EUROPEAN BIG DATA VALUE FORUM

Data Spaces

Data Spaces and Cybersecurity

27/10/2023, 09.00am -10.00am CET

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

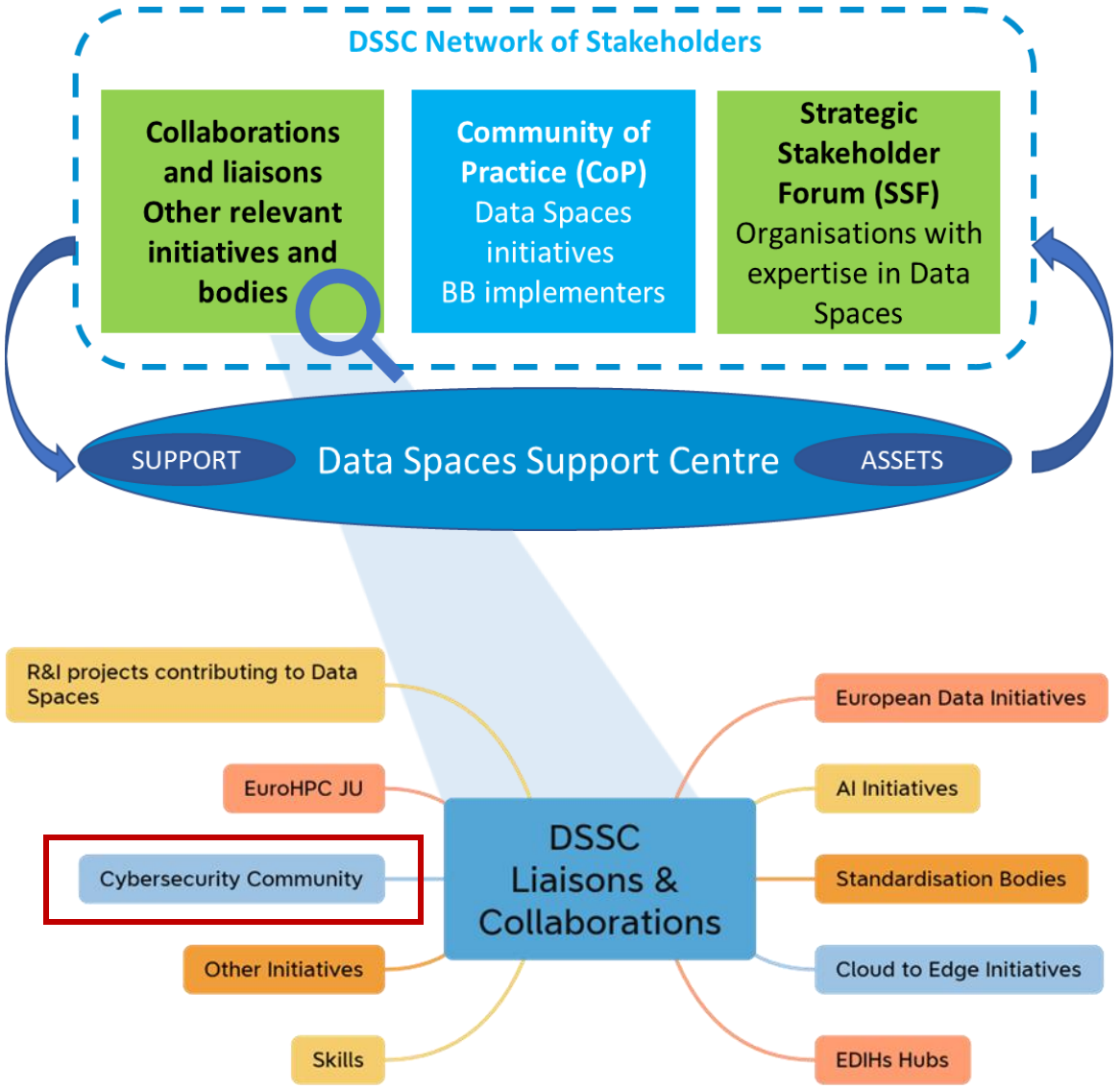
Why we are here

- The DSSC Network of Stakeholders includes all relevant organizations and initiatives involved in the development of data spaces.
- Cybersecurity community as part of the Collaborations and Liaisons Group

Session Objectives:

- Introduce to the main concepts, current developments and communities
- Initiate dialogue among communities
- Identify challenges and opportunities in the interplay between data spaces, cybersecurity and data protection
- Look for key areas for future more comprehensive discussions and collaborations

DATA SPACES SUPPORT CENTRE



DATA SPACES SUPPORT CENTRE

Tuomo Tuikka
VTT

Dinos Kokosis
European Commission

Jesus M. Santamaria
Tecnalia

Savvas Rogotis
Big Data Value Association

ebdvf.eu
#EBDVF23

Ricard Martinez Martinez
University of Valencia

Freek Bomhof
TNO

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC
Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

EU23 SPANISH PRESIDENCY
COUNCIL OF THE EUROPEAN UNION

DATA SPACES SUPPORT CENTRE

Data Spaces Support Centre
Overview of assets - links to Cyber Security and Data Protection

Tuomo Tuikka (VTT)

European Big Data Value Forum - 27 October 2023

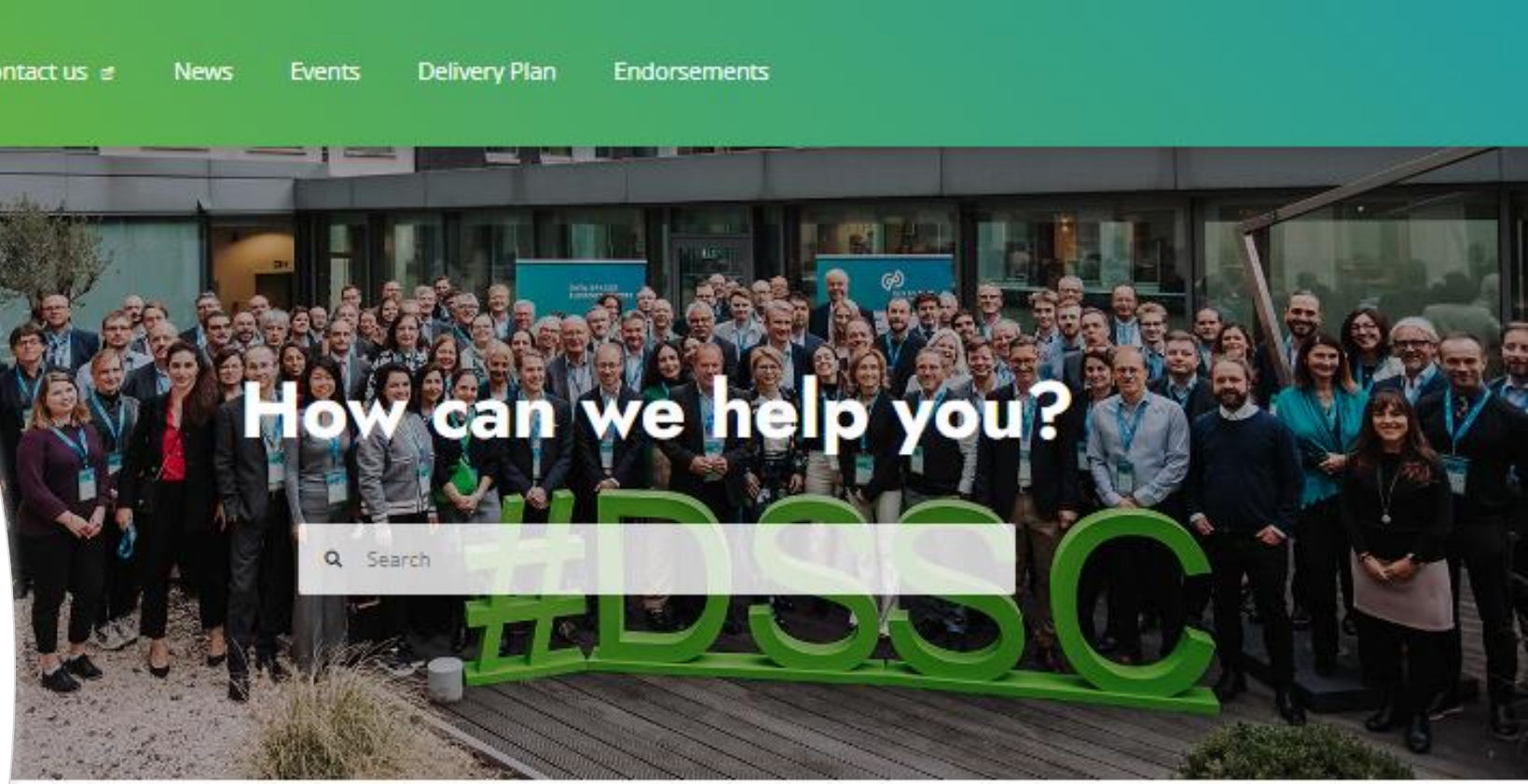
Data Spaces and Cyber Security

Funded by the European Union

DSSC.EU

Data Spaces Support Centre

- The virtual organization and EU-funded project which supports the deployment of common European data spaces and promotes the reuse of data across sectors



About

Support

Knowledge Base

The Data Spaces Support Centre receives funding from the European Union Digital Europe Programme under grant agreement n° 101083412.

Funded by the European Union

DSSC mission

DATA SPACES SUPPORT CENTRE

- Enable data spaces to reach a higher flight level faster: a **quick start** and an **accelerated scale-up**
- Provide the tools to address the **basic organizational and technical matters**, required by every data space
- This includes a **blueprint**, best practices, common standards and reference implementations which will be developed according to a **co-creation process**
- Enable dataspaces to focus on their domain-specific business challenges and **provide business benefits to their participants**

The Data Spaces Support Centre receives funding from the European Union Digital Europe Programme under grant agreement n° 101083412.

Funded by the European Union

Data Spaces Support Centre releases
October 2023

DATA SPACES SUPPORT CENTRE

https://dssc.eu/page/knowledge-base

Starter Kit

Blueprint

Building Blocks

Conceptual model

Glossary

Collection of Standards

The Data Spaces Support Centre receives funding from the European Union Digital Europe Programme under grant agreement n° 101083412.

