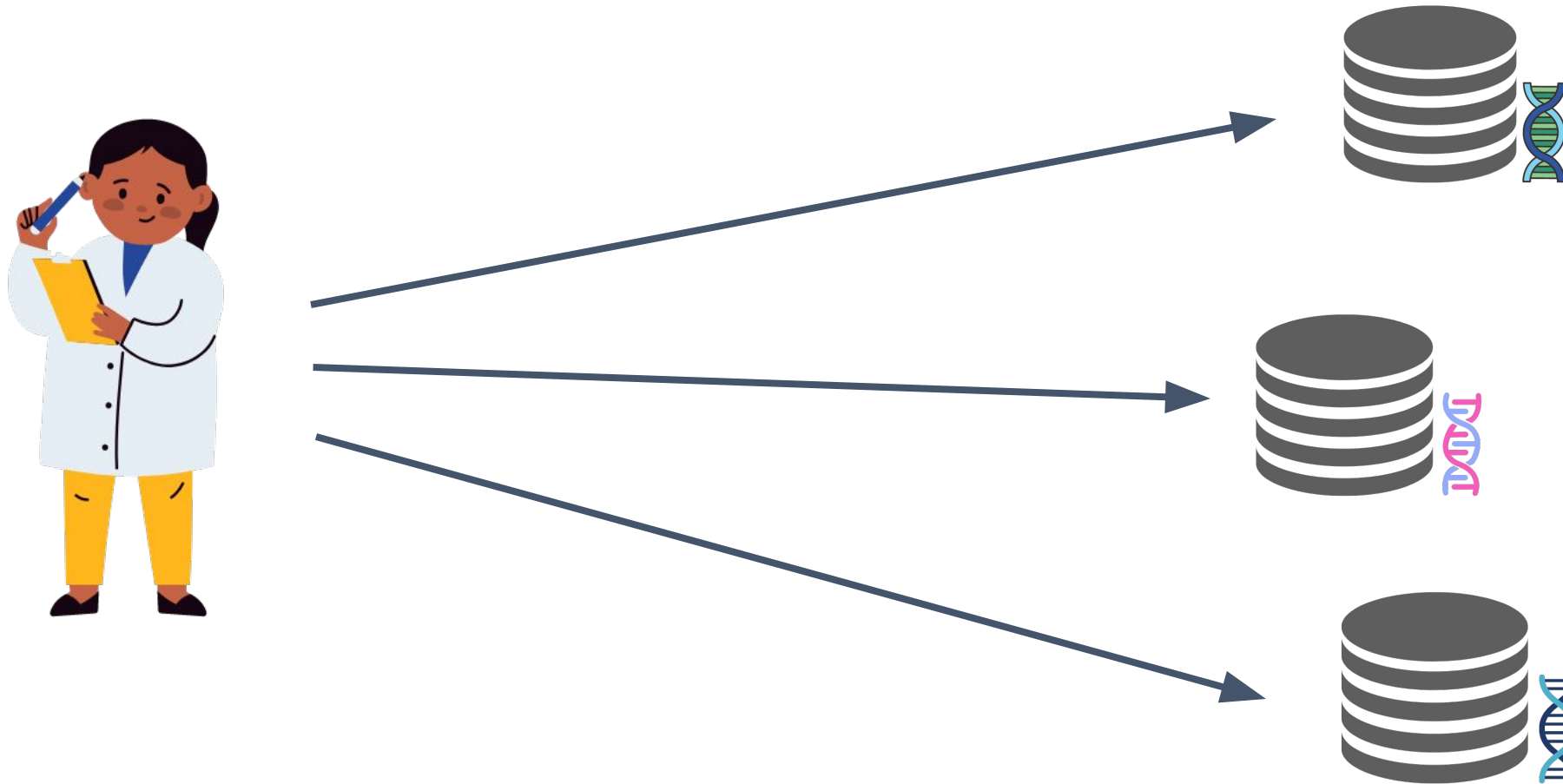


# Motivation

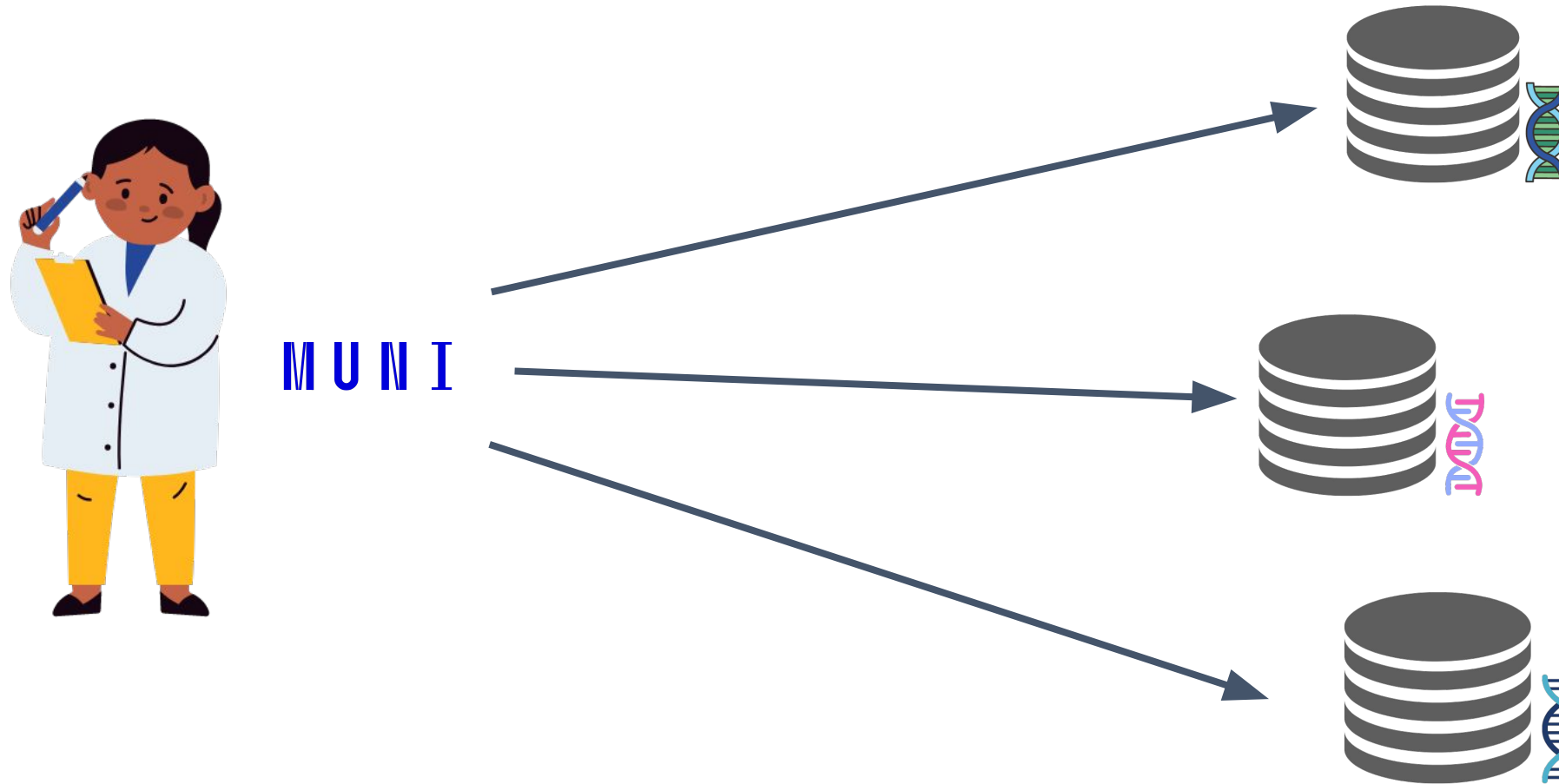




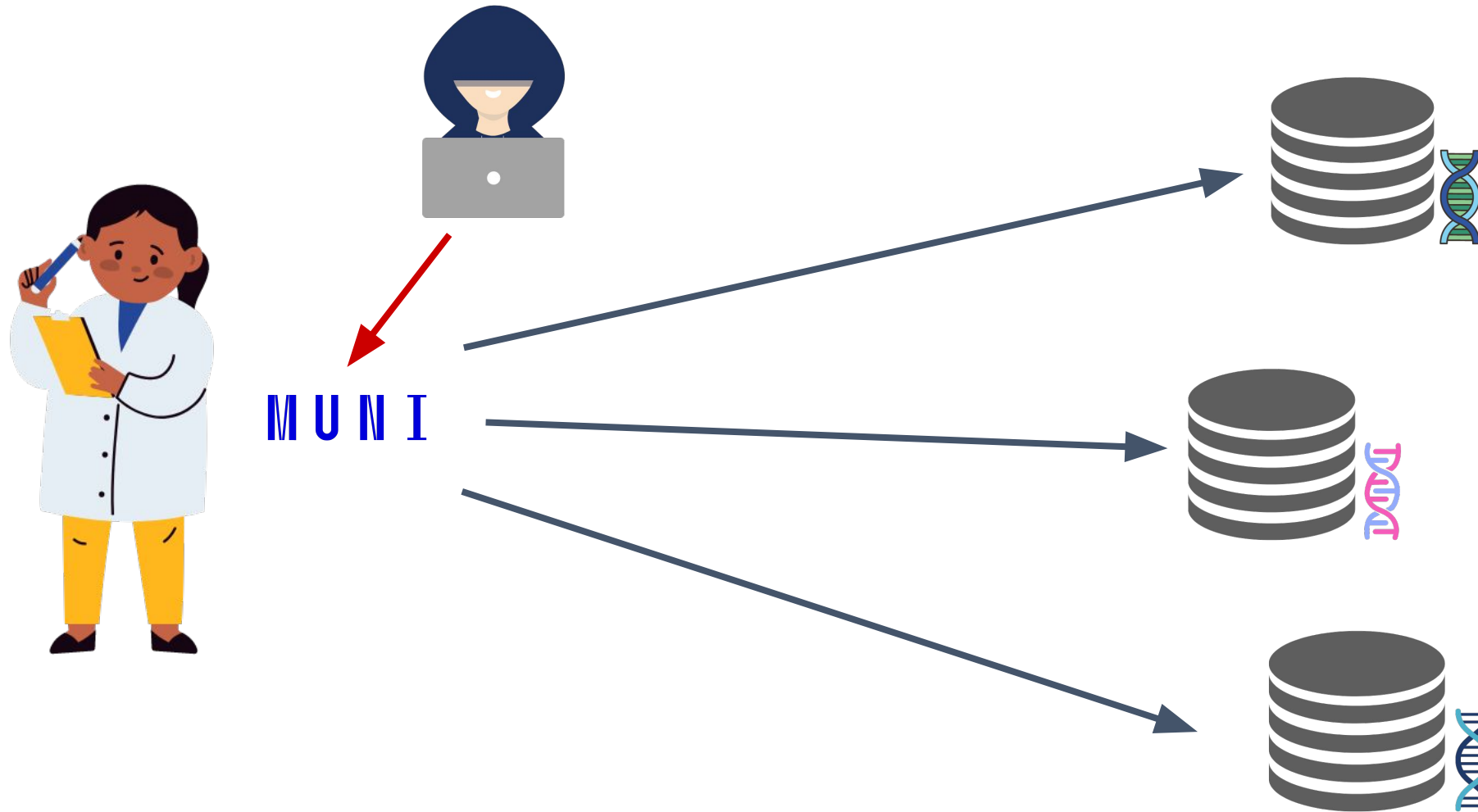
# Motivation



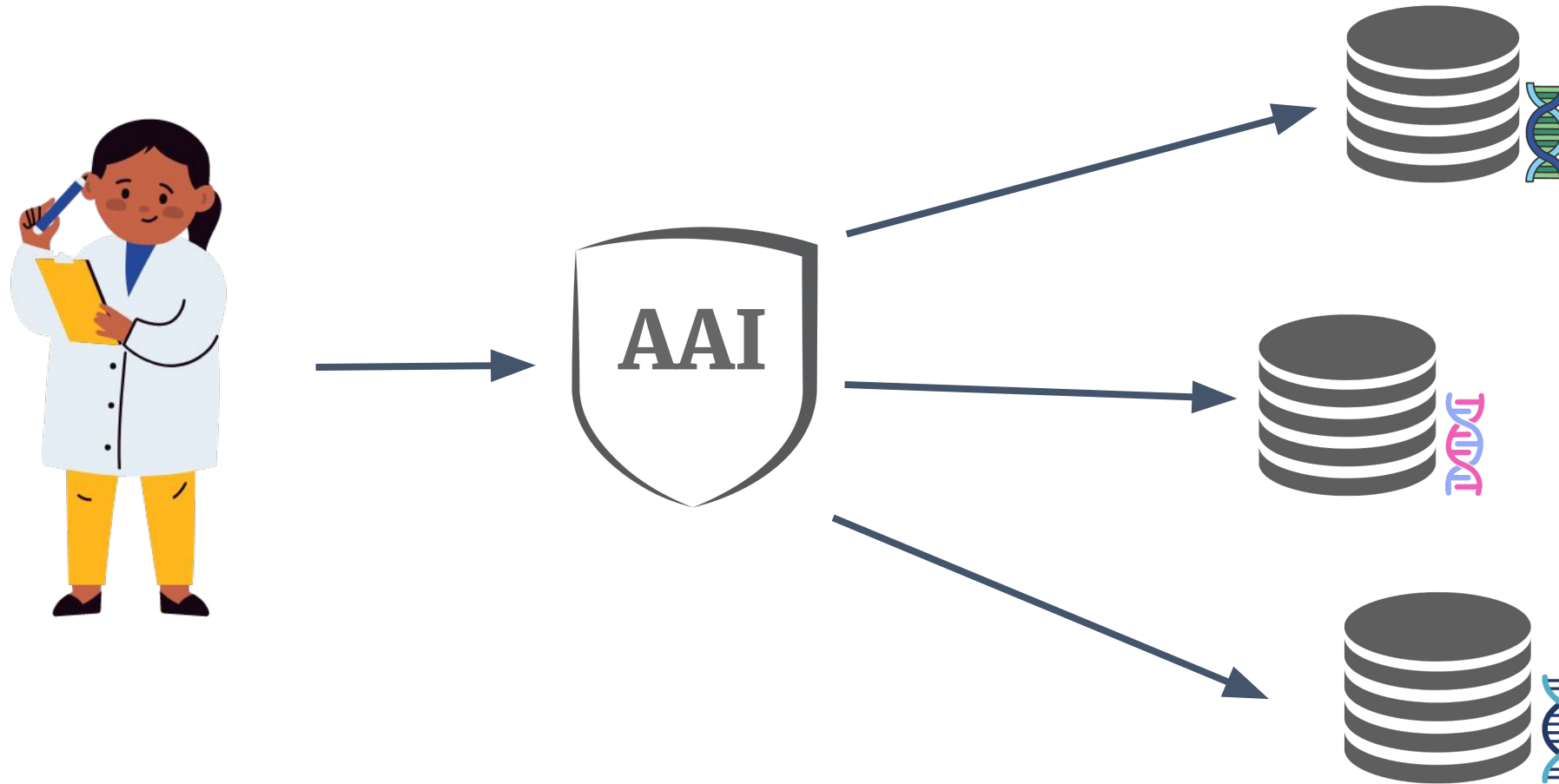
# Motivation



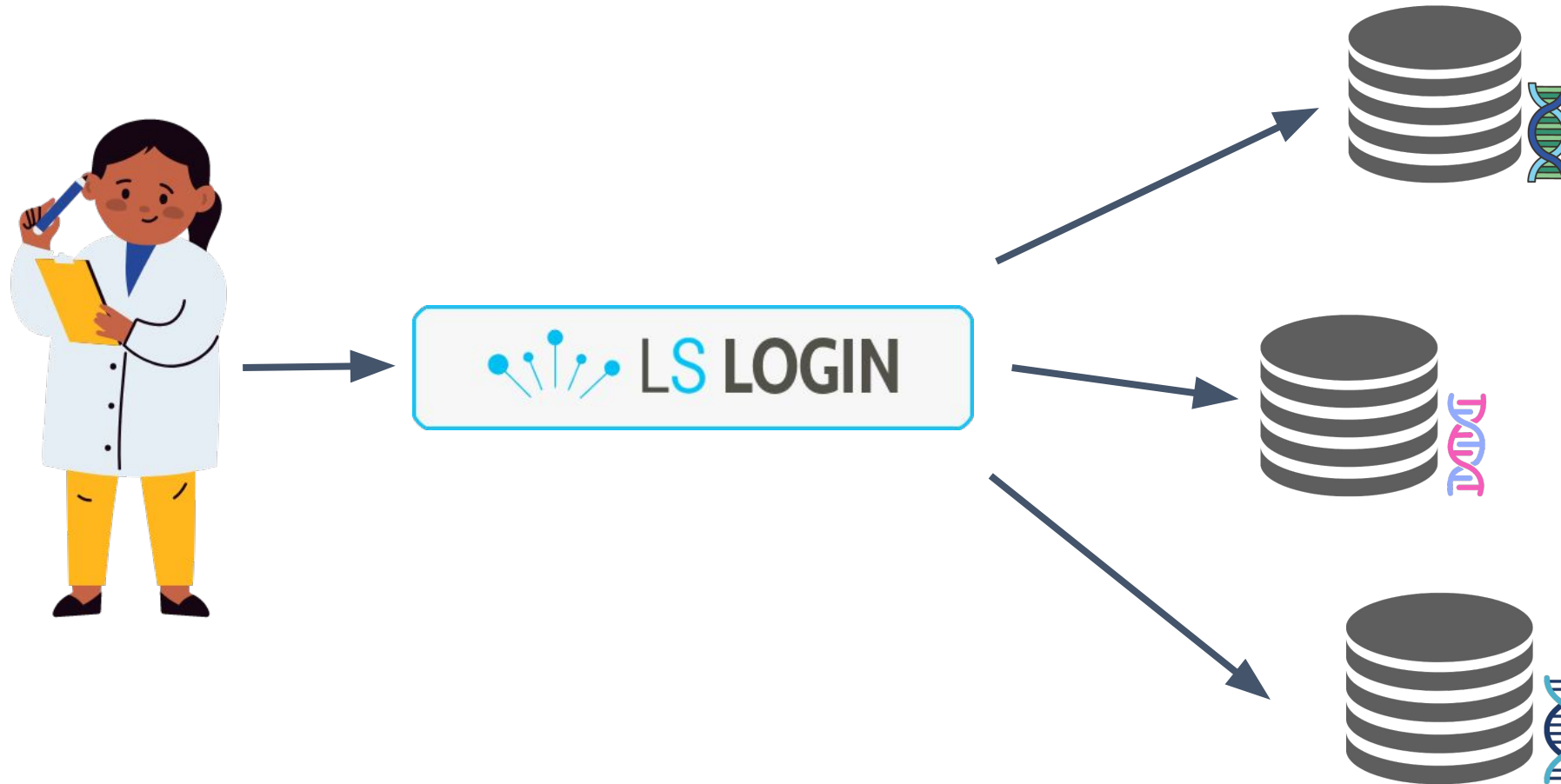
# Motivation



# Motivation



# Motivation



# Life Science AAI

- Complex Solution Providing
  - Authentication Capabilities
    - Single-Sign On - login once, access the whole infrastructure
  - Authorization Capabilities
    - Performs basic authorization (allowed to access, approved all policies)
    - Packs services with data for making authorization decisions
  - Identity Management
    - manage user identities (link, manage associated data, ...)
  - Access Management
    - define rules for authorization (e.g. user must be a member of a group)

# WP16 Challenges

- Secure Authentication
  - Multi-Factor & Passwordless Authentication
  - Policies & Processes
- Identity Assurance
  - Identity Federation & eIDAS Activities
- Identity Curation
  - Identity Life Cycle & Freshness
- Fine-Grained Access Control
  - Authorization in distributed & federated environments
  - Focus on authorization delegation
- Add “the third A”
  - Support of accounting and auditing the access to sensitive digital objects

# Ongoing Work

- Requirements Gathering & Evaluation
  - Cooperation with the Drivers and Architecture WPs
  - Bringing our own requirements
- eID Integration
  - Discussions about possible solutions



# Deadlines

- D16.1 AAAI for TREs Blueprint
  - 1st version (M12) - 02/2025
- D13.4 Year one version of EOSC-ENTRUST Blueprint & Interoperability Framework
  - (M9) - 11/2024
- D19.1 Deployable Demonstrator of Digital Objects & Workflows Developments
  - (M10) - 12/2024

# Digital Transformation to support FAIR, workflows and federated analytics

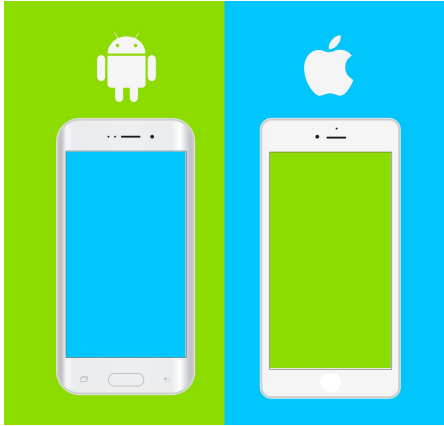
1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Laia Codó, Phil Quinlan, **Stian Soiland-Reyes**  
(WP19)



Funded by  
the European Union

# Mobile Phones



- I can pick a range of devices
- I can pick different operating systems
- I can pick different networks
- I can roam and be a guest on other networks
- I can run the same apps as others on different networks and different phones/systems

# Who in the room knows....



- The AAI process to allow you onto the network
- The AAI process to allow you onto a guest network
- The communication protocols for texts, calls, data
- The standards used for capturing consumption and billing?

If anyone does know the answer did it change your purchasing decision and what you could do with your phone?

# Trish the TRE

- Primary role to protect the reputation of the TRE as a trustworthy and secure environment
- A strong technical background
- TRE established to mitigate a *governance concern* of data controllers
- As interface between *data controllers* who provide data, and *researchers* who seek to access it
- Has to develop and manage cost recovery mechanisms





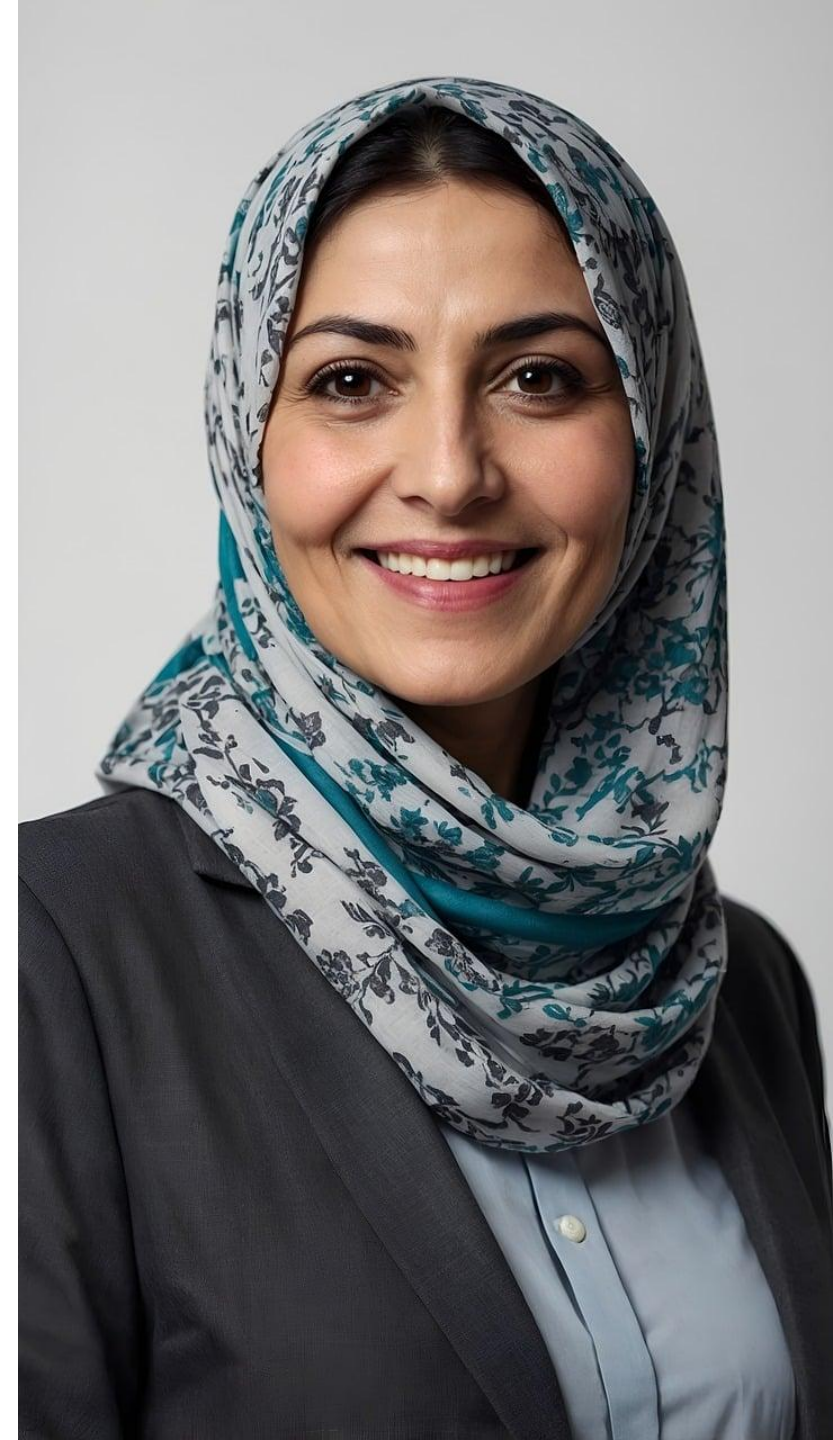
# Harriet the HPC

- Primary role to provide a high end compute environment
- A strong technical background
- Established to provide researchers with the required compute
- Some level of cost recovery and accounting
- Hardware refresh every few years



# Razia the Researcher

- Primary role to undertake research
- A real mix of technical expertise
- Finds it an increasingly hard environment to undertake research
- Has greater data needs from multiple sources in multiple environments
- Data is in multiple environments and jurisdictions



# The pain in the system



In order to do analyses across multiple environments, Razia has to do the heavy lifting and understand all the major components.



In order to support researchers, Trish is being asked to install multiple tools and platforms that have different mechanisms for AAI and governance considerations



In order to support research in sensitive data, Harriet must act more like a TRE, considering security implications and tool requirements

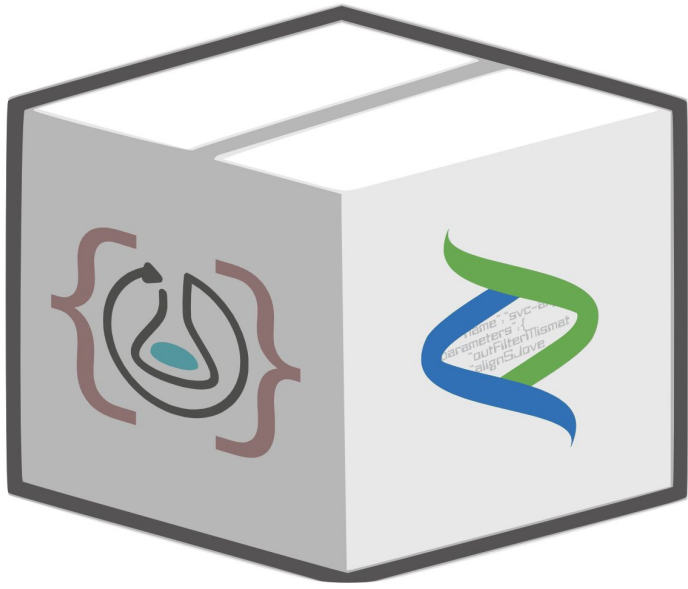


# The goal

Razia is able to *select the analytics* to run, *select the data* required across TREs, and chose the *level of compute* to use from a tool or platform of her choice.

In order to achieve this goal, **digital transformation** is required that is sympathetic to current governance. Must allow Trish to **secure data** *and* utilise existing high **compute** so others don't replicate what Harriet already has available.

# The idea....



RO-Crate: *Research Object Crate*

A **Research Object** that can be passed between tool providers, TREs and HPCs that is universally understood.

Within, the object can contain data, analytics, provenance and governance details.

Each actor reads and contributes different parts.

# If we pass boxes around...



[WfExS](#): *Workflow Execution Service*

We need software that can receive, unpack, process the contents, initiate compute, and re-package the results.....

Can the box simply contain a workflow that we run?

# What the text says....

- Task 7A.1: **Use-cases** for the deployment of Five Safes RO-Crate
- Task 7A.2: **Workflow engine** processing a Five Safes RO-Crate
- Deliverable D7A.1: Deployable **Demonstrator** of Digital Objects & Workflows Developments

# Translated

We will create a **demonstrator** that will show how...