Funded by the European Union

Building Blocks

DATA SPACES SUPPORT CENTRE

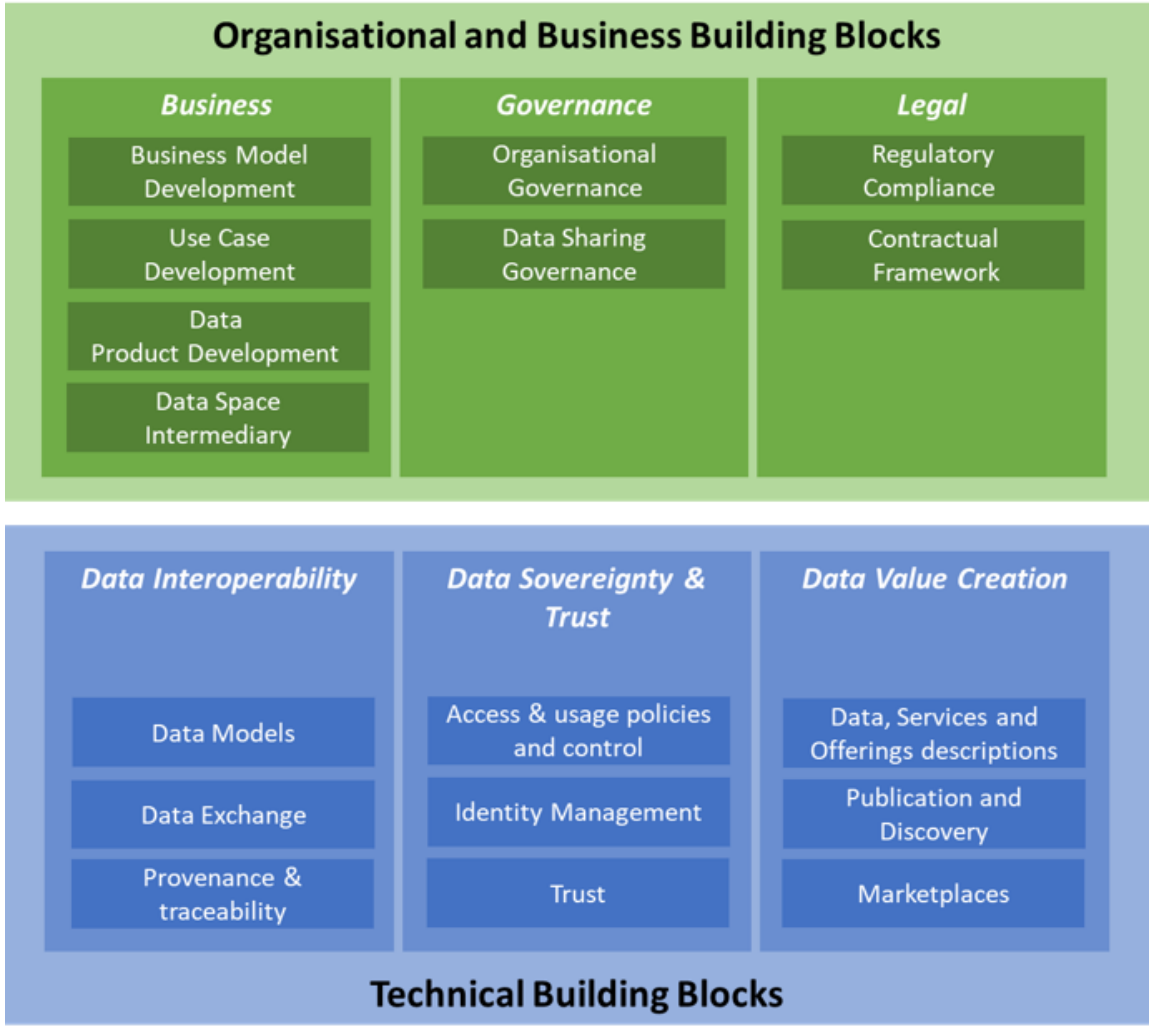
Organisational & business building blocks

Describe capabilities on a governance, legal and business level.

Technical Building Blocks

Describe capabilities on a technical level about:

Data Interoperability
Data Sovereignty & Trust
Data Value Creation



Funded by the European Union

DSSC and Cyber Security

DATA SPACES SUPPORT CENTRE

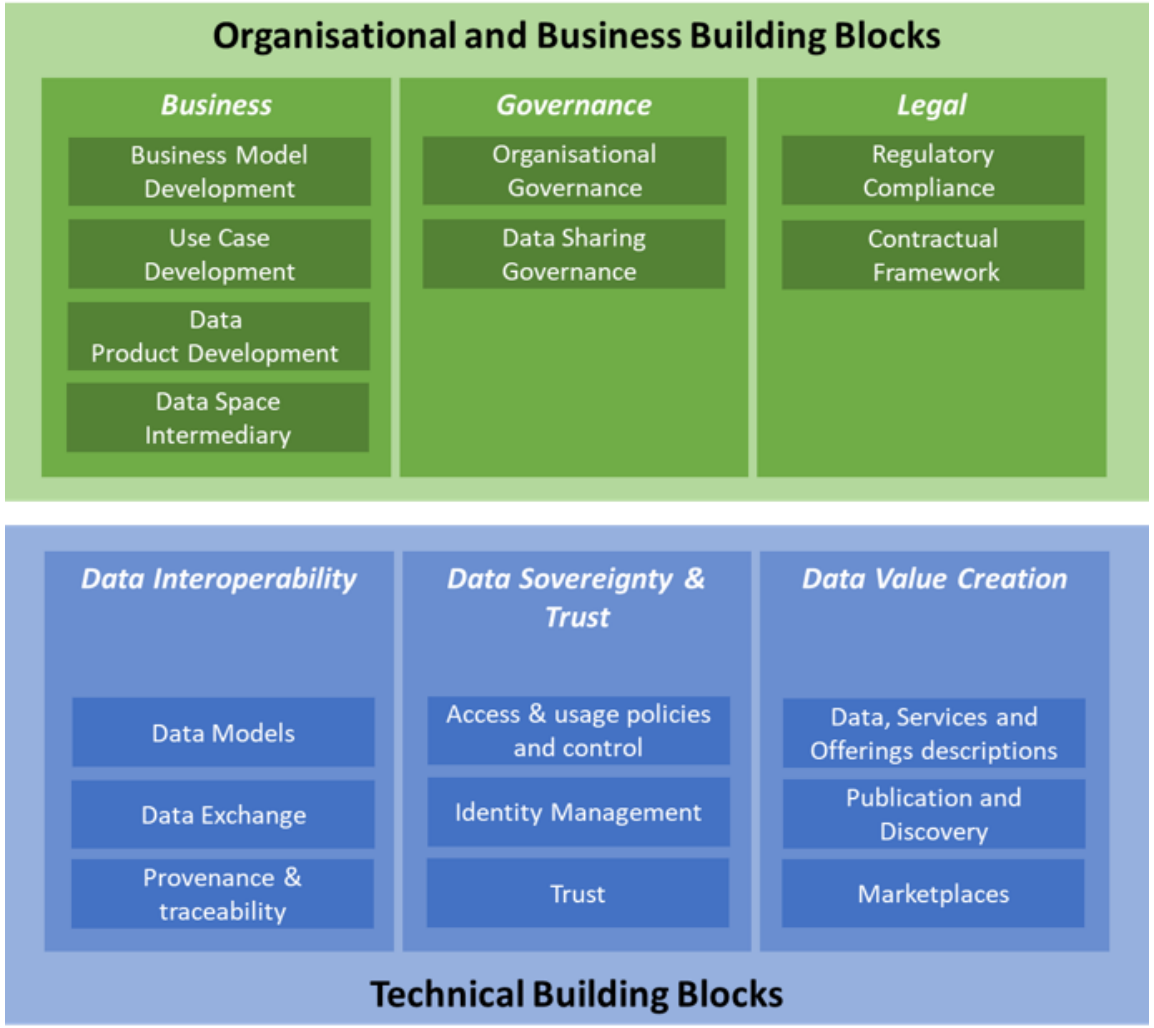
- Expert group input for building blocks
  - Data Sovereignty and Trust
- Cyber Security by design
  - Link to design principles and development
- CSA project requirements gathered:
  - Mechanisms that guarantee data control
  - Encryption services, cryptography
  - Identity and access management use of standards (SAML, AI, passports, GA4GH, VC)
  - Detecting and avoiding cyber-attacks
  - Anonymisation or deleting data

Funded by the European Union

Cybersecurity topics integration

DATA SPACES SUPPORT CENTRE

- **Common European Data Space projects**
- **Input from the community**
  - **Events, workshops with topic corresponding organizations, Web platform – dssc.eu**
- **Expert groups**
- **Blueprint 1.0 forthcoming spring 2024**



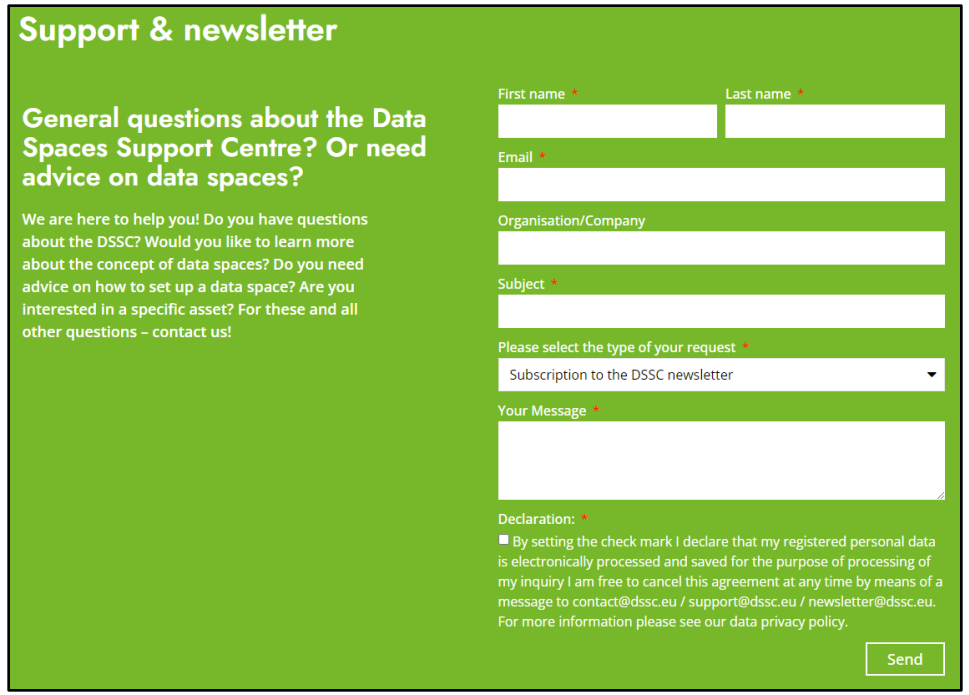
Funded by the European Union

Engage with us!

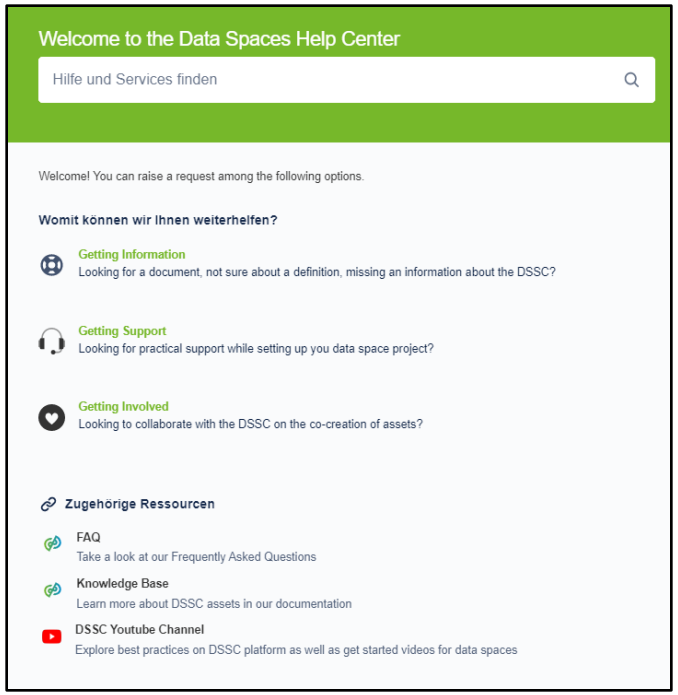
For support or contributions

DATA SPACES SUPPORT CENTRE

Visit www.dssc.eu for support and subscribing our Newsletter!



Visit the [DSSC Platform](#) for support and engagement!