Razia can go to the *HDR UK Cohort Discovery tool* and/or the *Nottingham Beacon* page. She will create a query via those tools natively.

Trisha has only installed the ability to receive and process *RO-Crates* in her TRE.

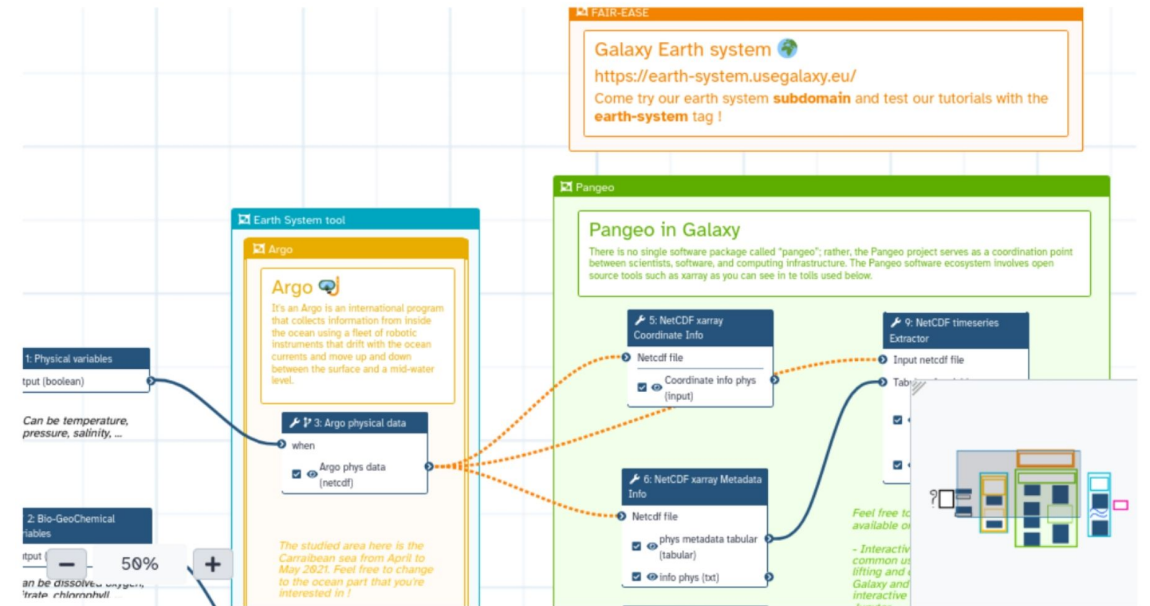
# Technology readiness

Mature **workflow systems** (e.g. *Snakemake*, *Galaxy*, *CWL*, *Nextflow*) adds:

**A**utomation **S**calability **A**daptation **P**rovenance  
([Ludäscher 2012](#))

Full Analyse Argo data

[Download](#) [View In Galaxy](#)



## COMMON WORKFLOW LANGUAGE

>350 known workflow systems

<https://s.apache.org/existing-workflow-systems>

**eOSC** | **ENTRUST**

European Network of Trusted Research Environments

# Technology readiness

Mature **workflow systems** (e.g. *Snakemake*, *Galaxy*, *CWL*, *Nextflow*) adds:

**A**utomation **S**calability **A**daptation **P**rovenance  
([Ludäscher 2012](#))

**FAIR** principles enables machine actionability and structured metadata

**F**indability **A**ccessible **I**nteroperable **R**eusable ([Wilkinson 2016](#))



Semantic Interoperability  
Task Force

Version: 27 March 2024  
DOI: 10.5281/zenodo.10843882

## Developing and implementing the semantic interoperability recommendations of the EOSC Interoperability Framework

*Deliverable of EOSC-A TF Semantic Interoperability (2021-2023)*

<https://doi.org/10.5281/zenodo.10843882>

European Network of Trusted Research Environments

# Technology readiness

Mature **workflow systems** (e.g. *Snakemake*, *Galaxy*, *CWL*, *Nextflow*) adds:

**A**utomation **S**calability **A**daptation **P**rovenance  
([Ludäscher 2012](#))

**FAIR** principles enables machine actionability and structured metadata

**F**indability **A**ccessible **I**nteroperable **R**eusable ([Wilkinson 2016](#))

**Containers** (*Docker*, *Singularity*) and package systems (*Conda*) allow software to reliably move across compute systems ([Grüning 2018](#), [Möller 2017](#))



**BIOCONDA<sup>®</sup>**



# Technology readiness

Mature **workflow systems** (e.g. *Snakemake*, *Galaxy*, *CWL*, *Nextflow*) adds:

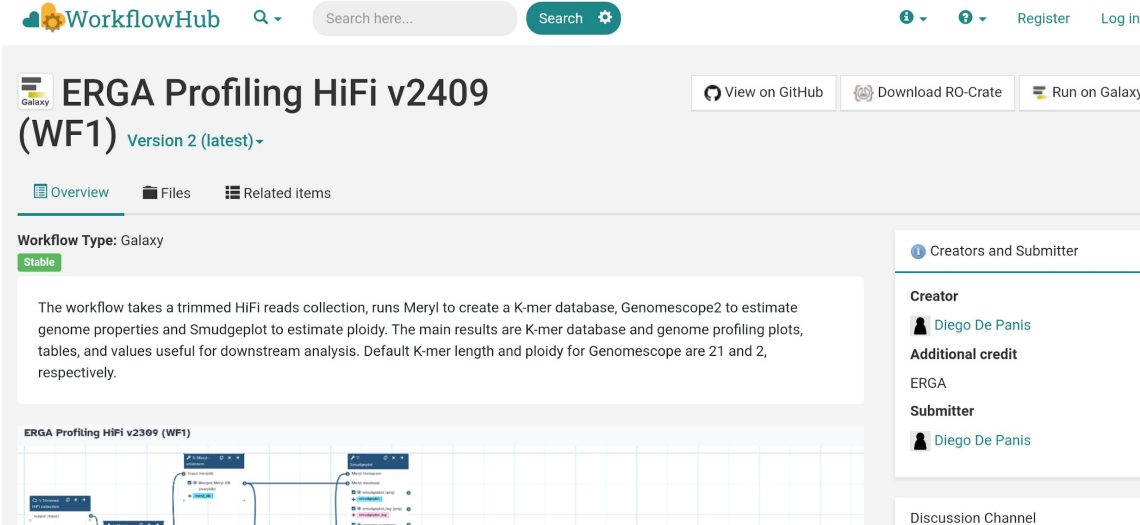
**A**utomation **S**calability **A**daptation **P**rovenance  
(Ludäscher 2012)

**FAIR** principles enables machine actionability and structured metadata

**F**indability **A**ccessible **I**nteroperable **R**eusable (Wilkinson 2016)

**Containers** (*Docker*, *Singularity*) and package systems (*Conda*) allow software to reliably move across compute systems (Grüning 2018, Möller 2017)

**FAIR Workflows** allows computational methods to be shared and documented (Goble 2020)



The screenshot displays the WorkflowHub interface for the 'ERGA Profiling HiFi v2409 (WF1)' workflow. The header includes the WorkflowHub logo, a search bar, and links for 'View on GitHub', 'Download RO-Crate', and 'Run on Galaxy'. The workflow is identified as 'Version 2 (latest)'. Below the title, there are tabs for 'Overview', 'Files', and 'Related items'. The 'Overview' tab is active, showing a description: 'The workflow takes a trimmed HiFi reads collection, runs Meryl to create a K-mer database, Genomescope2 to estimate genome properties and Smudgeplot to estimate ploidy. The main results are K-mer database and genome profiling plots, tables, and values useful for downstream analysis. Default K-mer length and ploidy for Genomescope are 21 and 2, respectively.' Below the description is a visual representation of the workflow graph. On the right side, there is a sidebar with 'Creators and Submitter' information, listing 'Creator' as Diego De Panis, 'Additional credit' as ERGA, and 'Submitter' as Diego De Panis. A 'Discussion Channel' link is also present at the bottom of the sidebar.

<https://workflowhub.eu/>

# Technology readiness

Mature **workflow systems** (e.g. *Snakemake*, *Galaxy*, *CWL*, *Nextflow*) adds:

**A**utomation **S**calability **A**daptation **P**rovenance  
(Ludäscher 2012)

**FAIR** principles enables machine actionability and structured metadata

**F**indability **A**ccessible **I**nteroperable **R**eusable (Wilkinson 2016)

**Containers** (*Docker*, *Singularity*) and package systems (*Conda*) allow software to reliably move across compute systems (Grüning 2018, Möller 2017)

**FAIR Workflows** allows computational methods to be shared and documented (Goble 2020)

**WfExS** has built support for provenance and [Five Safes Crate](#). Broader WfMS support for Workflow Run Crate



# Technology readiness

Mature **workflow systems** (e.g. *Snakemake*, *Galaxy*, *CWL*, *Nextflow*) adds:

**A**utomation **S**calability **A**daptation **P**rovenance  
([Ludäscher 2012](#))

**FAIR** principles enables machine actionability and structured metadata

**F**indability **A**ccessible **I**nteroperable **R**eusable ([Wilkinson 2016](#))

**Containers** (*Docker*, *Singularity*) and package systems (*Conda*) allow software to reliably move across compute systems ([Grüning 2018](#), [Möller 2017](#))

**FAIR Workflows** allows computational methods to be shared and documented ([Goble 2020](#))

**WfExS** has built support for provenance and [Five Safes Crate](#). Broader WfMS support for Workflow Run Crate

## Challenges:

1. Current workflow tech has default assumption of **open** Internet access
2. Convince Trish it is **safe**? (*or even safer than manual access*)
3. Get Harriet to **install** workflow technologies?
4. Working with tool providers so Razia can easily **use** the workflow systems?

# Next step on technology

- Making “full stack” **demonstrator** with Five Safes Crate
- Supporting workflows for **Driver 1** (FEGA/EGDI) with WfExS
- “Cratey” microservice within TRE.  
Offloading RO-Crates generation, **evidence** gathering of what’s executed
- Formalising how **containers** can move into the TRE (considering firewalls, software quality)
- What is **minimal FAIR metadata** for a TRE dataset? (DOI, RO-Crate ?)
  - Mapping to DCAT-AP, making a 4½ Safe Crate profile for TRE datasets
- **7 Oct 2024**: RO-Crate topic in ENTRUST Architecture call



 **CPRD** | UK data driving real-world evidence

Home ▾ News Public ▾ Data ▾ Our services ▾ General Practitioner ▾ Research ▾

[Home](#)

## CPRD GOLD Ethnicity Record September 2024

**Release date**  
18/09/2024

**Summary**  
Citation: Clinical Practice Research Datalink. (2024). CPRD GOLD Ethnicity Record September 2024 (Version 2024.09.001) [Data set]. Clinical Practice Research Datalink. <https://doi.org/10.48329/y5ws-tw17>

<https://doi.org/10.48329/y5ws-tw17>

The CPRD Ethnicity Record is comprised of a single derived ethnicity category for each patient in CPRD GOLD and CPRD Aurum. The Ethnicity Records draw ethnicity data from the primary care databases and, for linkage eligible patients, Hospital Episode Statistics (HES) datasets.

Access is subject to fees and an approved study protocol. Further information is available at <https://cprd.com/cprd-algorithm-derived-data>

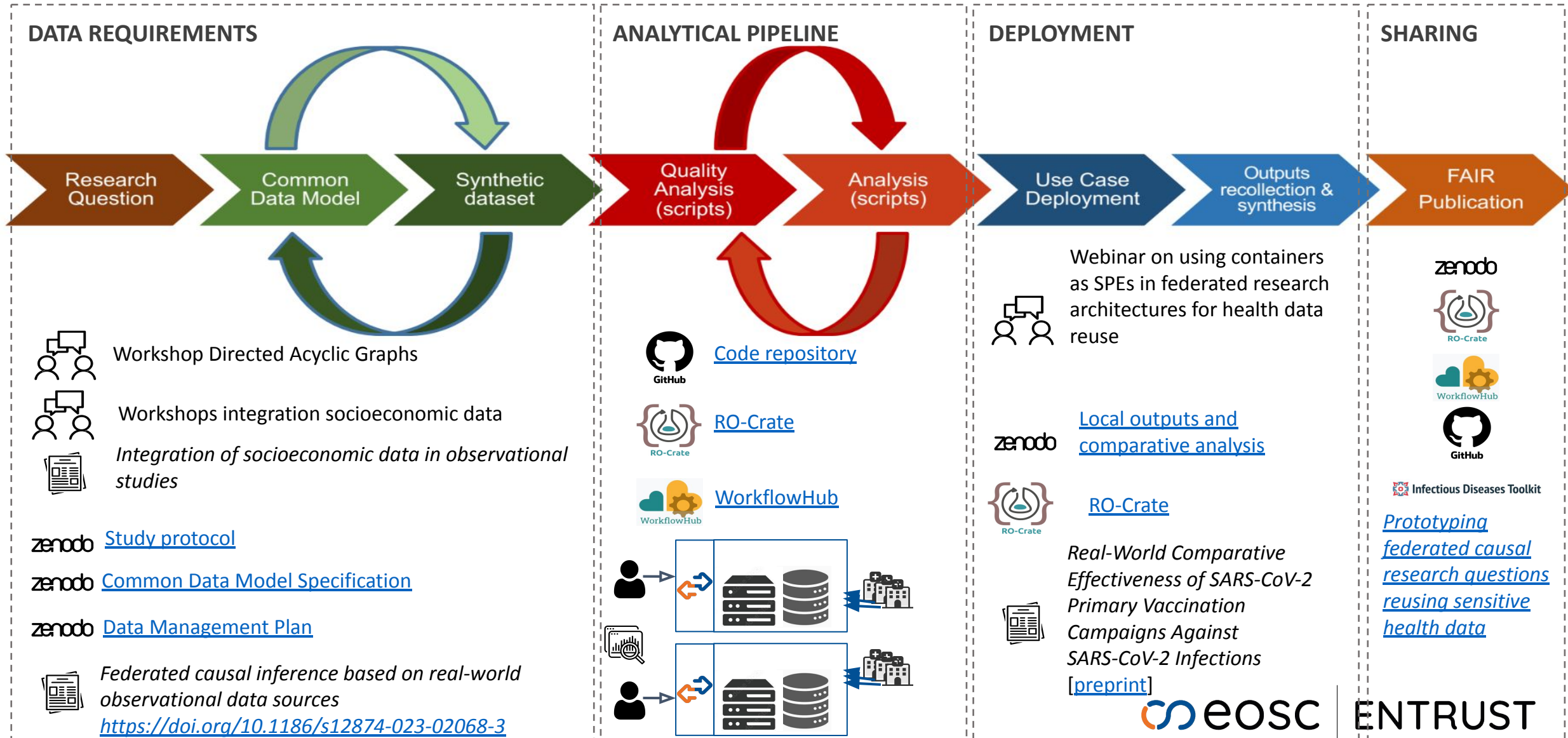
# Next step on governance

Engage with drivers to gauge potential of digital transformation

- Not just aligning with state of the art! (*SATRE mapping, DARE TRE framework*)
- Showcase what are the **possibilities** for the TRE ecosystem and their users
- Agree new **capabilities** for federated analytics and workflow technologies
- Define new **governance** processes for FAIR TREs and evidence gathering