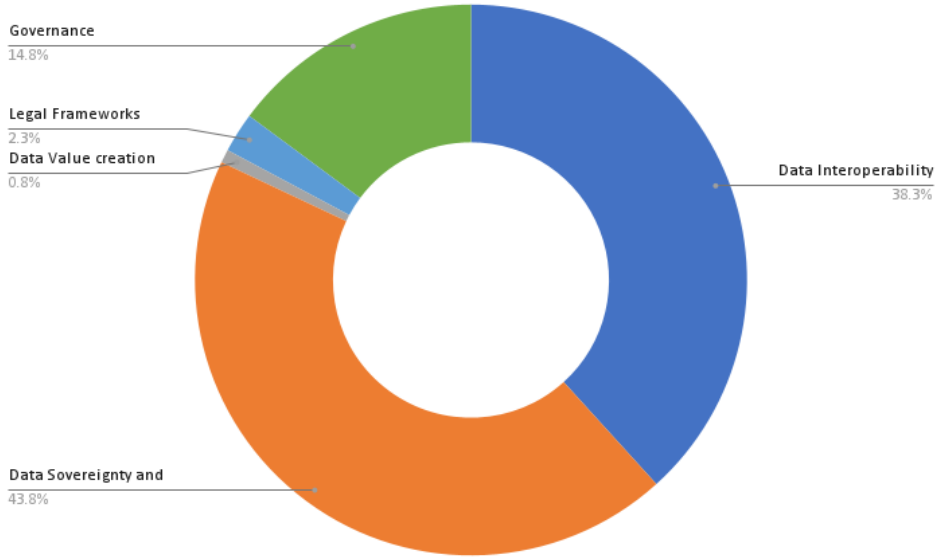
The Data Spaces Support Centre receives funding from the European Union Digital Europe Programme under grant agreement n° 101083412.

Funded by the European Union

Collection of Standards

DATA SPACES SUPPORT CENTRE

- Lists all the candidate standards and technologies to be referred in the Specifications of Building Blocks for their implementation.
- Standards are mostly related to the technical building blocks. A technical building block is designed by providing both a functional and a technical specification.
- Users: Expert groups, Data Spaces initiatives, Standardization initiatives, Research and industrial communities
- What are the most needed standards from Cyber Security point of view?



Funded by the European Union

How to keep posted

DATA SPACES SUPPORT CENTRE

- Strategic Stakeholder Forum
- News and publications at dssc.eu
  - Get support
- Join the Thematic Groups
  - Knowledge base and periodic meetings
  - Get involved
- Monthly DSSC Insights Series
  - Next one about the Blueprint on 12th October at 16:00
- Data Spaces Symposium in March 2024

The Data Spaces Support Centre receives funding from the European Union Digital Europe Programme under grant agreement n° 101083412.

Funded by the European Union

DATA SPACES SUPPORT CENTRE

Thanks!

More info at contact@dssc.eu

The Data Spaces Support Centre receives funding from the European Union Digital Europe Programme under grant agreement n° 101083412.

Funded by the European Union

European Big Data Value Forum (EBDVF)

The Digital Europe Programme and Horizon Europe: Unlocking the Power of Data Spaces and Cybersecurity

Dinos Kokosis

DG CNECT H1, Cybersecurity Technology and Capacity Building

27 October 2023

European Commission

The Digital Europe Programme

- DEP is a funding initiative designed to harness the potential of digital technologies across Europe
- Its primary aim is to accelerate digital transformation, making Europe a global leader in the digital age
- DEP Work Programme 2023-2024 is going through a revision, which will include several modern technologies by the Security Operational Centres (SOCs) (including but not limited to AI, data management, deployment & uptake)
- National Contact Points for DEP on the Digital Europe section of the FTP > Helpdesk & Support Services tab (updated list expected on Friday 27.10.2023)

European Commission

Horizon Europe

- Horizon Europe is the EU's flagship research and innovation program
- It has a budget of nearly €100 billion and is a key component of the DEP
- Horizon Europe addresses societal challenges and promotes scientific excellence
- This specific Horizon Europe topic focuses on building data spaces and enhancing cybersecurity
- National Contact Points for HE on the HE section of the FTP > Helpdesk & Support Services tab

European Commission

Overview of HE CL3 CS 2023 call

Topic	Instrument	EUR (million)	Projects	Opening date	Deadline date
Increased Cybersecurity (CS)					
CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructure					
HORIZON-CL3-2023-CS-01-01:Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)	IA	28,00	4	29/06/2023	23/11/2023
CS02 –Privacy-preserving and identity technologies					
HORIZON-CL3-2023-CS-01-02: Privacy-preserving and identity management technologies	IA	15,70	4	29/06/2023	23/11/2023
CS03 - Secured disruptive technologies					
HORIZON-CL3-2023-CS-01-03: Security of robust AI systems	RIA	15,00	2	29/06/2023	23/11/2023

The European Cybersecurity Competence Centre

- Aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community.
- Make strategic investment decisions and pool resources from the EU, its Member States
- Improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy
- Deliver on the ambitious cybersecurity objectives of DEP & HE
- Support the deployment of innovative cybersecurity solutions
- Facilitate collaboration and sharing of expertise and capacities among all relevant stakeholders, in particular research and industrial communities, as well as public authorities, in the Community

Q&A

European Commission

European Commission

Thank you!

© European Union 2021

Unless otherwise noted the reuse of this presentation is authorised under the CC BY 4.0 license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

Image credits: © ivector #235536634, #249868181, #251163013, #266009682, #273480523, #362422833, #241215668, #244690530, #245719946, #251163053, #252508849, 2020. Source: Stock.Adobe.com. Icons © Flaticon – all rights reserved.

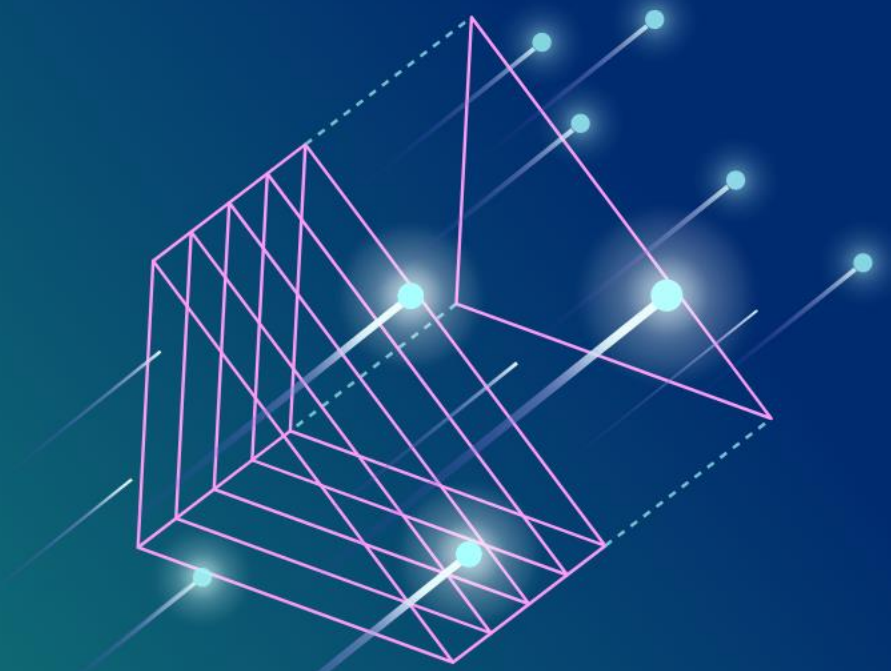
European Commission

EUROPEAN BIG DATA VALUE FORUM

BDV BIG DATA VALUE ASSOCIATION

Data Spaces & Cybersecurity

Where Data Spaces and Cybersecurity meet



Jesus M. Santamaria

Oct 27th, 09:00

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

Landscape of cybersecurity actors

- European Commission
- ENISA
- ECCC
- ECSO

Landscape of cybersecurity actors

European Commission

- **EC and the EU Cybersecurity Strategy**
- It addresses three areas of EU action
  - ▷ resilience, technological sovereignty and leadership
  - ▷ operational capacity to prevent, deter and respond
  - ▷ cooperation to advance a global and open cyberspace

Landscape of cybersecurity actors

- **ENISA, European Union Agency for Cybersecurity**
  - EU agency dedicated to achieving a high common level of cybersecurity across Europe.
  - Established in 2004 and strengthened by the EU Cybersecurity Act
  - Contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies

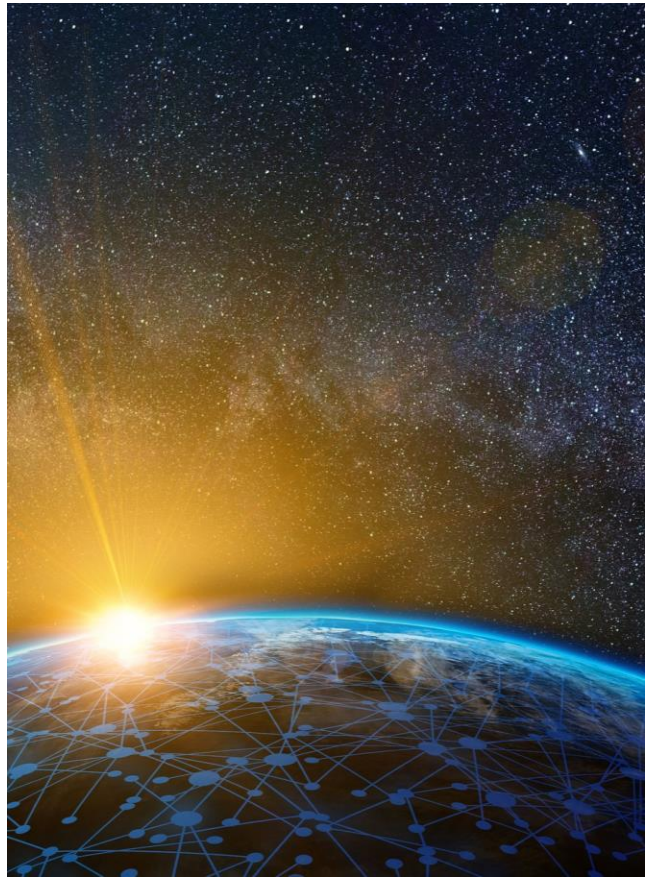
Landscape of cybersecurity actors

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **ECCC, European Cybersecurity Competence Centre** (and associated NCCs, Network of National Coordination Centres)
  - contributing to the wide deployment of the latest cybersecurity technology
  - providing financial support and technical assistance to cybersecurity start-ups
  - supporting research and innovation based on a comprehensive industrial and research agenda
  - driving high cybersecurity standards
  - facilitating the cooperation between the civil and defence spheres

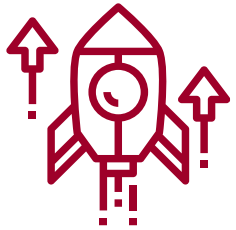
Landscape of cybersecurity actors

- **ECSO, European Cyber Security Organisation**
  - Created in 2016 as the contractual counterpart to the European Commission for implementing Europe's unique **Public-Private Partnership in Cybersecurity** (2016-2020)
  - The aim of the partnership was to **foster cooperation between public and private actors** in order to allow people in Europe to access **innovative and trustworthy European solutions**
  - Today, ECSO builds upon the many successes of the Partnership and with its cross-sectoral membership contributes to **developing cybersecurity communities** and builds the **European cybersecurity ecosystem**
  - ECSO is leading the **ECCO project** (contract from DG-CNECT) for the development of the **European Cybersecurity Community**



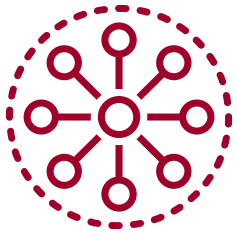
Landscape of cybersecurity actors

Large companies (users and providers)



SMEs & start-ups

Research centres, Universities



European, National and Regional clusters & associations

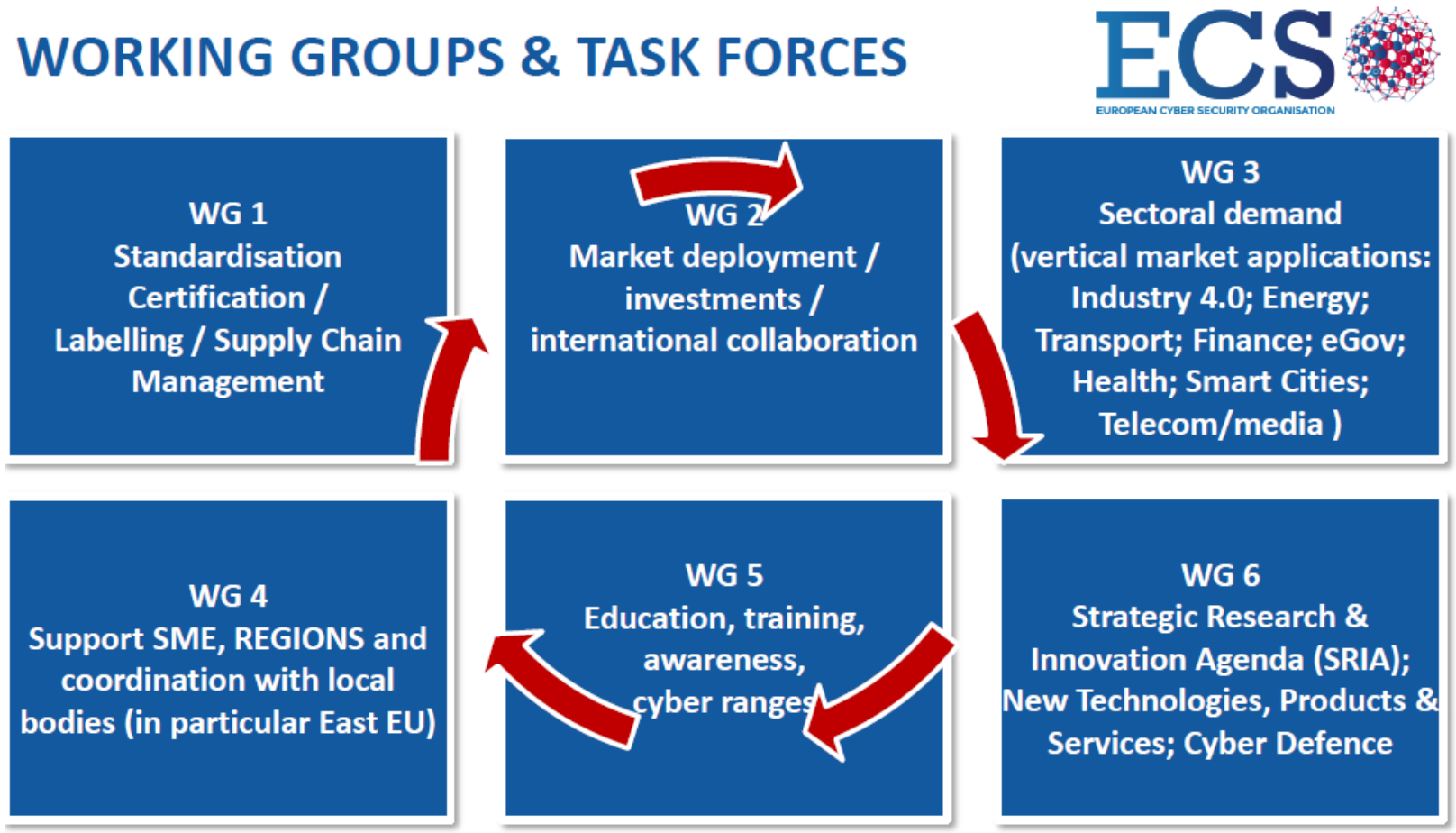
Local, regional and national public administrations

Investors

End-users and operators of critical infrastructures and essential services

As of today, ECSO counts more than 300 Members

Landscape of cybersecurity actors



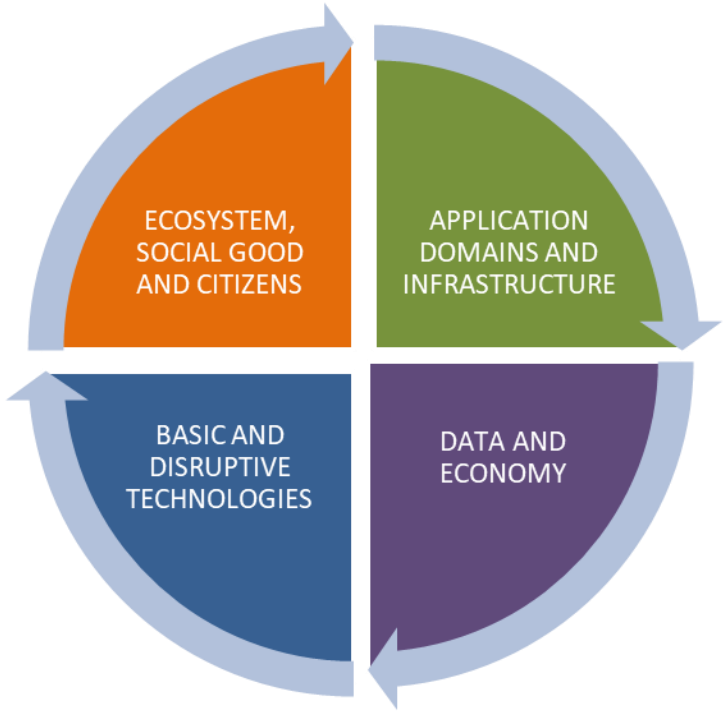
TASK FORCE

EU Legal and Policy

Landscape of cybersecurity actors

WG6 – SRIA and Cyber Security Technologies: ECSO cybersecurity priorities for Horizon Europe and Digital Europe Programmes

- Risks / Threat management
- Data & AI (including privacy)
- Cyber secure HW & SW (including crypto) supply chains
- Infrastructure resilience
- Skills
- Support to European competitiveness

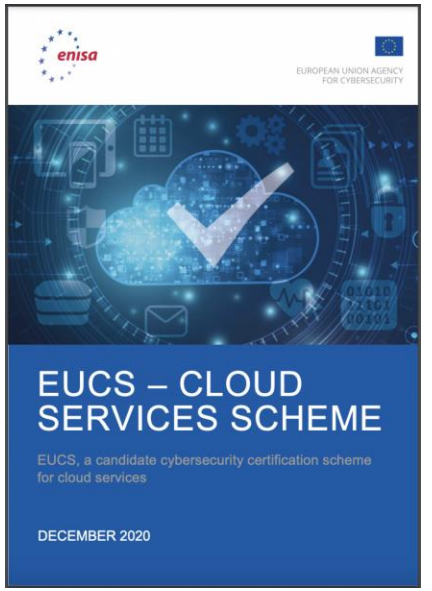


Some key security aspects related to ECSO WGs and Data Spaces

- Certification schemes
- PETs and Trust Anchor Framework related technologies
- Legal Compliance (Cybersecurity Act and GDPR)

Certification schemes

- Related to ECSO WG1 task: Support the roll-out of **EU ICT security certification schemes**, standard and legislative recommendations
- A relevant case is **EUCS, European Union Cybersecurity Certification Scheme for Cloud Services**, which looks into the certification of the cybersecurity of cloud services supporting the three assurance levels in the EU Cybersecurity Act ('basic', 'substantial' and 'high')
- For instance, DOME project (implementing a Federated European Marketplace Ecosystem for Cloud and Edge services) is addressing the certification of the services inside the Marketplace according to EUCS



PETs and Trust Anchor Framework related technologies

- For data spaces **PETs-Privacy Enabling Technologies** (secure multi-party computation, homomorphic encryption, differential privacy, federated learning…) are extremely relevant for managing data privacy
- Data spaces need a **Trust Anchor Framework** and associated **Decentralized Identity and Access Management Framework** for trusted operations among participants (based on Verifiable Credentials and SSI)

Legal Compliance (Cybersecurity Act and GDPR)

- Application of **proactive accountability**
- Privacy and data protection **by design**
- **Personal data protection** issues in a data space

EUROPEAN BIG DATA VALUE FORUM

Thank you!

Jesus Santamaria, TECNALIA, jesusm.santamaria@tecnalia.com
ECSO, European Cyber Security Organisation

ORGANISED BY
BDV BIG DATA VALUE ASSOCIATION

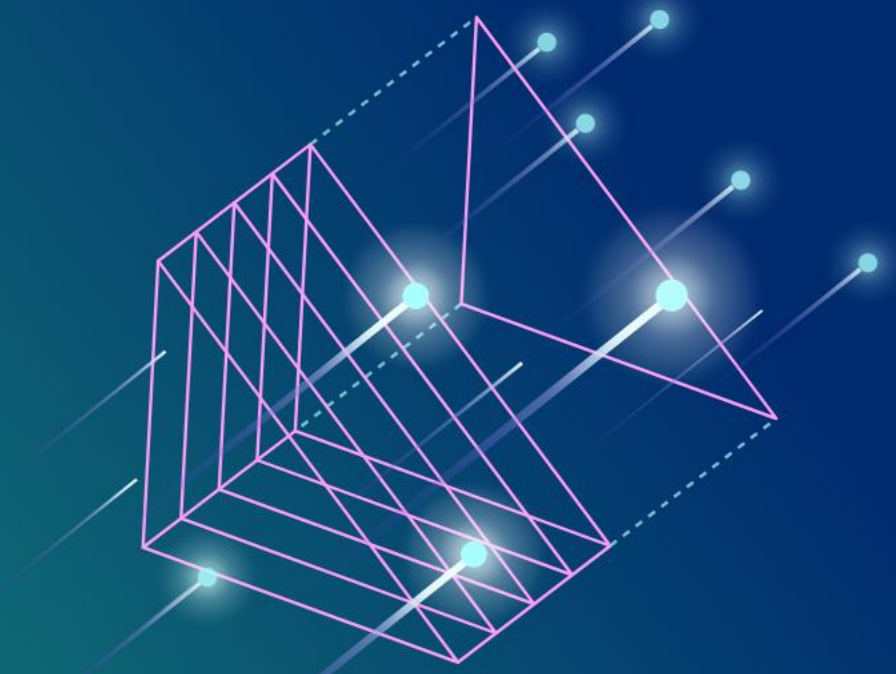
IN COLLABORATION WITH
ITI INVESTIGATE TO INNOVATE
European Commission
INCLIVA | VLC Biomedical Research Institute
POLITÉCNICA
UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF
EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

EUROPEAN BIG DATA VALUE FORUM

Data spaces

Data Spaces and Cybersecurity



Ricard Martínez

26/10/2023, 9,00

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

EUROPEAN BIG DATA VALUE FORUM

This document analyses, from a data protection perspective, a technological model for the efficient implementation of the 'internal data market' called Data Spaces, as it involves the processing of personal data.

aepd agencia española protección datos

APPROACH TO DATA SPACES FROM GDPR PERSPECTIVE

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

SECURE PROCESSING ENVIRONMENT

- the physical or virtual environment and organisational means to ensure compliance with Union law, such as, for example, the GDPR, in particular with regard to data subjects' rights, intellectual property rights and commercial and statistical confidentiality, integrity and accessibility, as well as to ensure compliance with applicable national law and to allow for the operator of the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data, as well as the calculation of derivative data through computational algorithms.