# Can it be done? Federated causal research reusing sensitive real-world population health data





---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# DARE UK TRE Federation Architecture v2.0

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Rob Baxter  
National Digital Infrastructure Technical Lead

<https://docs.google.com/document/d/17RjaSsudziwq6Af3910ji50risVdUXg0/>



Funded by  
the European Union



## Phase 1: Design & Dialogue

July '21 – March '24

£7.5m

- UK-wide public dialogue
- Two landscape reviews
  - Initial review
  - Infrastructure review
- Two portfolios of funded projects
  - 9x Sprint Exemplars
  - 5x Driver Projects
- Phase 1 recommendations report
- Community building initiatives
- Three drafts of a *federated architecture blueprint*

## Phase 2: Build, Test & Establish

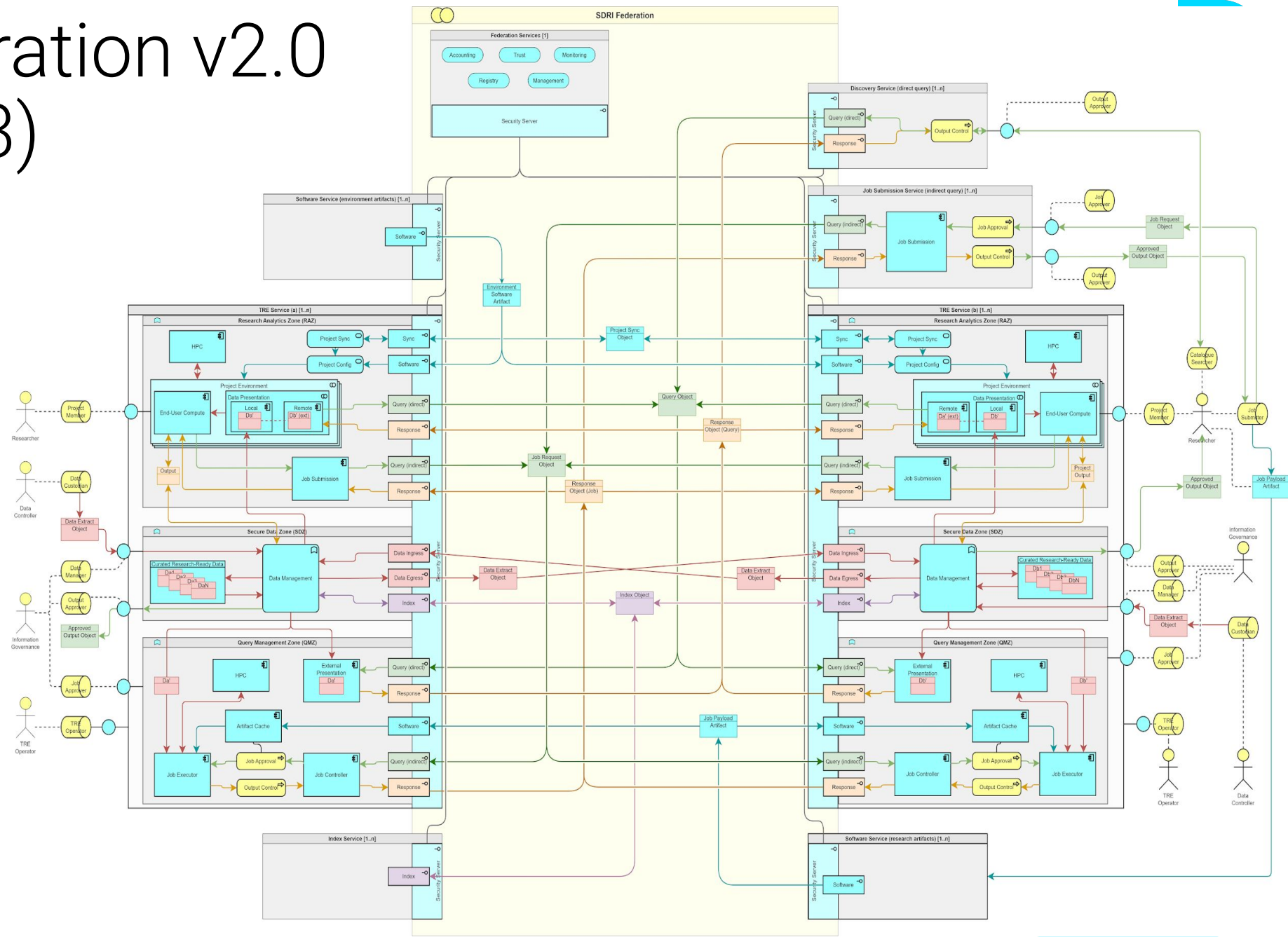
August '24 – March '27

£18.2m

- Transformational Programmes
  - Bring new capabilities to production-readiness
  - Test, configure and adopt these capabilities working with early adopter TREs
  - Use these new capabilities to support researchers and TREs to deliver real-world science
- Portfolio of sprint-style prototype / proofs-of-concept
  - Identify & address missing capabilities
- Early testing of a national network of TREs
- Community building, engagement and standards development
  - Supporting communities
  - Promote information sharing
  - Build consensus around common standards and good practice

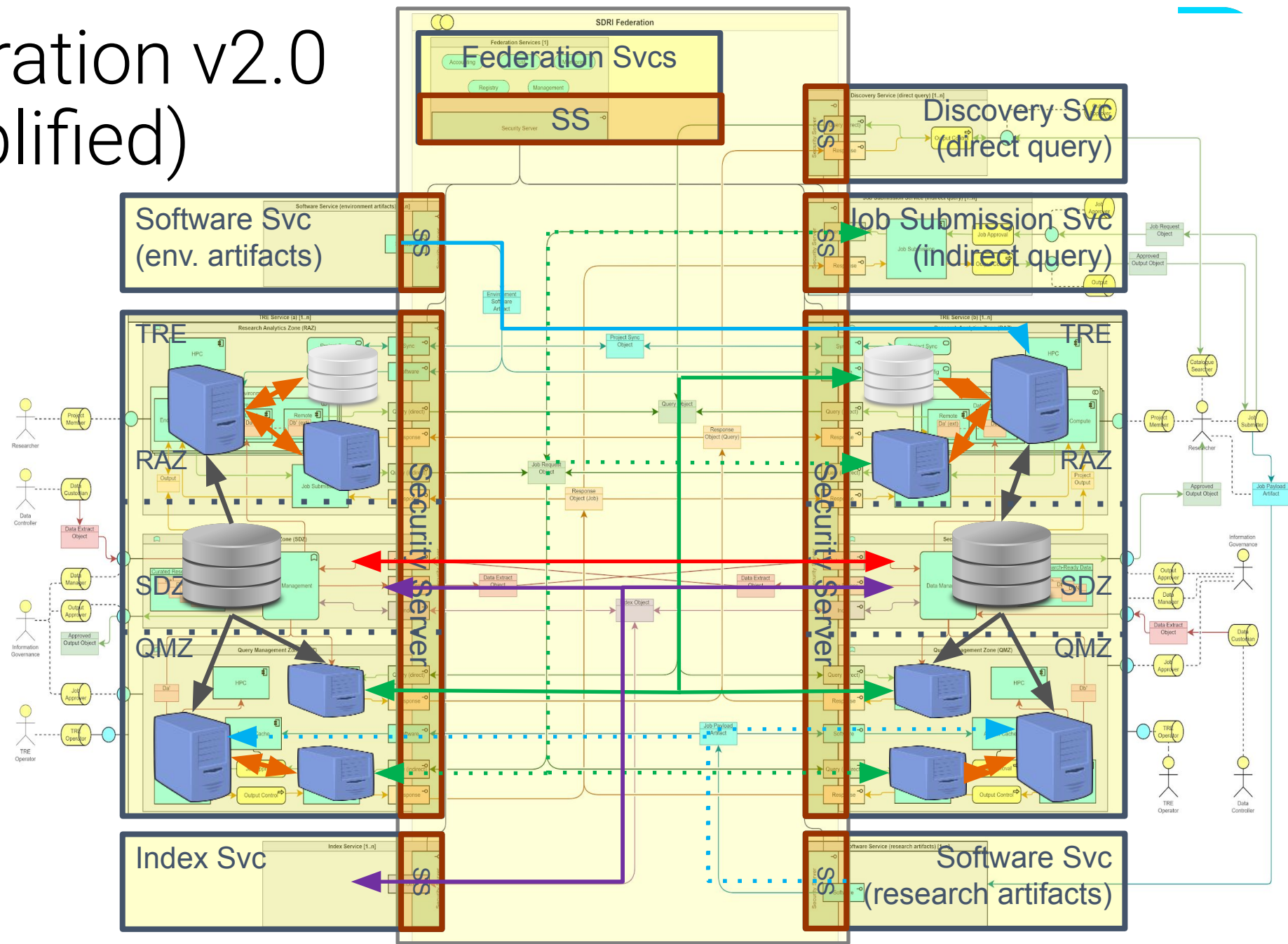
# Federation v2.0 (2023)

DARE UK

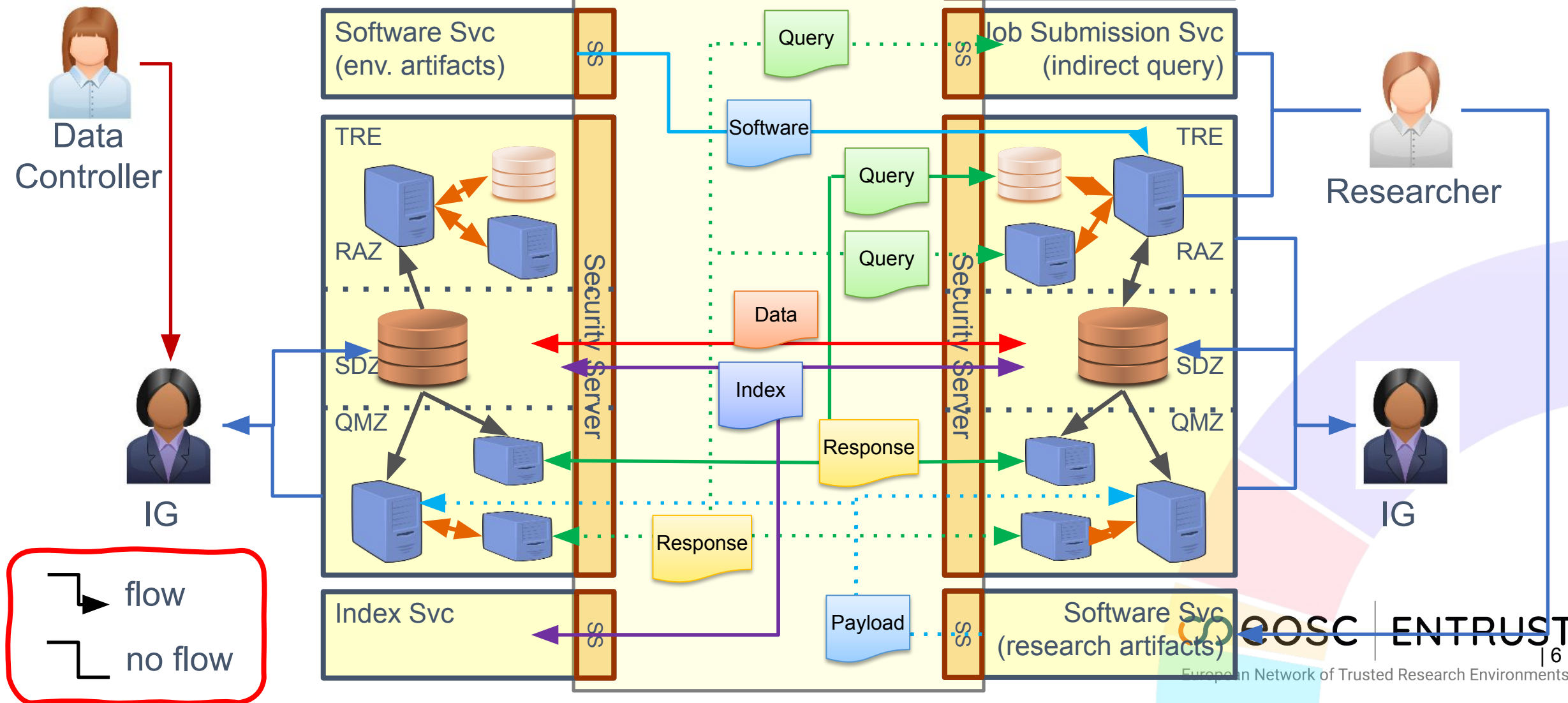


# Federation v2.0 (simplified)

DARE UK



# Federation v2.0 (simplified)



# TRE "Blueprint"

- TRE Zones

- **RAZ: Research Analytics Zone**

- Provides researcher access to project environments via VDI etc.
    - MAY support direct & indirect query (qv)
    - MAY support access to external software/package repos

- **SDZ: Secure Data Zone**

- Grants Information Governance access to datasets
    - Supports curation & linkage of research-ready datasets
    - Supports provision of datasets for research

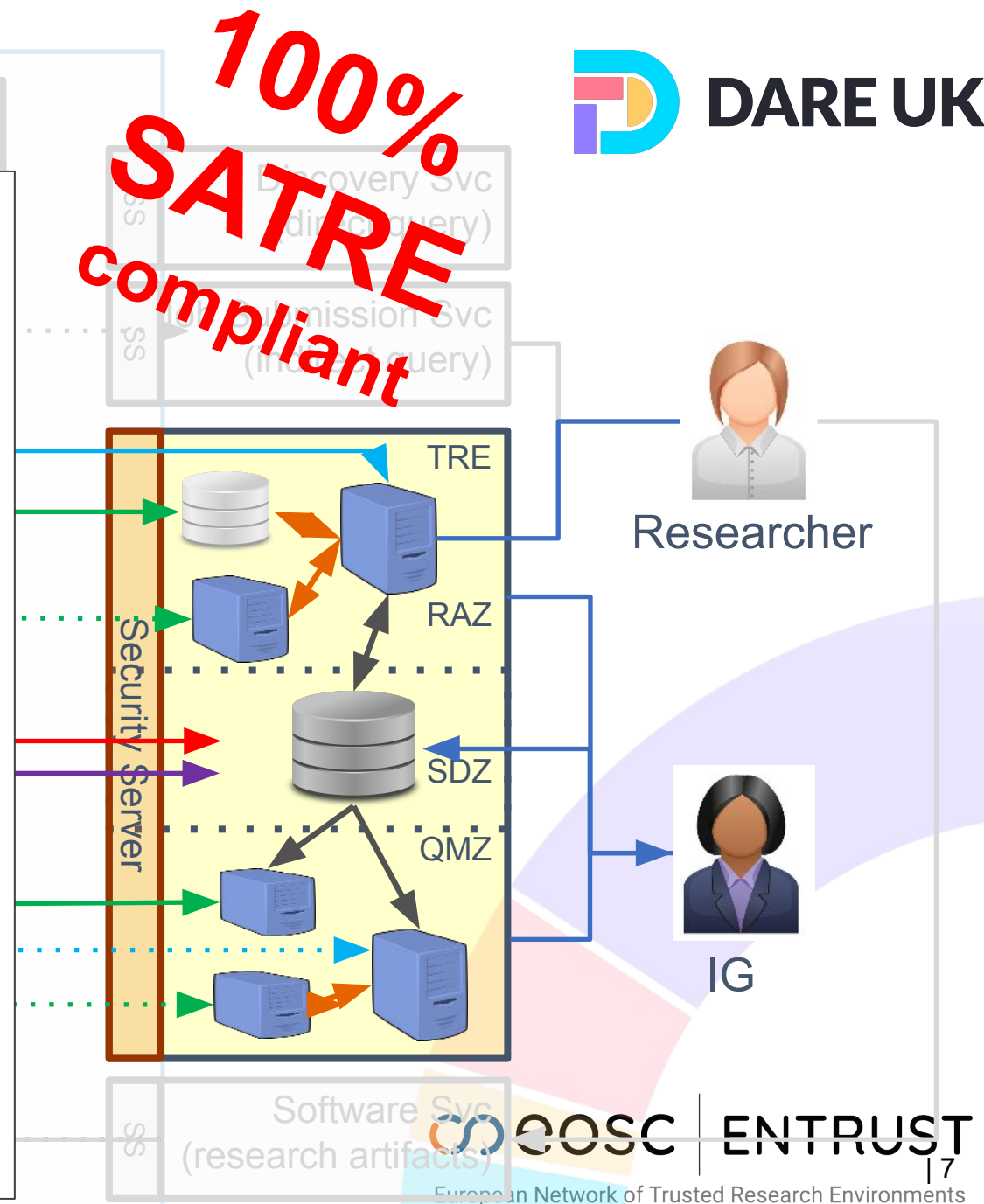
- **QMZ: Query Management Zone**

- Handles incoming queries, direct & indirect
    - Returns results to calling TREs
    - MAY pull in job payloads from external repos

- **Not every TRE needs every zone**

- Security Server

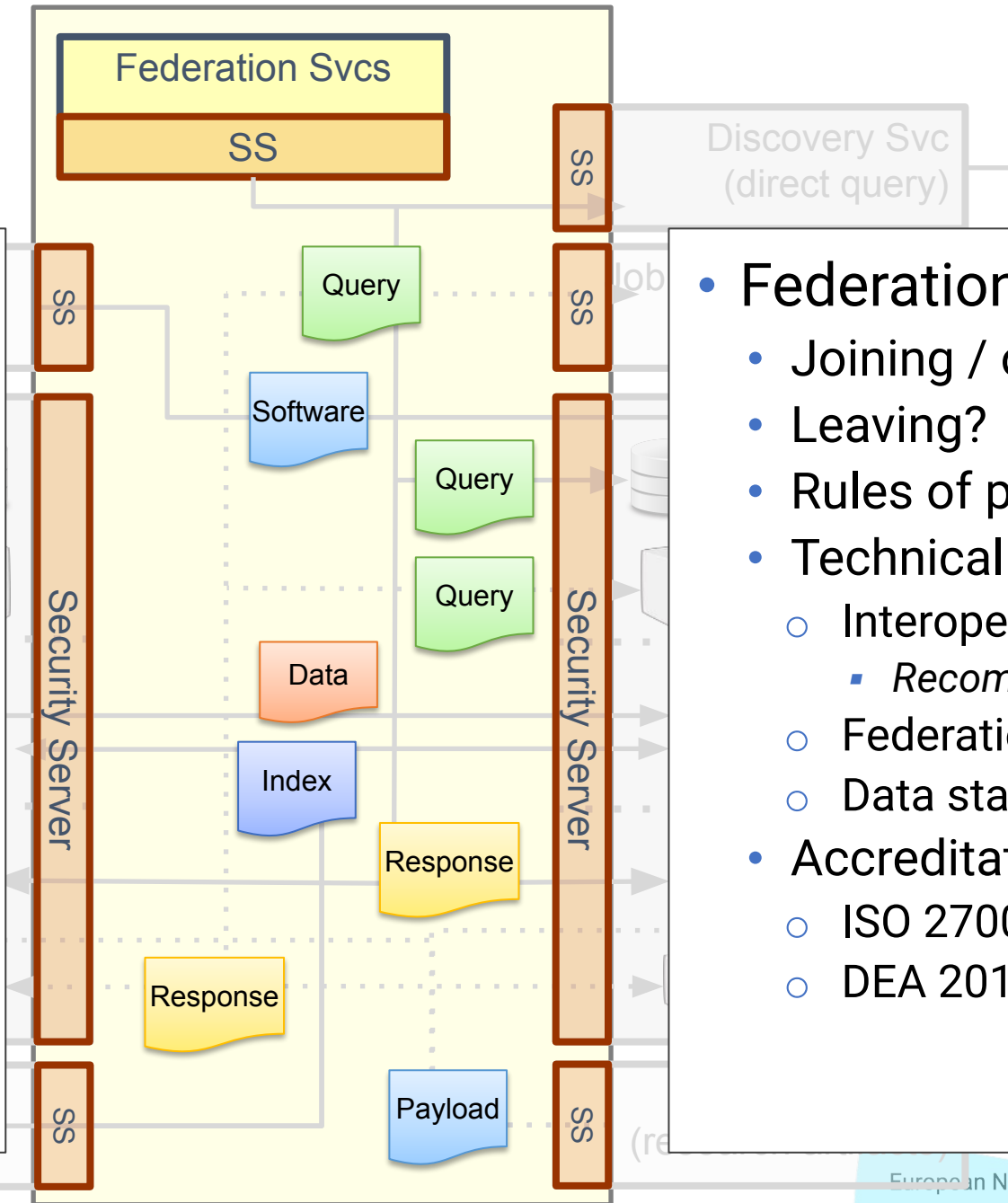
- Common (standardised) API gateway
  - All intra-federation connections route through this





# Federation Services

- Central Registries of:
  - Services
  - Projects
  - Users
  - Data
- PKI signing authority
  - CA
  - RAs
- Known-good config for Security Servers
  - Auto-update?
  - Auto-sync?



- Federation Governance for:
  - Joining / on-boarding?
  - Leaving?
  - Rules of participation?
  - Technical standards?
    - Interoperability/exchange?
      - Recommend **RO-Crate**
    - Federation metadata?
    - Data standards?
  - Accreditation?
    - ISO 27001?
    - DEA 2017?



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union





# D13.2 - Training package for EOSC-ENTRUST Year one Blueprint & Interoperability Framework

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Christine Stansberg  
University of Bergen  
Norwegian TREs - NORTRE



Funded by  
the European Union

Introduction:

## D13.2: Training package for EOSC-ENTRUST Year one Blueprint & Interoperability Framework

Description from proposal:

“Collection of training materials for building interoperable TRE services according to the year one version of the EOSC ENTRUST Blueprint & Interoperability Framework”

Responsible: NORTRE and ELIXIR Norway, valued input received from all over EOSC-ENTRUST during WP13 generic- and D13.2-specific calls.

# Training package?

A structured set of educational materials and activities designed to teach specific skills or knowledge

# Training package?

A structured set of educational materials and activities designed to teach specific skills or knowledge

Typical components:

# Training package?

A structured set of educational materials and activities designed to teach specific skills or knowledge

Typical components:

- Objectives

# Training package?

A structured set of educational materials and activities designed to teach specific skills or knowledge

Typical components:

- Objectives
- Audience

# Training package?

A structured set of educational materials and activities designed to teach specific skills or knowledge

Typical components:

- Objectives
- Audience
- Content

# Training package?

A structured set of educational materials and activities designed to teach specific skills or knowledge

Typical components:

- Objectives
- Audience
- Content
- Structure



# Training package?

A structured set of educational materials and activities designed to teach specific skills or knowledge

Typical components:

- Objectives
- Audience
- Content
- Structure
- Delivery format

# Revisiting the proposal:

“Collection of **training materials for building interoperable TRE services** according to the **year one** version of the EOSC-ENTRUST Blueprint & Interoperability Framework”

## Revisiting the proposal:

“Collection of **training materials for building interoperable TRE services** according to the **year one** version of the EOSC-ENTRUST Blueprint & Interoperability Framework”

We read this as:

“Given the current state of the Blueprint, what does an aspiring TRE need to know to be able join the ENTRUST network?”

# D13.2: Training package for EOSC-ENTRUST

## Year one Blueprint & Interoperability Framework

- Objective
- Audience
- Content
- Structure
- Delivery format

# D13.2: Training package for EOSC-ENTRUST

## Year one Blueprint & Interoperability Framework

- Objective
  - Enable TREs to onboard the EOSC-ENTRUST network and federation
- Audience
- Content
- Structure
- Delivery format

# D13.2: Training package for EOSC-ENTRUST

## Year one Blueprint & Interoperability Framework

- Objective
  - Enable TREs to onboard the EOSC-ENTRUST network and federation
- Audience
  - Owners and operators of existing and emerging TREs
- Content
- Structure
- Delivery format

# D13.2: Training package for EOSC-ENTRUST

## Year one Blueprint & Interoperability Framework

- Objective
  - Enable TREs to onboard the EOSC-ENTRUST network and federation
- Audience
  - Owners and operators of existing and emerging TREs
- Content
  - Comprehensive guide to all aspects that will influence the process
- Structure
- Delivery format

# D13.2: Training package for EOSC-ENTRUST

## Year one Blueprint & Interoperability Framework

- Objective
  - Enable TREs to onboard the EOSC-ENTRUST network and federation
- Audience
  - Owners and operators of existing and emerging TREs
- Content
  - Comprehensive guide to all aspects that will influence the process
- Structure
  - Sections corresponding to Blueprint
- Delivery format



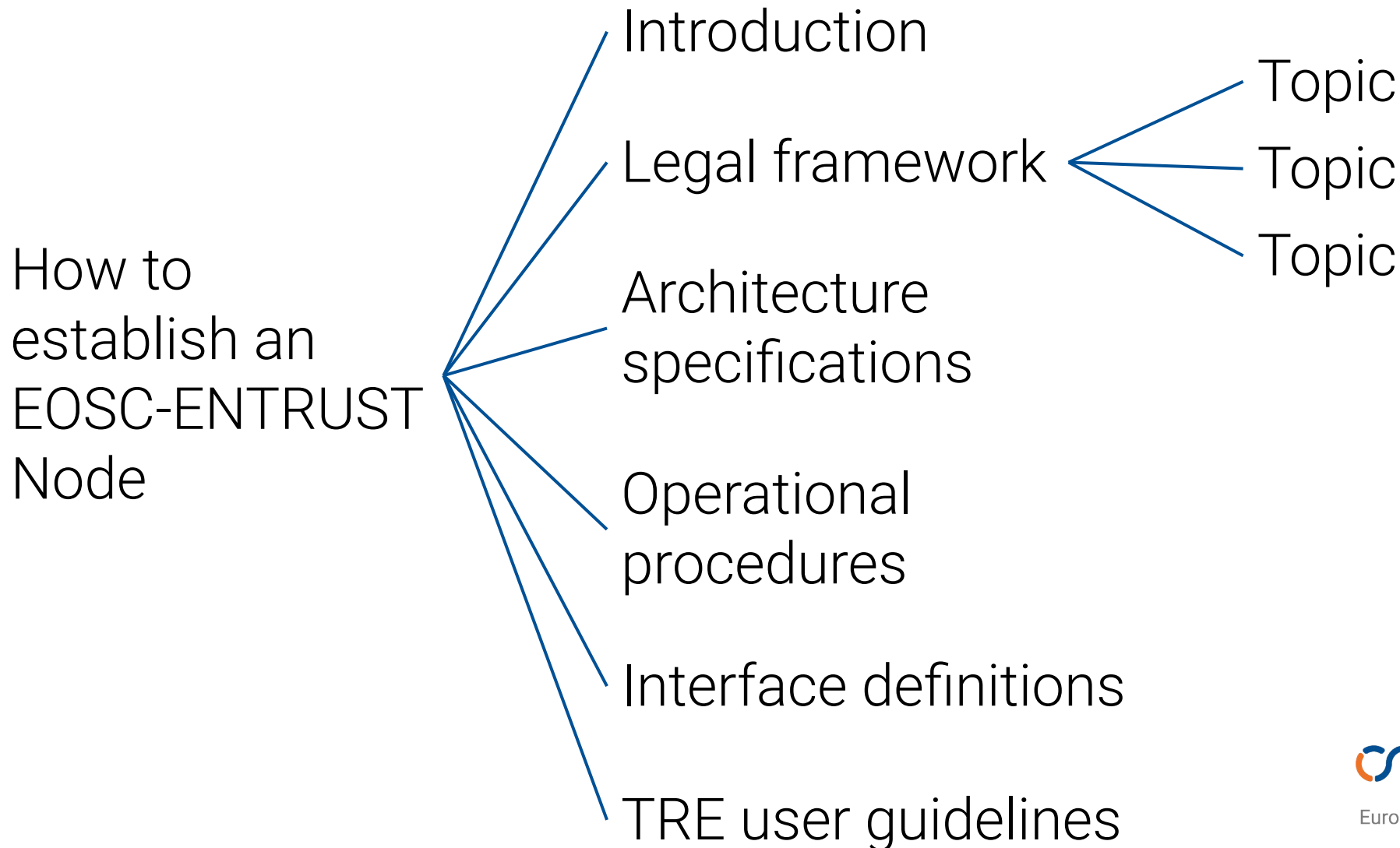
# D13.2: Training package for EOSC-ENTRUST

## Year one Blueprint & Interoperability Framework


- Objective
  - Enable TREs to onboard the EOSC-ENTRUST network and federation
- Audience
  - Owners and operators of existing and emerging TREs
- Content
  - Comprehensive guide to all aspects that will influence the process
- Structure
  - Sections corresponding to Blueprint
- Delivery format
  - Online guide

# Suggested structure

- aligned with emerging D13.4 Blueprint sections



# Inspiration:



Federated  
European  
Genome-phenome  
Archive

Establishing a Federated EGA Node

What am I doing here?