EHDS REQUIREMENTS

- The health data access bodies shall provide access to electronic health data only through a secure processing environment, with technical and organisational measures and security and interoperability requirements. In particular, they shall take the following security measures:
- (a) restrict access to the secure processing environment to authorised persons listed in the respective data permit;
- (b) minimise the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technological means;
- (c) limit the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals;
- (d) ensure that data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only;
- (e) keep identifiable logs of access to the secure processing environment for the period of time necessary to verify and audit all processing operations in that environment;
- (f) ensure compliance and monitor the security measures referred to in this Article to mitigate potential security threats.

CATEGORIES OF DATA SPACE INTERVENERS FROM A GDPR PERSPECTIVE

- 1. Data subjects
- 2. Data holder
- 3. Data user
- 4. Data Space Mediators
- 5. Technical and legal enablers
- 6. Supervisor of access requests
- 7. Others, such as supervisory authorities

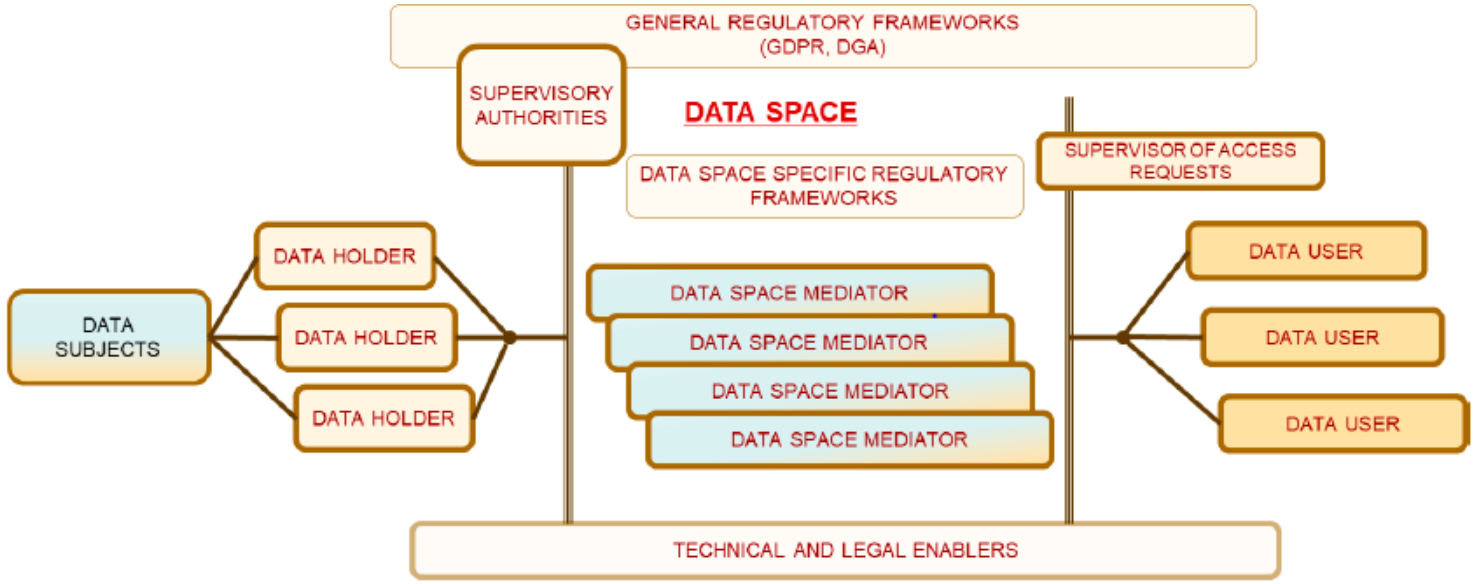


Figure 1: Diagram of interveners relationships from a GDPR perspective

POSSIBLE CONFIGURATIONS OF A DATA SPACE

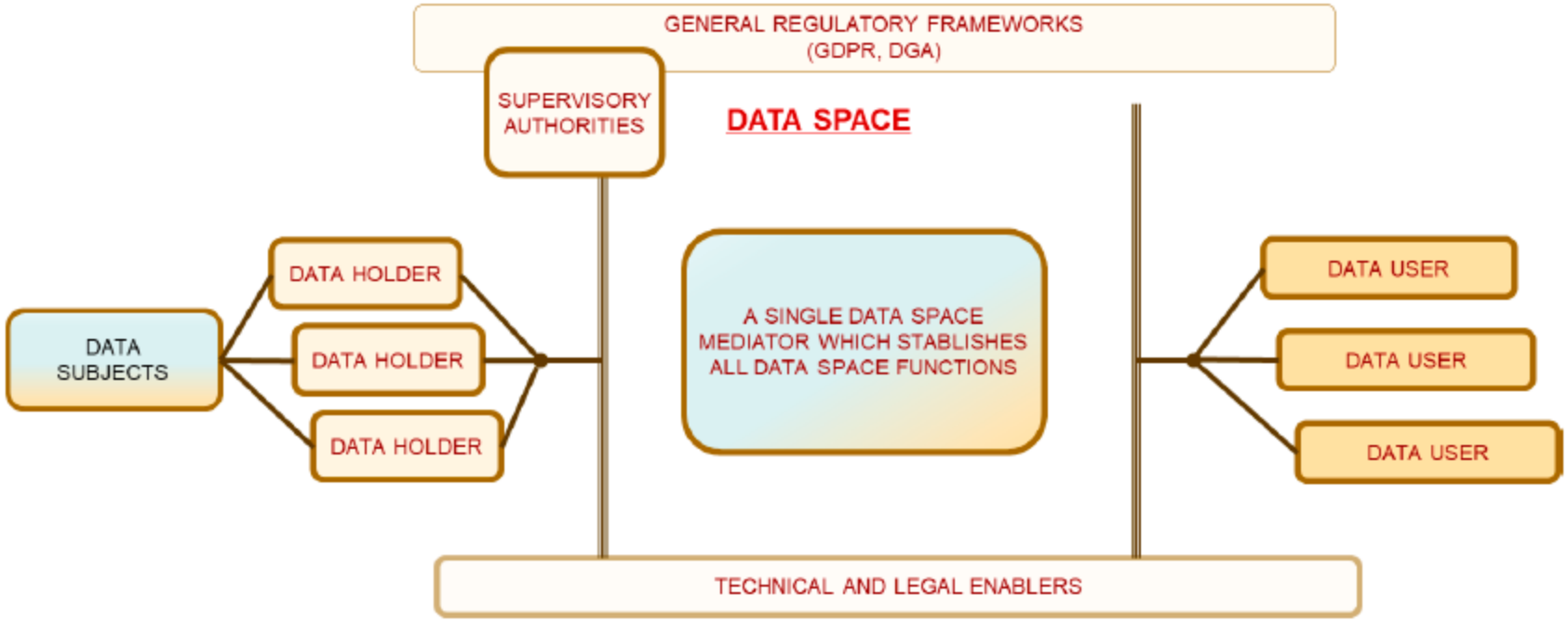


Figure 3: Configuration of a Data Space based on sharing via a central node

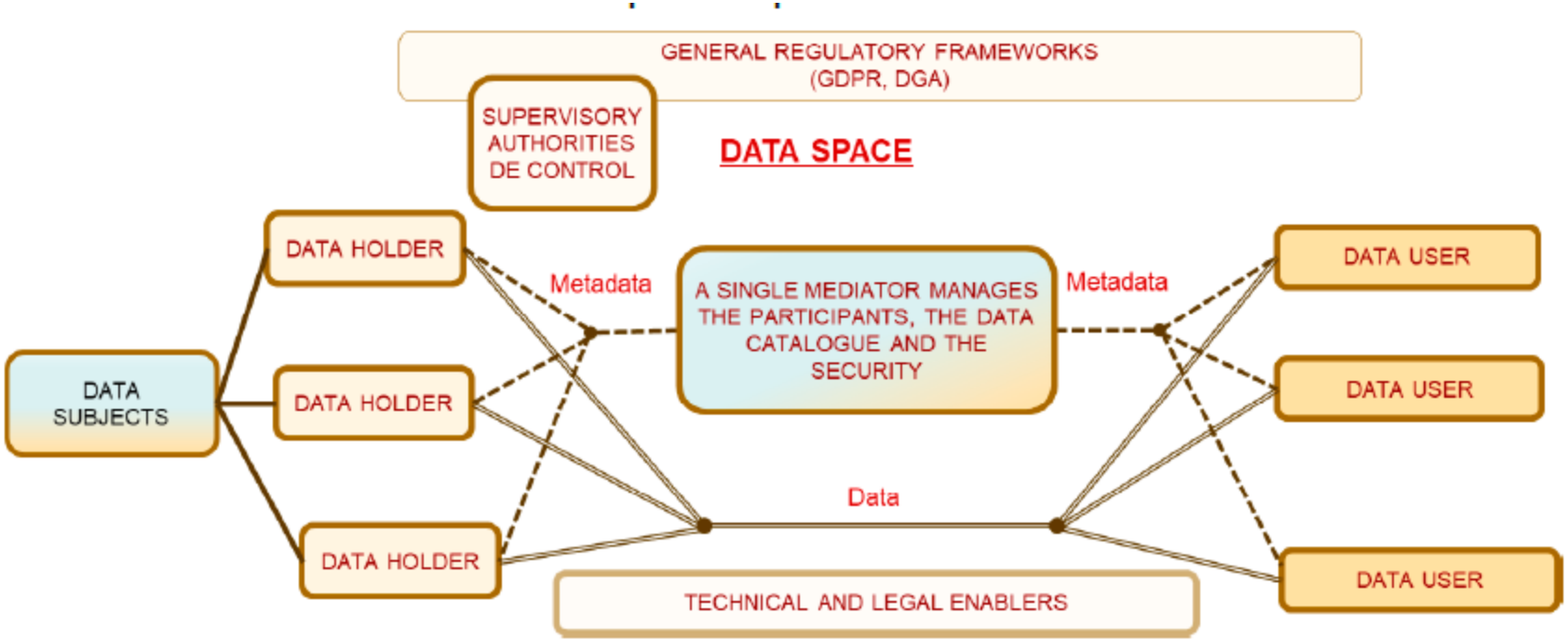


Figure 4: Configuration on the basis of a Data Space Mediator as a central hub or data marketplace