What is Federated EGA (FEGA)?

What are the benefits of joining Federated EGA?

How do I start?

What does the journey look like?

License

Acknowledgements

TOPICS

Maturity Model

Data and Metadata Management

Outreach and Training

Technical and Operational

Governance and Legal


GitHub

Vis meny

Next »

[Docs](#) » Establishing a Federated EGA Node

## Establishing a Federated EGA Node



Welcome to this collection of onboarding materials for establishing a Federated EGA Node!

### What am I doing here?

If you are reading this, you are probably looking for information on how to join the Federated EGA. Great! There is a lot of information here for you.


These materials provide guidance for establishing a node within the Federated EGA. The materials are based on the knowledge and experiences of current nodes and their use cases. Your node's development might differ depending on your use cases and mandates from stakeholders. Please view these materials as suggestions and best practices - not hard requirements!

### What is Federated EGA (FEGA)?

The Federated EGA is an ecosystem or network of Federated EGA Nodes. FEGA Nodes constitute the primary global resource for discovery and access of sensitive human omics and associated data, consented for secondary use, through a network of national human data repositories to accelerate disease research and improve human health.

Over the last 10 years, most individual-level human omics data have been generated in the context of research consortia and shared via global repositories such as the European Genome-phenome Archive (EGA). Many countries now have emerging personalized medicine programmes which are

# Inspiration:



Federated  
European  
Genome-phenome  
Archive

Search docs

Establishing a Federated EGA Node

- What am I doing here?
- What is Federated EGA (FEGA)?
- What are the benefits of joining Federated EGA?
- How do I start?
- What does the journey look like?
- License

Acknowledgements

TOPICS

- Maternity Model
- Data and Metadata Management
- Outreach and Training
- Technical and Operational
- Governance and Legal

Vis meny

Next »

## Establishing a Federated EGA Node

What am I doing here?

What is Federated EGA (FEGA)?

What are the benefits of joining Federated EGA?

How do I start?

What does the journey look like?

License

Acknowledgements

phenome

EGA.

erials

's

se

stitute

d

o

context

me

Archive (EGA) Many countries now have emerging personalized medicine programmes which are

# Suggested content - unstructured

What am I doing here?

What is Federated EGA (FEGA)?

What are the benefits of joining Federated EGA?

How do I start?

What does the journey look like?

License

**Acknowledgements**

# Introduction

- What is the EOSC-Entrust network
  - What is the purpose?
  - What are we trying to accomplish?
- Why should our TRE join the EOSC-Entrust network
  - What are the benefits?
  - What are the consequences?
- How can our TRE join the EOSC-Entrust network
  - Outline the journey from start to onboarded of TREs
  - Requirements? Compliance?

# Legal framework

- Governance
  - Who can agree that a TRE and its data joins the network?
  - Who can approve that access to its data can be shared?
  - Who approves that a TRE fulfils minimum regulatory requirements?
  - What legal entities can represent a node
- Regulations, legislations that will influence
  - Common regulations in European setting
  - Local regulations vs Europeans.
  - GDPR, EHDS
- Implications of joining
  - What may happen to the data? Worst case?
  - Benefits for TRE - what legal obligations can you let go when joining - to make it more interesting to join - do not need to make agreements for every data sharing
- Is there any user certification or passports that we need? If different countries have different requirements - what does a user need to do in order to access data in a TRE that requires a passport?
- Possible sanctions if rules are not followed - exclusion of entire TREs or organisations - linked to GDPR? Local implication

# Architectural specifications

- Understand the different zones and components
  - borrow from DARE-UK
- Understand how these translate to your TRE and how your TRE fits into the network
- Use the ongoing mappings as examples - both for drivers and TREs
- Minimum requirements - the zones that one need to have in order to be a TRE in this context



# Operational procedures

- Requirements that need to be fulfilled to be a compliant EOSC-Entrust node (whatever that is)
  - 5 safes, SATRE, ISO 27001
- How-to approach listing procedures as step-by-step:
  - Fulfil requirements
  - Adjust to changes in requirements
  - Connect to others through federation services
  - Make local/national services interoperable with those of the other nodes
- System admin perspective
- Management perspective

# Interface definitions

- Technical parameters for different protocols to be interoperable

# User guidelines

- Eventually also guiding researchers on how they should use TREs and the network



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# D13.3 - Machine-readable First Edition of the EOSC-ENTRUST TRE Provider Catalogue

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

**Miikka Kallberg,**  
Stefanie Kirschenmann, Heikki Lehväslaiho (CSC)  
Rob Baxter (DARE UK), Mark van de Sanden (SURF)



Funded by  
the European Union

# Introduction to the topic

## **D13.2 Machine-readable Edition of the EOSC-ENTRUST TRE Provider Catalogue**

**Deliverable lead:** Miikka Kallberg (CSC)

Contributing: CSC, NO, SURF, UK

+ And more participants in the calls from the whole project

# Introduction to the topic

## Machine-readable Edition of the EOSC-ENTRUST TRE Provider Catalogue

- **Definitions from the project plan**
  - “A catalogue of suitable national or institutional TREs as part of the EOSC offering”
  - “A machine-readable catalogue of TRE capabilities allowing detailed, comparative analysis of technical capabilities and identification of gaps”
- **Deliverable has direct links to**
  - M10 (Providers): “Inventory & summary of current TRE Provider capabilities”
  - M7 (Drivers): “Initial Driver Requirements for TREs from the four Drivers”

# Planning and next steps

## Task-specific meetings and schedule

- Deliverable D13.3 due **November 2024**
- Two meetings were held to brainstorm and align on the contents of the task
- Meetings will continue after the workshop

## First conclusions

- Format:
  - First version of the TRE provider catalogue will be a spreadsheet
  - Spreadsheet to be developed into database for further iterations
- Contents/use case
  - Discovery: Allow the user to look up which provider/TRE provides which components and capabilities; services; analysis tools
  - TRE Inventory survey (Providers M10) to be used as basis for the spreadsheet



**[Link to spreadsheet](#)**

## Main Categories

-  **EOSC** | **ENTRUST**  
European Network of Trusted Research Environments



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# EOSC-ENTRUST Blueprint & Interoperability Framework – Year 1

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Pål Sætrom



Funded by  
the European Union

# Notes on the contents/Leading questions

## **Presentation-specific**

- Introduction to the topic and current status
  - please include links to outputs and deliverables, if available
- Main proponents in the topic/task
- Planning/next steps
  - Are there any follow-up or related deliverables/milestones?

## **As we have representatives from all the different WPs, please think about:**

- What do you want to share with the other WPs?
- Where is alignment needed?
- What is your update on TRE/SPE requirements?
  - Alignment with SATRE/thoughts on DARE UK/...
  - Providers: What capabilities do you already have within your TRE/SPE? What is missing?

# The Blueprint – Components (proposal)

- Template legal agreements
- Operating procedures
- Architecture specifications
- Interface definitions
- Terminology/Glossary

# The Blueprint – Year 1 Deliverable ([D13.4](#))

- Analysis of DARE UK Federated Architecture Blueprint
  - The DARE UK Federated Architecture Blueprint (“DARE UK Blueprint”)
  - Mapping ENTRUST TRE Providers to the DARE UK Blueprint
    - NorTRE, SURF, CSC
  - Mapping ENTRUST Driver requirements to the DARE UK Blueprint
    - Milestone report M7.1: Initial Driver Requirements for TREs from the four Drivers
    - [Driver mapping](#)
  - Mapping aligning European sensitive data projects to the DARE UK Blueprint
    - EHDS, SIESTA, TITAN
- ENTRUST Blueprint
  - Legal frameworks
  - Architecture specifications
  - Operating procedures
  - Interface definitions
  - Glossary