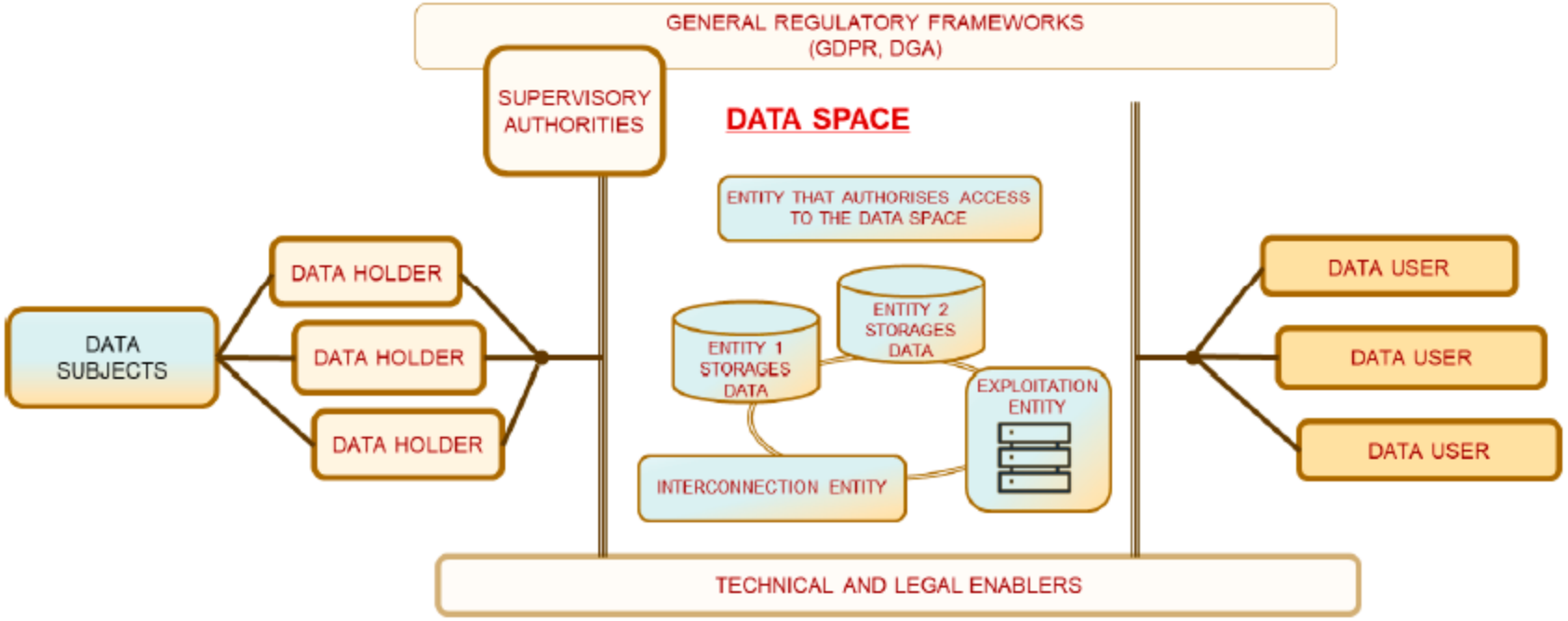


Figure 5: Complex configuration in the definition of interveners in a Data Space

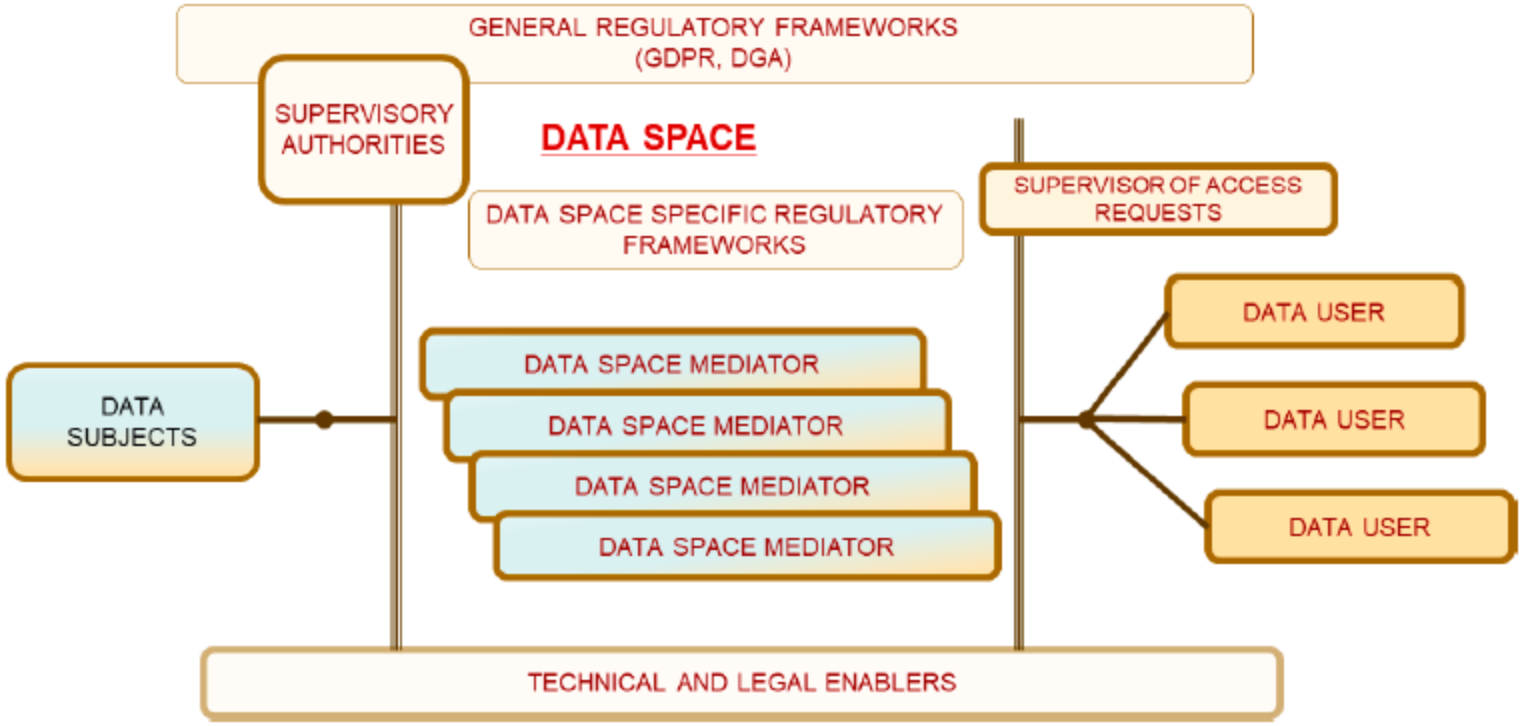


Figure 6: Complex configuration in the definition of interveners in a Data Space

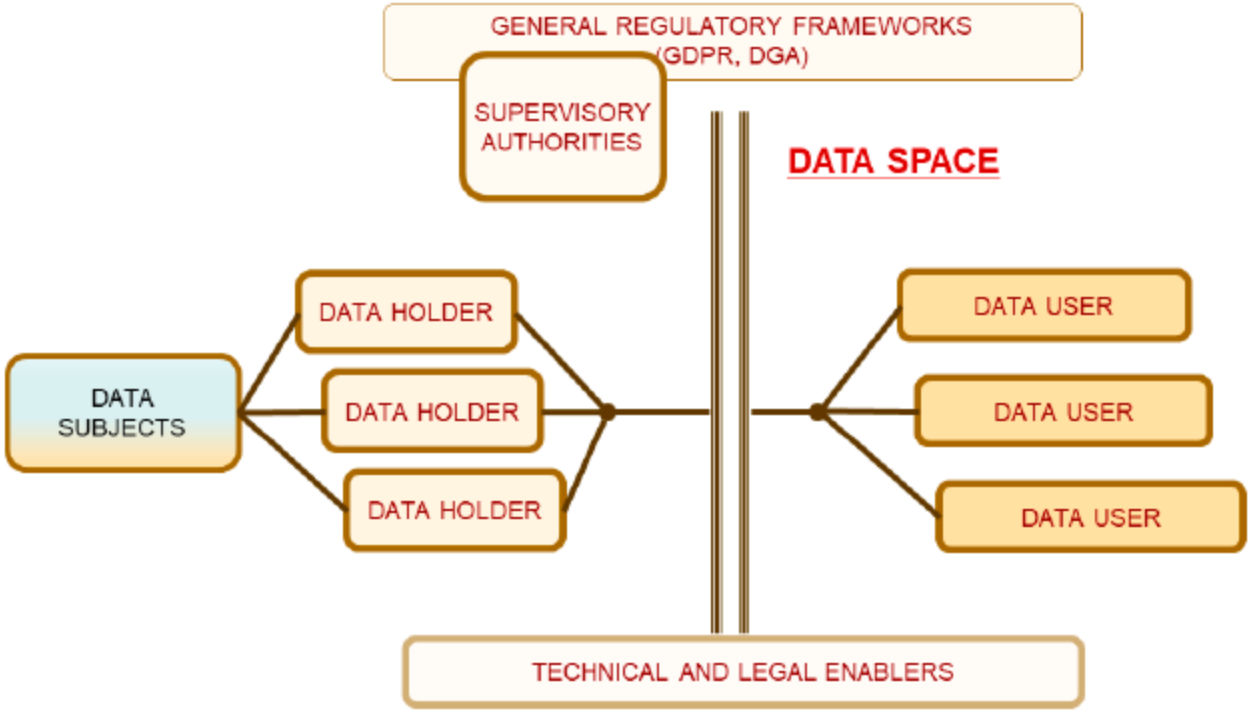


Figure 7: Data Space configuration without the use of data mediaton services

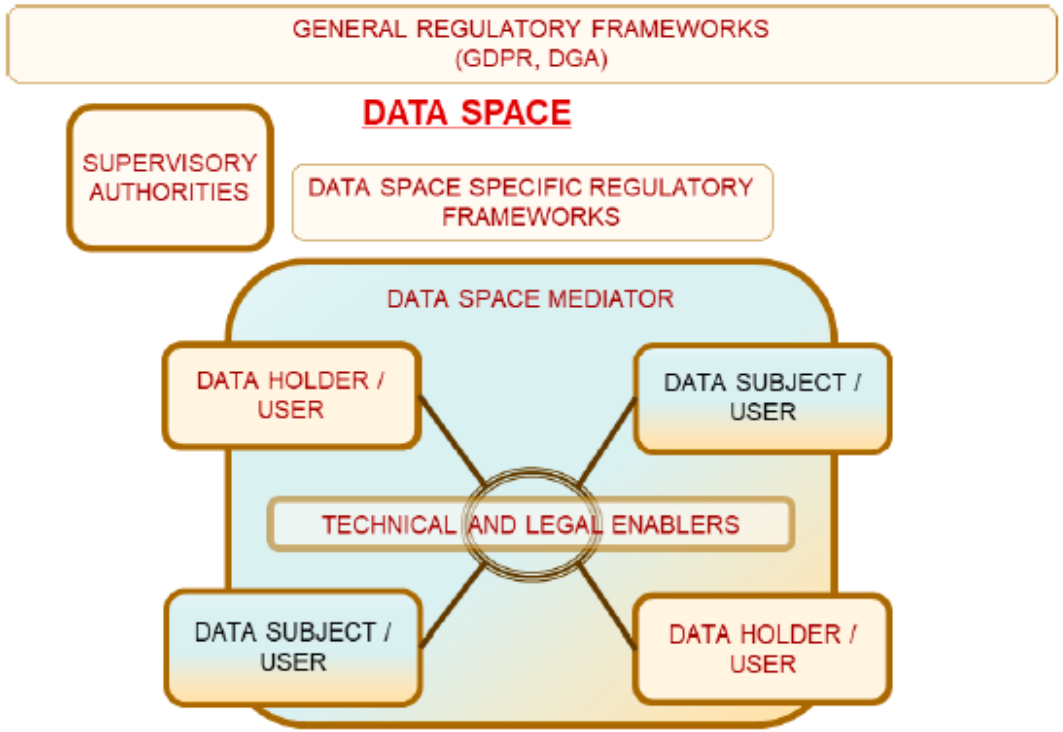


Figure 8: Configuration of a Data Space with data access agreements between Data Subjects and Data Holders

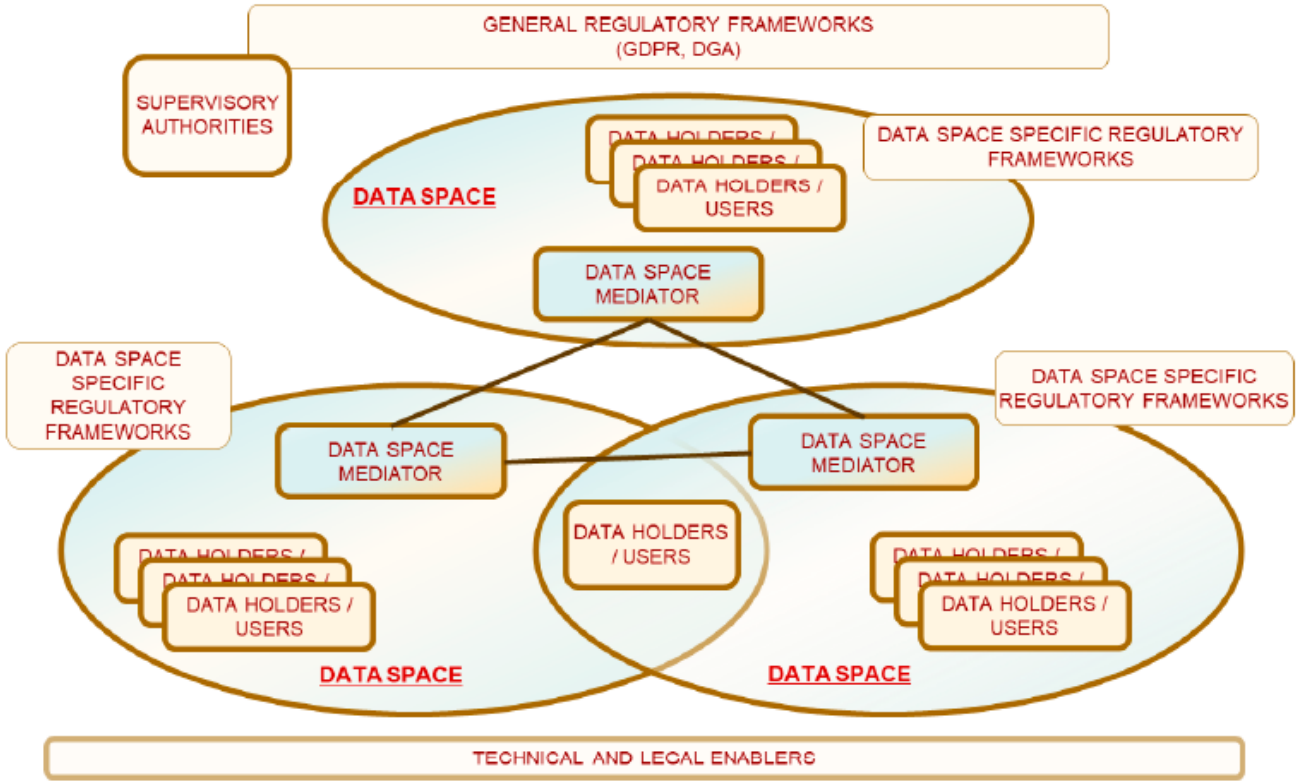


Figure 9: Federation of Data Spaces

USES CASES AND ARCHITECTURES FOR PRIVACY RESPONSE: non personal data

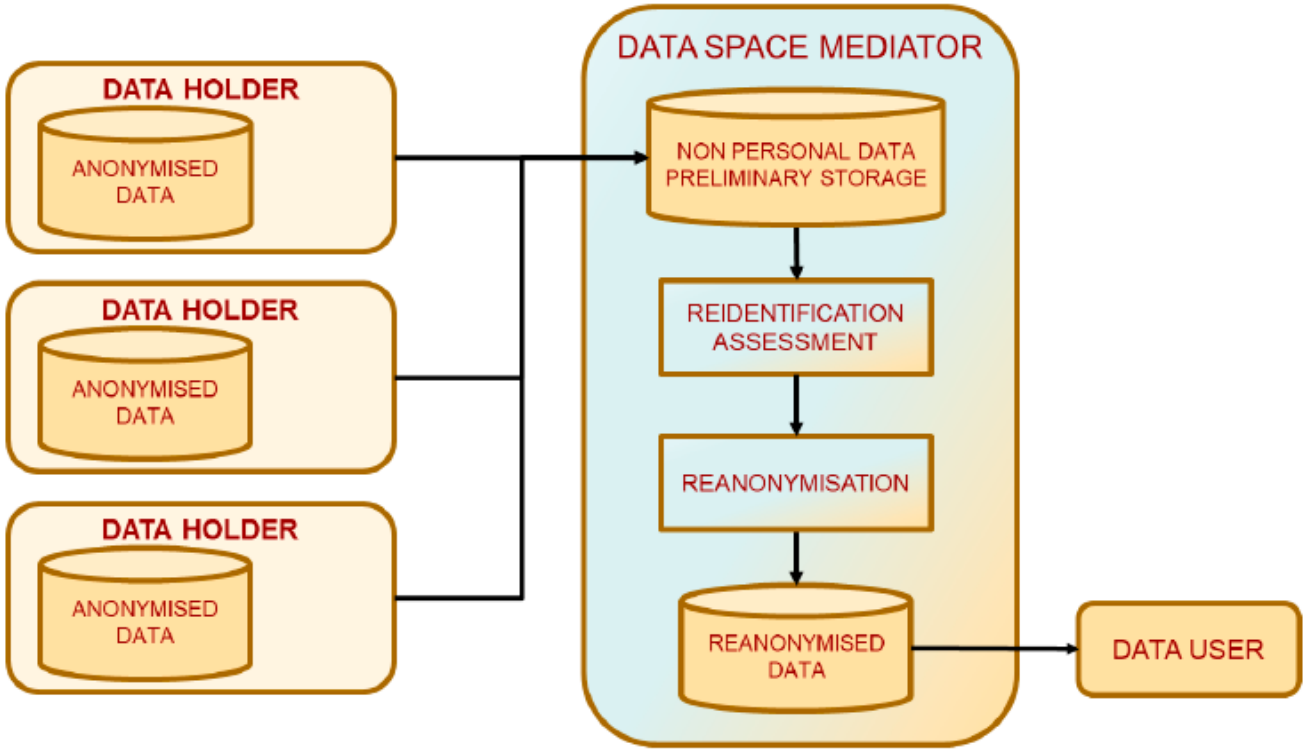


Figure 14: Diagram of the architecture for the use case for the consolidation of non-personal data from different Data Holders

USES CASES AND ARCHITECTURES FOR PRIVACY RESPONSE: anonymisation

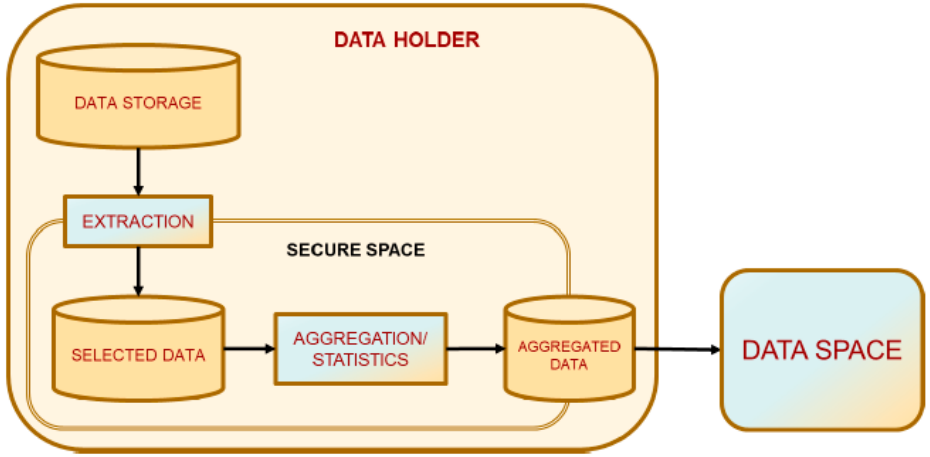


Figure 18: Diagram of the architecture for the use case of anonymised data without linkage between the data from different Data Holders

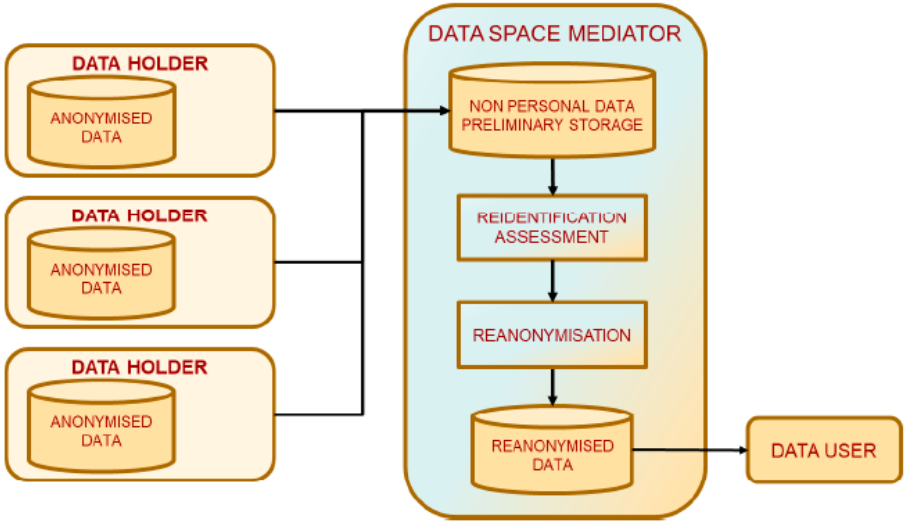


Figure 19: Diagram of the architecture for the use case for the consolidation of anonymised data from different Data Holders