# DARE UK Blueprint – Data usage patterns

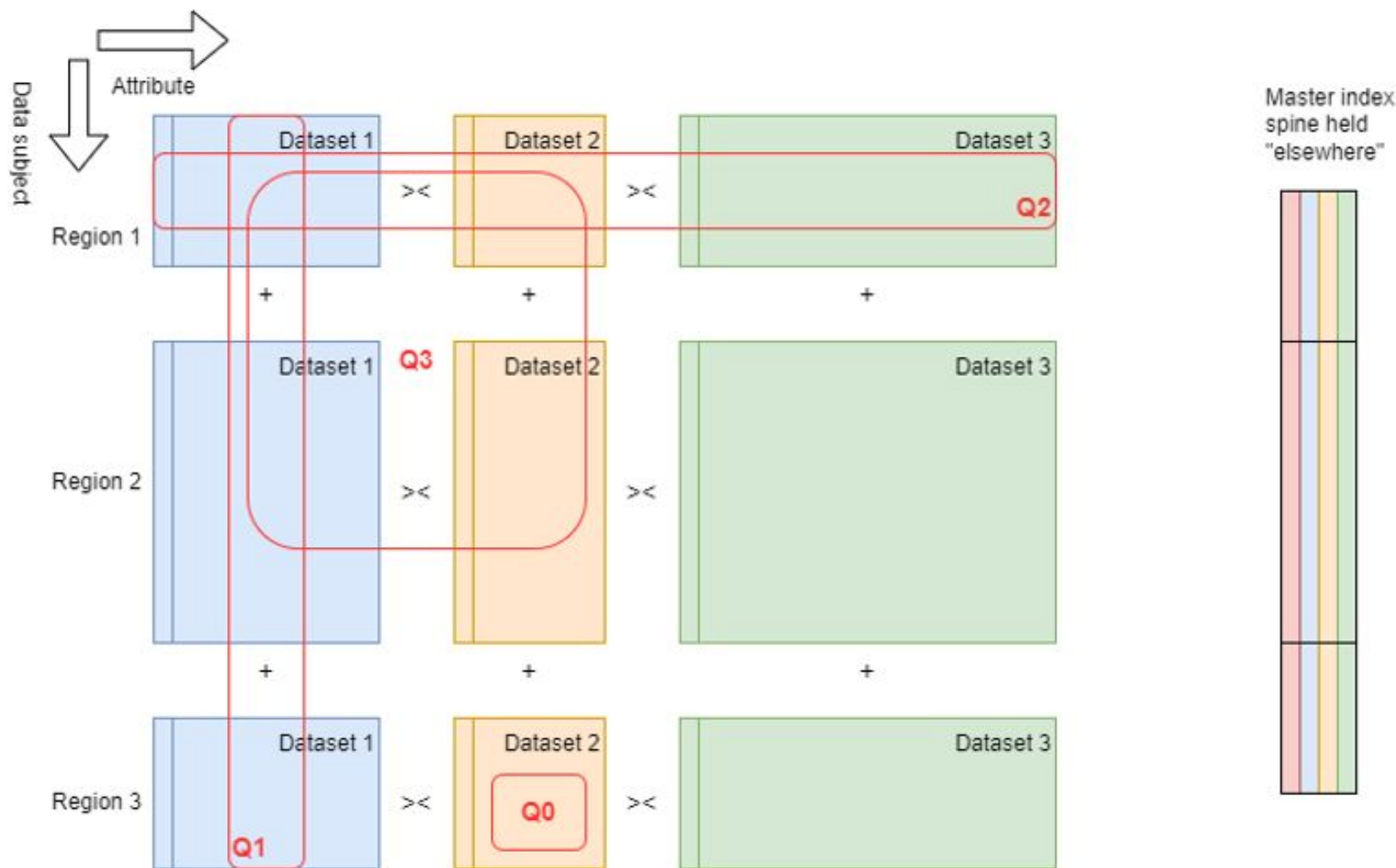


Figure from DARE UK Federated Architecture Blueprint

# DARE UK Blueprint – Capabilities/components

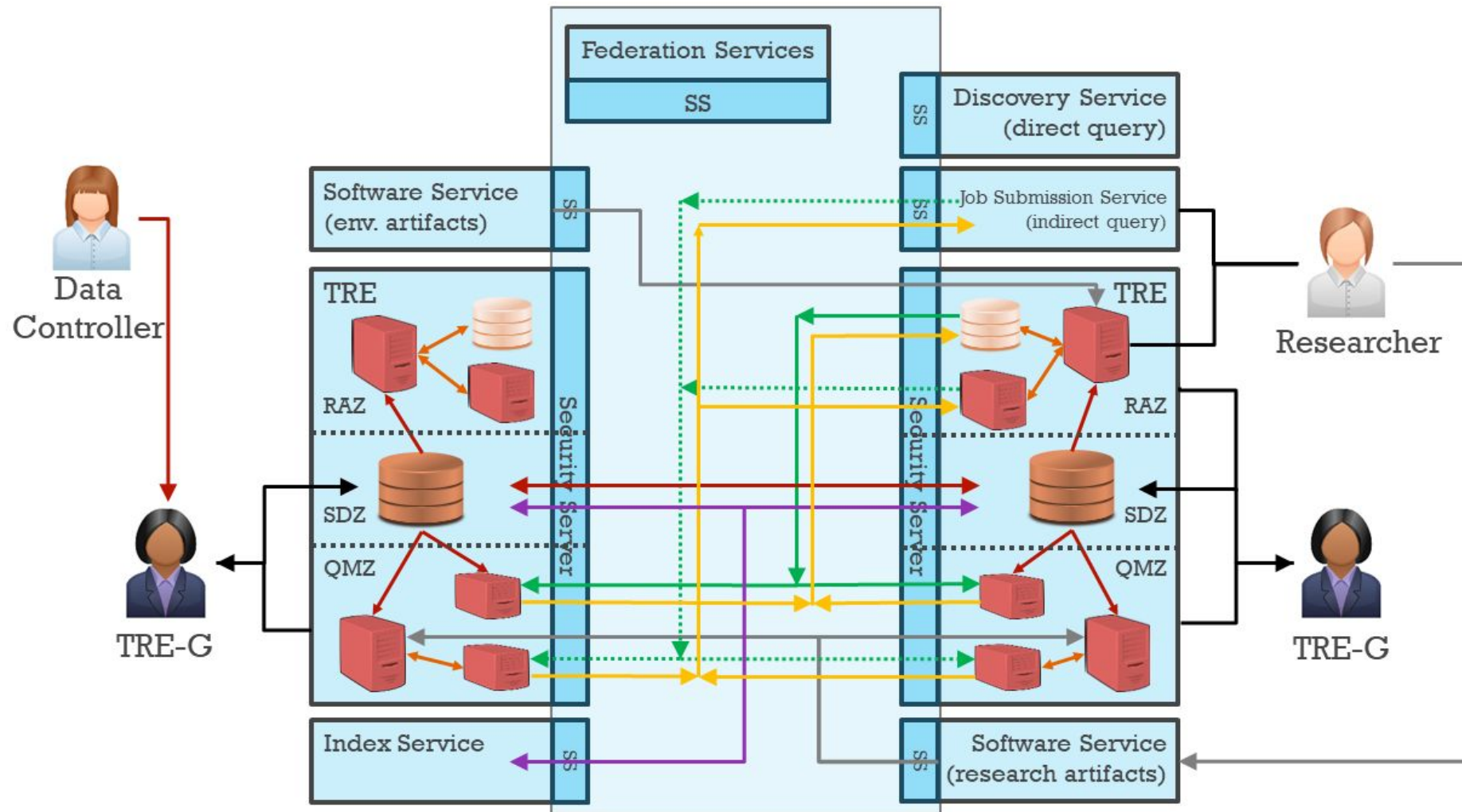
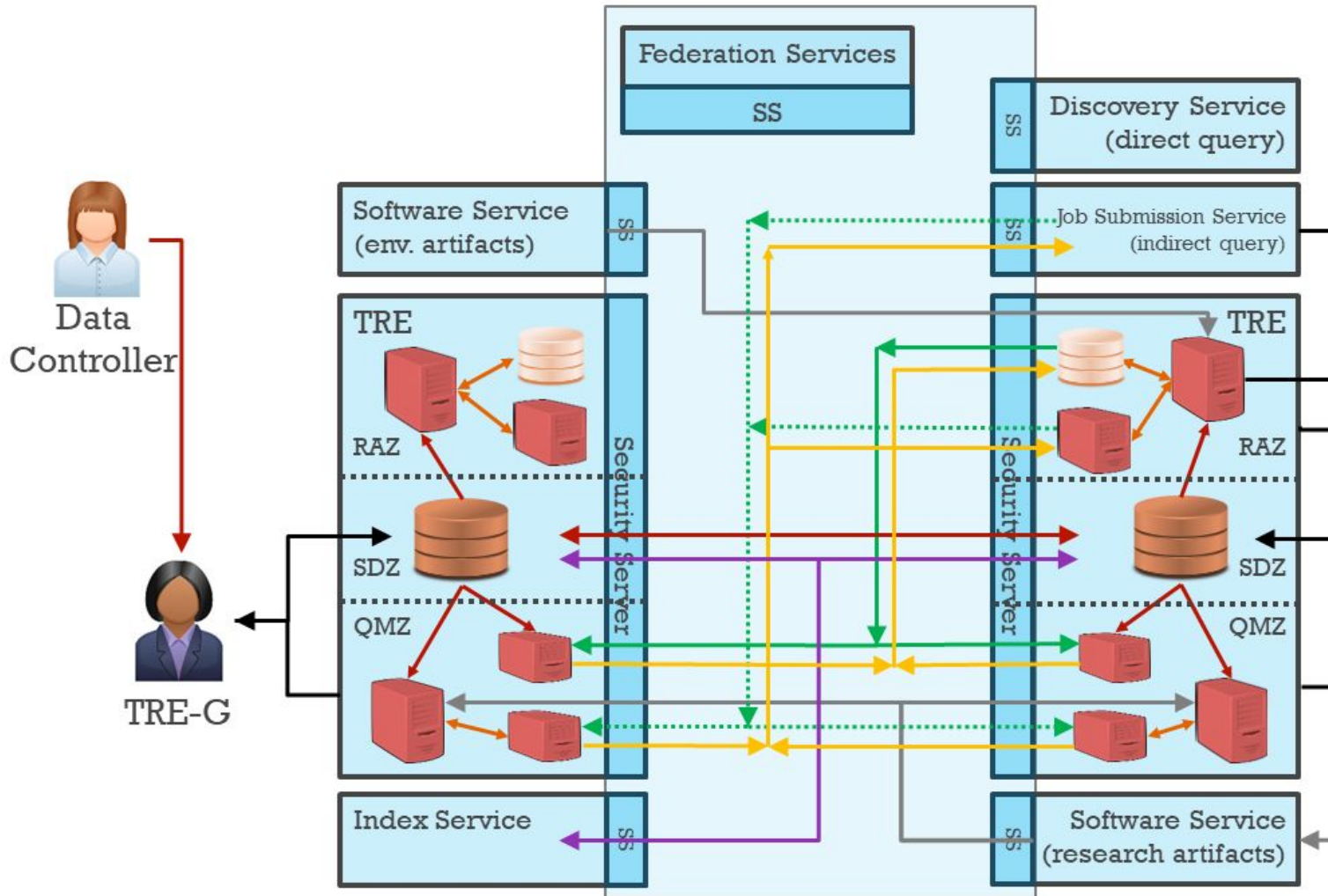


Figure from DARE UK Federated Architecture Blueprint



# DARE UK Blueprint – Capabilities/components



- Federation Services
- Security Server
- Software Service
- Discovery Service
- Job Submission Service
- Index Service
- Research Analytics Zone
- Secure Data Zone
- Query Management Zone

Figure from DARE UK Federated Architecture Blueprint

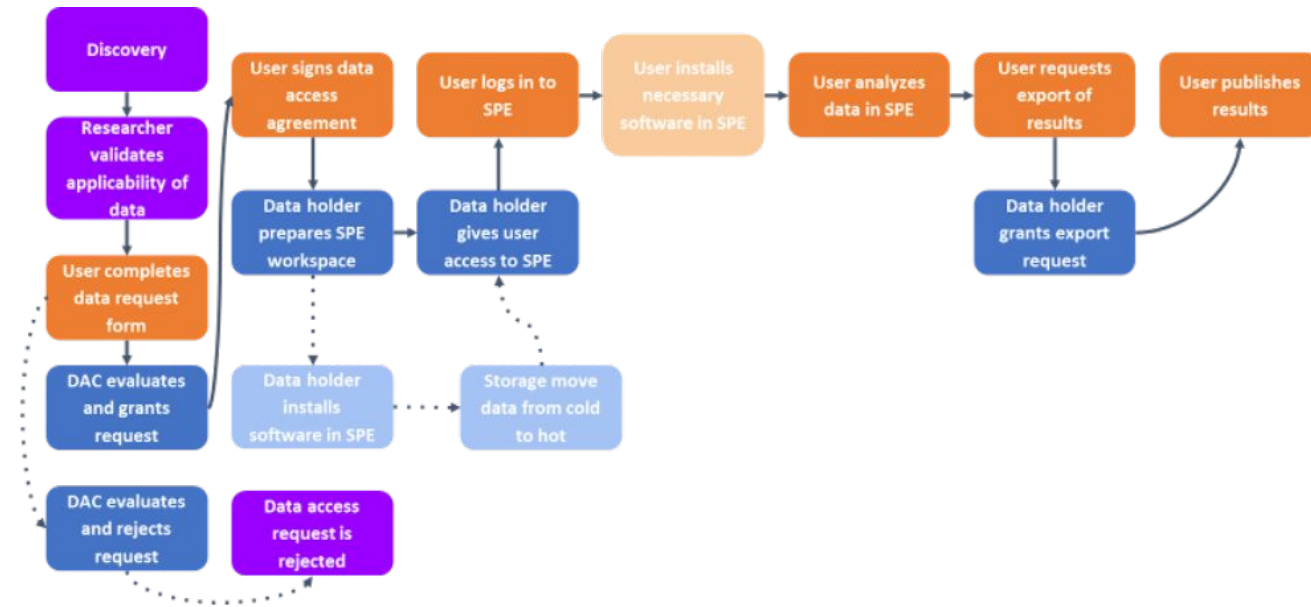
# Drivers – Data usage patterns

Driver	Vertical Usage	Horizontal Usage
Driver 1 – Federated Human Genomics	X data reuse, meta-analyses	data from other domains
Driver 2 – Administrative and social science data	X analyses between countries	(x) data from other domains
Driver 3 – Clinical trials data	X data reuse, meta-analyses	X data from other domains
Driver 4 – Public-Private interactions	(x)	(x) (data from multiple domains)

# User journeys vs DARE UK Blueprint capabilities

## Ex: Driver 1 – Federated Human Genomics

- Data discovery -> “Discovery service”
- Access application -> not part of Blueprint?
- Data access and analysis -> “Research analytics zone”
- Export of results-> “Output Control” (sub-capability within Blueprint)
- Compliance and reporting -> not explicitly modelled?



# User journeys vs DARE UK Blueprint

## Supported capabilities

- Discovery service (D1, D2, D3)
- Research analytics zone (D1, D2, D3, D4)
- Output Control (D1, D2, D3)

## Missing capabilities

- Data access/project application/approval (D1, D2, D3)
- User certification (D2, D3)
- Compliance and reporting (D1)
- Data publishing/archiving (D3)
  - "Publishing with Data credit attribution"
- Role-based services within Research Analytics Zone (D4)
  - "Assign SD services to the project"

# Key interoperability requirements vs DARE UK Blueprint

## Supported capabilities

- (Encrypted) Data transfer between environments (D2, D3)
- Software applications (D3, D4)
- Mechanisms for timely deletion of data post-expiration (D2)
- Archiving for future validation or reproducibility under regulations (D3)

## Possible capabilities

- Internet connection from within TRE (Software services?) (D1)
- Scalable infrastructure (through Blueprint itself?) (D1)
- Metadata (General + domain-specific) (D3)
- Service design (Research analytics zone) (D4)

# Key interoperability requirements vs DARE UK Blueprint

## Missing capabilities

- Data access/project application/approval (D1, D2, D3)
- User certification (Safe Researcher' training and/or passport; Ethical guidance) (D2, D3, D4)
- General user training (D2, D3)
- Anonymization (pseudonymization?) (D1, D3)
- Data standardization/archiving/publishing/citation (D2, D3)
- Compliance with varied national legal frameworks for data sharing (D2)
- Compliance and reporting (D1)

# Next steps

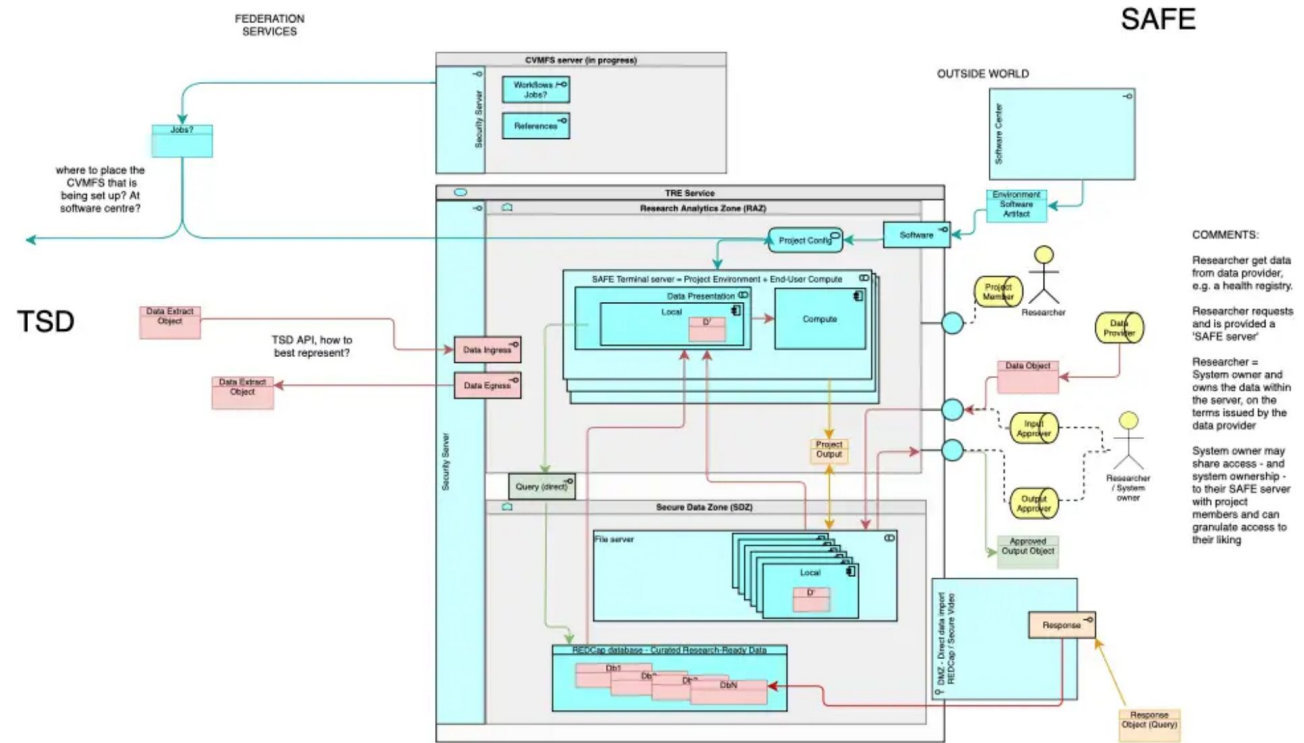
- Mapping TRE providers to DARE UK Blueprint

- NorTRE
- SURF
- CSC

- ENTRUST Blueprint

- Architecture specifications
- Glossary
- Operating procedures
- Legal frameworks
- Interface definitions

For internal review Nov. 1





---

# ENTRUST

European Network of Trusted  
Research Environments

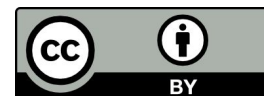
 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union