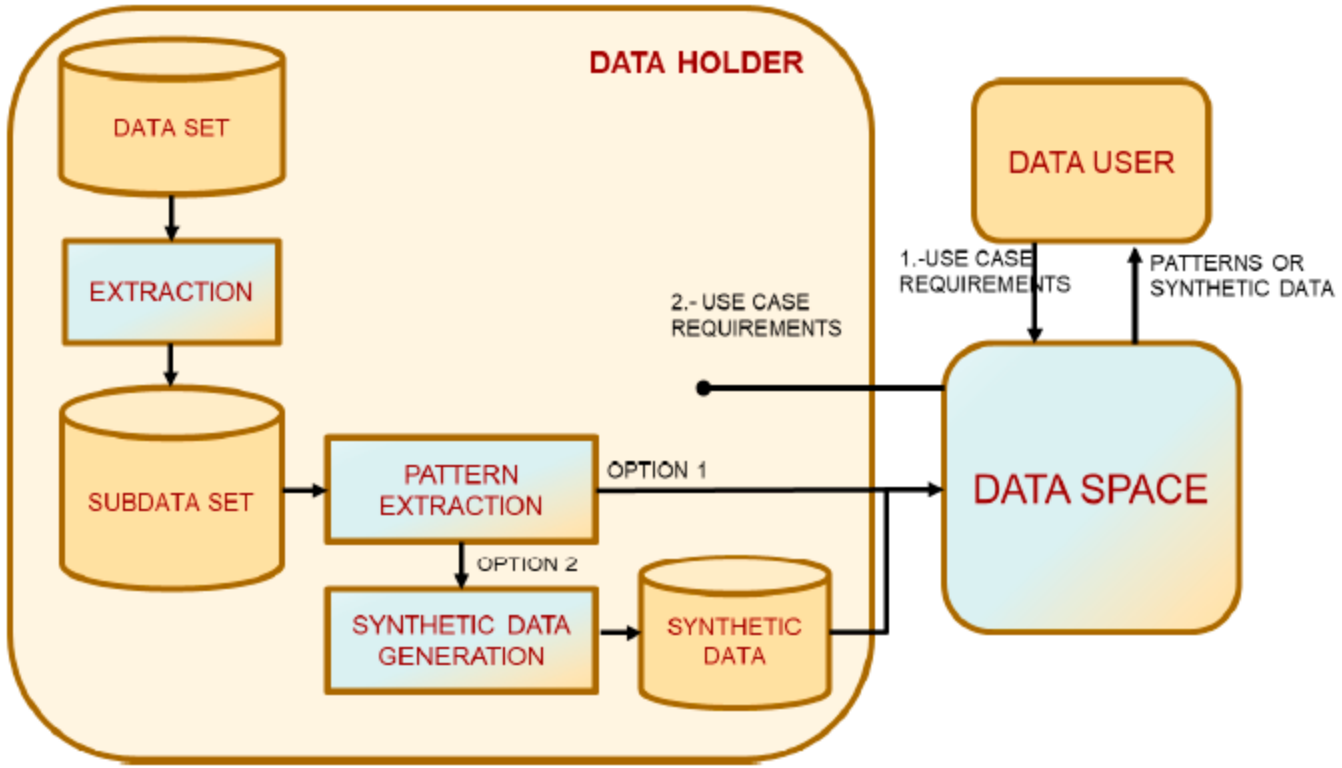


Figure 20: Diagram of the architecture for the synthetic data provision use case

- Secure Multiparty Computing
- Differential privacy
- Homomorphic encryption

USES CASES AND ARCHITECTURES FOR PRIVACY RESPONSE: pseudonymisation

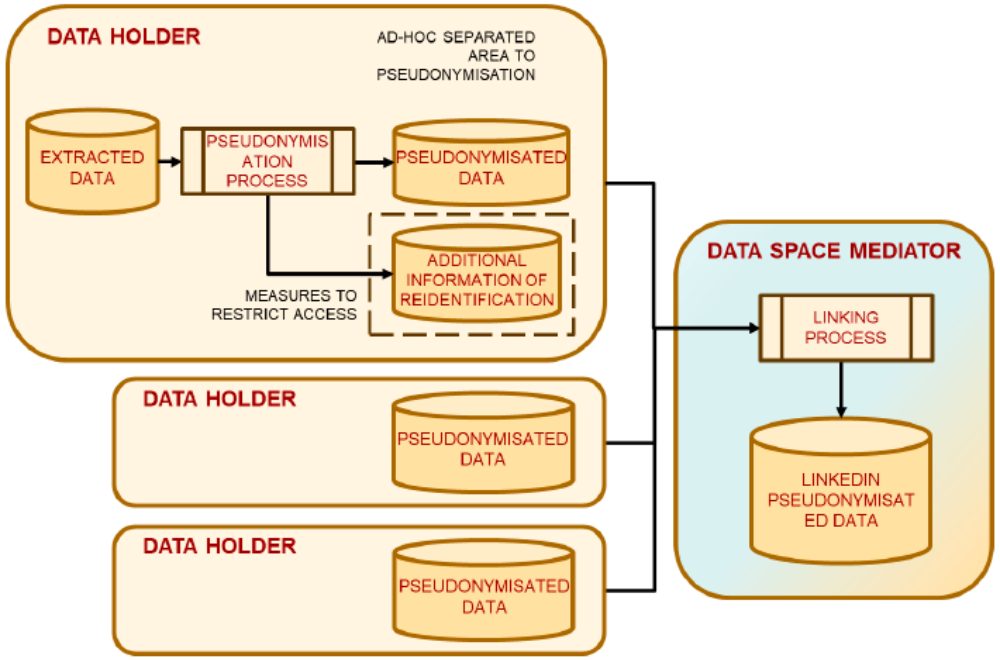


Figure 21: Diagram of the architecture for the pseudonymisation use case

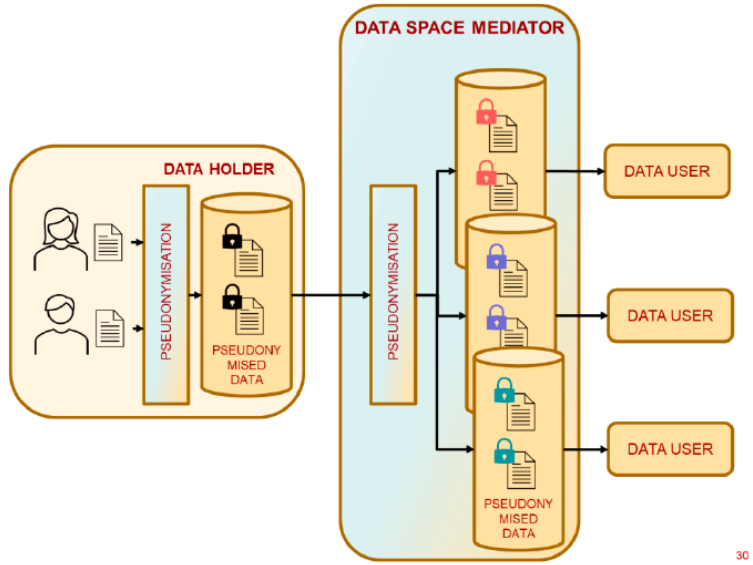


Figure 22: Diagram of the architecture for pseudonymisation of the same data set for different Data Users

Processing where it is not possible to anonymise data

- 1. Transfer the desired processing by the Data User to the Data Holders (e.g., using federated learning techniques).
- 2. Transfer or communicate personal data to the Data Space, to a Mediator, and move the processing to a Secure Processing Environment provided by the Mediator (applying where appropriate pseudonymisation or anonymisation in the Data Space or other strategies).
- 3. Transfer or communicate personal data to the Data Space and from the Data Space to the Data User.

RISK MANAGEMENT AND DATA PROTECTION IMPACT ASSESSMENT

- Risk Based Approach
- Risks for fundamental rights
- Security measures: resilience
  - Inventory of processing activities
  - Availability
  - Personal data breach scenarios
  - Anonymisation/Reidentification
  - Traceability
  - Review and update of measures
- Risk management in the selection of processors/sub-processors
- Data subject rights: consent, transparency, retention period and limitation of processing
- International data transfers

Governance: data protection policy for processing in the framework

- 1. The involvement of DPOs and data protection advisors in the design of Data Spaces and the processing operations with them.
- 2. The procedures for authorising the processing of personal data in the Data Space.
- 3. The precise definition of the purposes of the processing.
- 4. The establishment of the legal bases for processing.
- 5. The determination of controller/processor/sub-processor roles for each of the interveners.
- 6. Risk management for the risks and freedoms of data subjects, including, where appropriate, a DPIA, coordinated between the interveners in the processing.
- (…)
- 32. Implementing activity logs and conducting audits on them to ensure accountability.
- 33. The creation of an iterative process to ensure compliance with the GDPR based on the principle of proactive accountability.
- 34. Having an entity in charge of the supervision of the Data Space, at least from the perspective of compliance with data protection regulations.

EUROPEAN BIG DATA VALUE FORUM

Thank you!

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

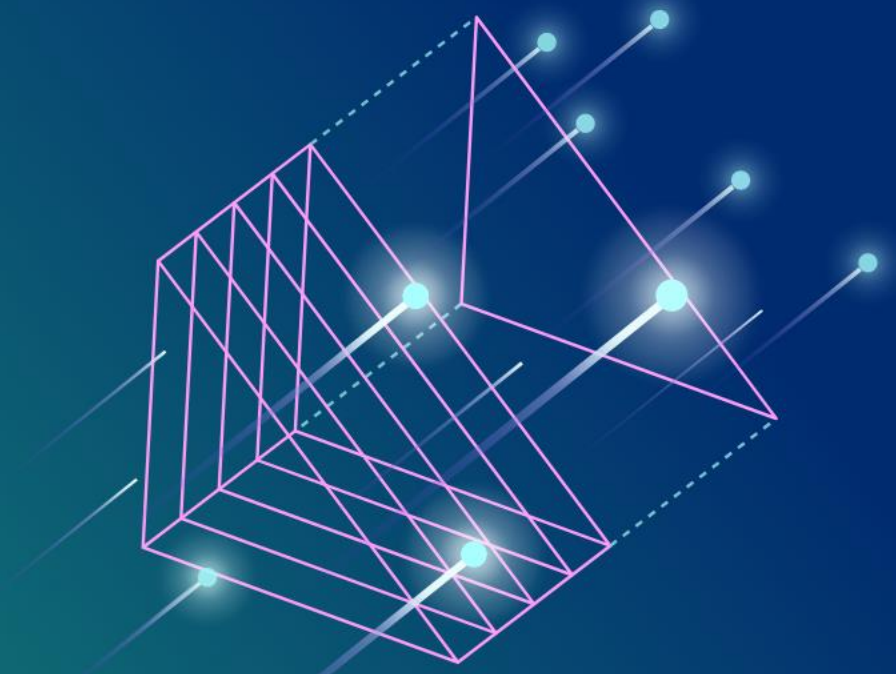
EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

EUROPEAN BIG DATA VALUE FORUM

BDV BIG DATA VALUE ASSOCIATION

Data Spaces & Cybersecurity

Data Spaces and PETs



Freek Bomhof

Oct 27th, 09:00

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

Motivation

Data spaces are at the core of the European Data Strategy
They will be federated across domains, countries and organizations

Societal concerns around all this data sharing
Data processing needs to comply with GDPR
Modern PETs are available now

- Data spaces architectures do not include modern PETs
- Modern PETs are not interoperable or standardized

Background

- Started as a TNO / CoE-DSC initiative early 2023
- TF Data protection & TF Data Spaces
- Proposed as BDVA whitepaper
- Session at Data Week 2023 (Lulea)
- Editorial team (18)
- Sneak preview EBDVF 2023 (Valencia)

Editorial team

- Abishek Raju (TNO)
- Aitor Corchero (NTT Data)
- Antonio Kung (Trialog)
- Daniël Worm (TNO)
- Elena Lazovik (TNO)
- Enric Staromiejski (NTT Data)
- Evangelos Markatos (Forth)
- Freek Bomhof (TNO)
- Harrie Bastiaansen (TNO)
- Jose M. del Alamo (UPM)
- Lucas Sanjuan Viñas (ITI)
- Monica Florea (SIMAVI)
- Patricia Jimenez (NTT Data)
- Rizkallah Touma (i2CAT Foundation)
- Roberto di Benardo (ENG)
- Venkatesh Kannan (Ichec)
- Vincenzo Savarino (ENG)
- Zoltan Mann (UvA)

Different worlds (1): Data ownership

Data spaces people

- Practical concept
- Describes the party that holds the data and that can manage access to the data

PET people

- Meaningless concept
- Data cannot be owned like a physical asset

Different worlds (2): Trust

Data spaces people

- Trust is a good thing
- Establishing and maintaining trust is a key activity

PET people

- Trust is a bad thing
- When your technology is good, you don’t need to revert to trust

Conclusions

- PETs contribute to enforcing policies, creating trust and sovereignty
- Interoperability in data sharing means interoperability in processes
- PETs are very specific; automated deployment is a challenge
- Standardization and formalization of data sharing processes is needed

Draft recommendations

Methodological & design

- Taxonomy
- Scenarios
- Templates of usage policies
- Definitions of roles

Organizational & policy

- Community on privacy patterns
- Certification

Technological & implementation

- PET marketplace
- PET compiler
- PET interoperability
- Definition of MVPs

EUROPEAN BIG DATA VALUE FORUM

Comments or questions:

freek.Bomhof@tno.nl

ORGANISED BY
BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH
ITI INVESTIGATE TO INNOVATE
European Commission
INCLIVA | VLC Biomedical Research Institute
POLITÉCNICA
UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF
EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION

EUROPEAN BIG DATA VALUE FORUM

Thank you!

ORGANISED BY

BDV BIG DATA VALUE ASSOCIATION

IN COLLABORATION WITH

ITI INVESTIGATE TO INNOVATE

European Commission

INCLIVA | VLC Biomedical Research Institute

POLITÉCNICA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNDER THE AUSPICES OF

EU23 SPANISH PRESIDENCY COUNCIL OF THE EUROPEAN UNION