# Interoperability challenge demonstrations

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Per Kulseth Dahl

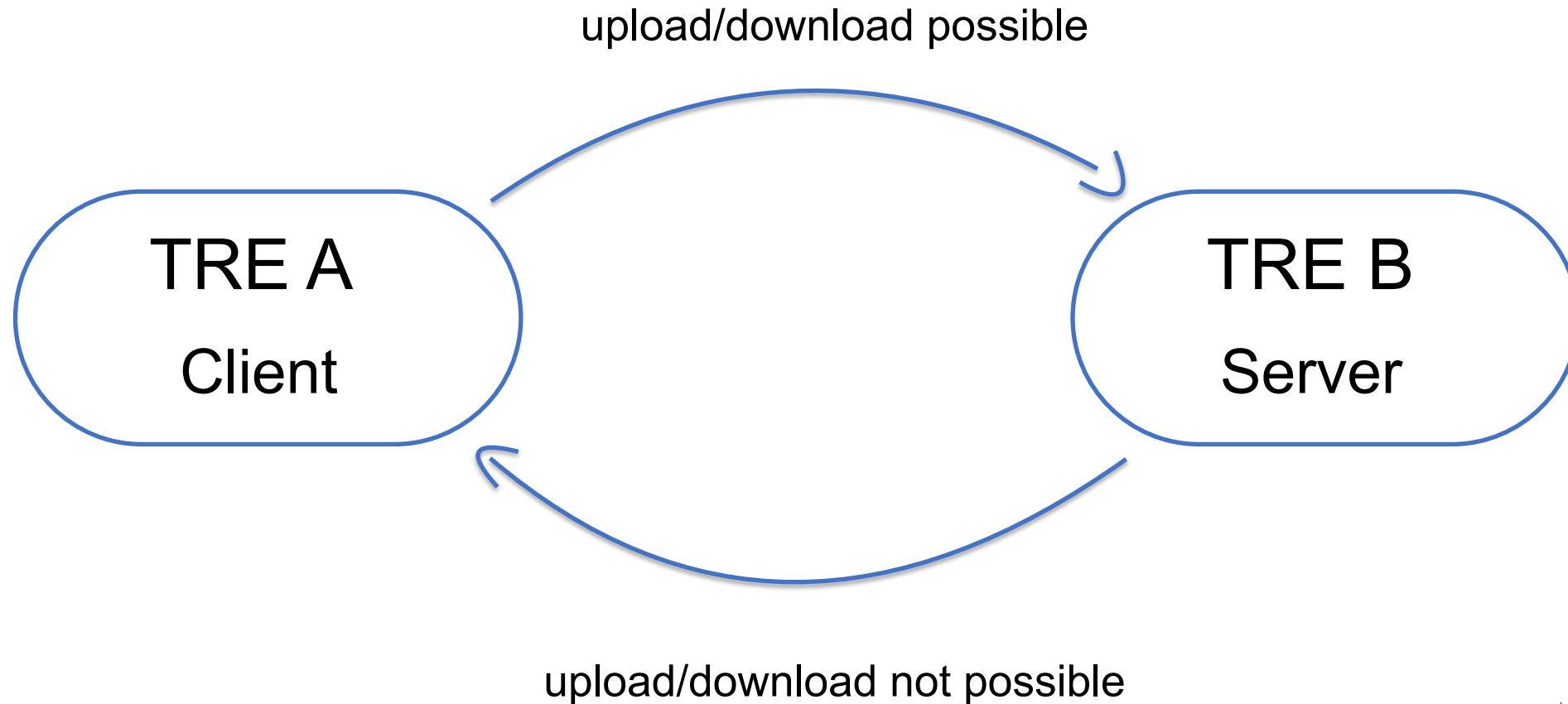


Funded by  
the European Union

Sensitive data transfer between TREs

Reusable information from secure environments

# Sensitive data transfer between TREs



# Challenges

- Respecting policies of both TREs

# Challenges

- Respecting policies of both TREs
- Logging without central infrastructure

# Challenges

- Respecting policies of both TREs
- Logging without central infrastructure
- TRE A's export policy

# Reusable information from secure environments



UNIVERSITY  
OF OSLO



Clinical Research Data Sharing Repository

Supporting clinical researchers in sharing their data

Login

Contact Us

Browse

The clinical research Data Sharing Repository is capable of holding any type of digital object -data sets, documents, media file etc- in a secure research environment (TRE). The repository collects the metadata necessary for the Findability of the objects, promoting data sharing in clinical research.



About  
User Guide  
crMDR

All Projects are supported by the Horizon Europe and Horizon 2020  
Programme.  
Canserv under GA 101058620, BY-COVID under GA 101046203  
EOSC-Life under GA 824087



<https://crdsr.ecriin.org/login>

# Search - Request Access - Submit



crDSR: Data Sharing Repository  
v1.5.3

## Studies

Title



Search study...

Study ID	Title	Organisation	Type	Status	Actions
DSRS-1	Example Study to demonstrate and to evaluate the functionality of the clinical research Data Sharing Repository	ECRIN	Observational	Ongoing	
DSRS-2	Assessing Immune Response of Different COVID-19 Vaccines in Older Adults	Universitätsklinikum Köln	Interventional	Active, not recruiting	

<https://crdsr.ecriin.org/browsing>



# Search - Request Access - Submit



crDSR: Data Sharing Repository  
v1.5.3

## Data Objects

Title		Search data object...			
Study ID	Title	Organisation	Type	Linked study	Actions
DSRO-1	Example Data Object within Example Study	ECRIN	Study overview	DSRS-1	
DSRO-6	Trial Protocol	Universitätsklinikum Köln	Study protocol	DSRS-2	
DSRO-7	Master trial protocol	Universitätsklinikum Köln	Study protocol	DSRS-2	
DSRO-8	Data Management Plan	Universitätsklinikum Köln	Data management plan	DSRS-2	

<https://crdsr.ecriin.org/browsing>

# Submit

- Data Transfer Process
- Repository Manager
- Data Object Provider
- TSD User
- TSD Import

# Request Access

- Data Use Process
- Data Object Requester
- TSD Export

# Repository Storage Structure

```
repository/  
  <study>/  
    <dataset>/  
      data/  
        <instance>  
        <instance> ...
```

```
pnnn-r<dataset>-group  
pnnn-w<dataset>-group
```

# Links

- TSD API Client  
<https://github.com/unioslo/tsd-api-client>
- ECRIN metadata schemas  
<https://newmdr.ecrin.org/About>
- ECRIN RMS user interface  
<https://github.com/ecrin-github/rms-portal-new/tree/main>
- ECRIN back end  
<https://github.com/ecrin-github/esbs-django>
- Clinical Research Data Sharing Repository guide  
<https://crr.gitbook.io/crdsr>



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union



# Closing remarks

1st EOSC-ENTRUST Evaluation & Adoption Workshop,  
24-25 September 2024, Helsinki

Pål Sætrom



Funded by  
the European Union

# Thanks for your participation!

## **Thank you all for the great presentations and input**

Technicalities regarding the workshop

- We would like to publish the outcomes again via zenodo (presentation slides)
  - Speakers: Please fill out the [consent form](#)
- Follow-up:
  - Upcoming deliverables: Reviewers needed
  - Please feel welcome to participate in upcoming task-related meetings



# Points moving forward

- Driver Requirements vs Provider Capabilities
  - User journeys inform requirement/capability mappings
  - How to (best) Capture, Describe, Present Provider capabilities?
  - Agree on common framework between ENTRUST WPs
    - Requirements gathering framework
  - Language disconnect:
    - Driver/User “Federation” vs Provider/Technical “Federation”
    - All Drivers describe distributed Data usage patterns
- Driver Requirements vs Technologies & Workflows
  - User certification (training, accountability)?
  - Researcher registry – what information is needed?
  - Project level vs. fine grained data access control?
  - FAIR: Data discovery vs Metadata standards vs Standardized data vs Data credit attribution

# Points moving forward (2)

- Cross-WP alignment & priorities
  - Be aware & beware of EHDS
  - Ambitions: Blueprint & Interoperability Framework vs Federation
  - Prioritisation should come from the drivers
    - Fundamental capabilities vs ease of implementation
- Future work & discussions
  - Legal agreement frameworks – general vs tied to specific capabilities?
  - Operating procedures
    - Setting up/Joining an ENTRUST federation (“a group of computing providers”)
    - Running specific ENTRUST capabilities
  - Interface definitions

# Blueprint – Roadmap

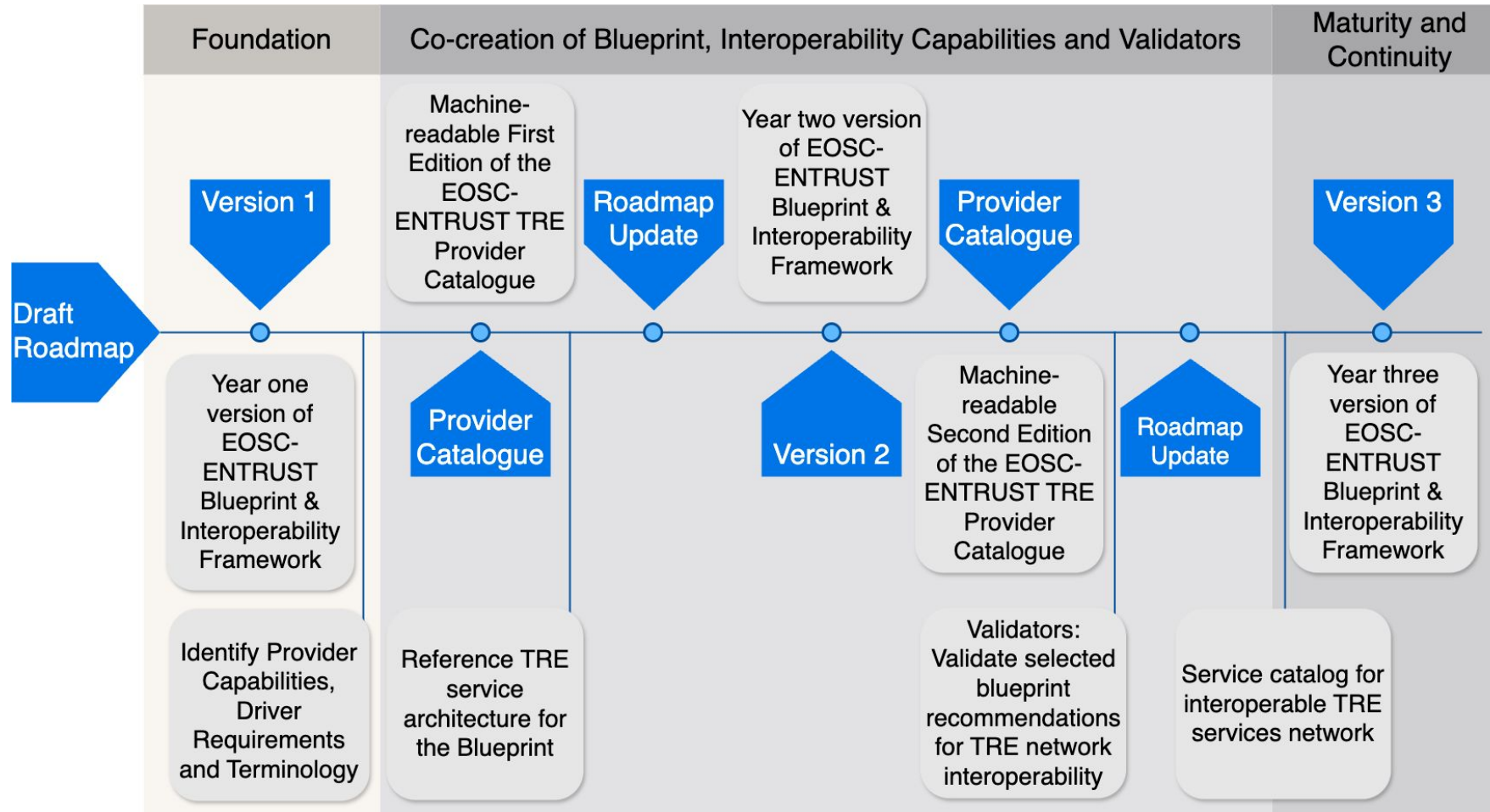
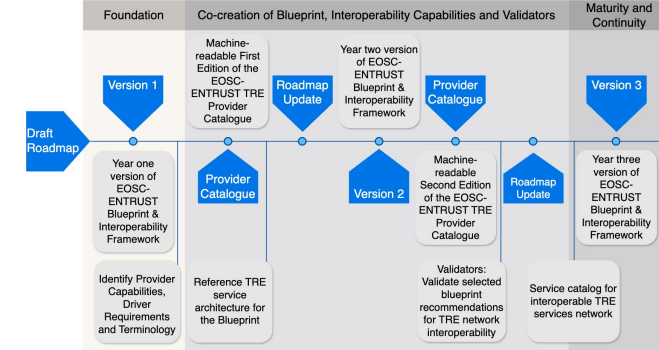


Figure from D13.1 Draft Roadmap

# Blueprint – Next steps

- Nov. 1, '24
  - D13.2 – Training package for EOSC-ENTRUST Year one Blueprint & Interoperability Framework
  - D13.3 – Machine-readable First Edition of the EOSC-ENTRUST TRE Provider Catalogue
  - D13.4 – Year one version of EOSC-ENTRUST Blueprint & Interoperability Framework
  - M15 – Key selected interoperability challenge demonstrations implemented
- May, '25
  - M17 – 2nd EOSC-ENTRUST Requirements and Capabilities Workshop
  - D14.2 – Updated Roadmap for EOSC-ENTRUST Blueprint



# Architecture WP – Upcoming meetings

- WP meeting
  - Oct. 7, 13:00-14:00 CEST
  - RO-Crate
- D13.4 Blueprint:
  - Oct. 2, 15:00-16:00 CEST?
  - NorTRE mapping to DARE UK Blueprint
  - Oct. 9, 14:00-15:00 CEST?
  - SURF mapping to DARE UK Blueprint
  - Oct. 15, 14:00-15:00 CEST?
  - ENTRUST Blueprint Architecture draft
- D13.3 Provider catalogue
  - Oct 3, 13:00-14:00 CEST
- D13.2 Training package
  - Oct 4 10:00-11:00 CEST (Weekly until deadline, may adjust next slots)

*“...there is so much going on in the TRE/SPE space, the World needs a more robust framework to make sense of it all...”*

— Peter M, optimist



---

# ENTRUST

European Network of Trusted  
Research Environments

 [www.eosc-entrust.eu](http://www.eosc-entrust.eu)

 [@eosc\\_entrust](https://twitter.com/eosc_entrust)

 [/company/eosc-entrust](https://www.linkedin.com/company/eosc-entrust)



Funded by  
the European Union

