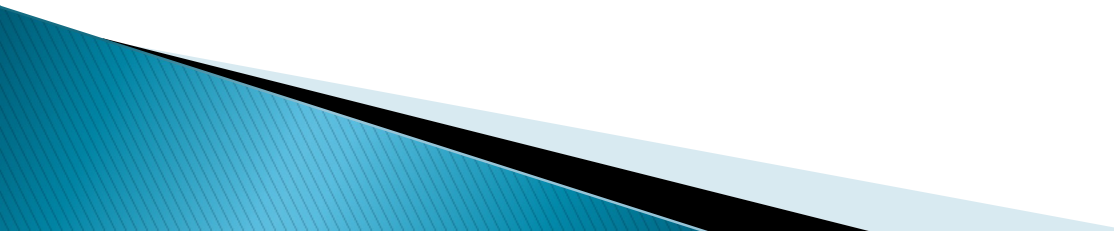
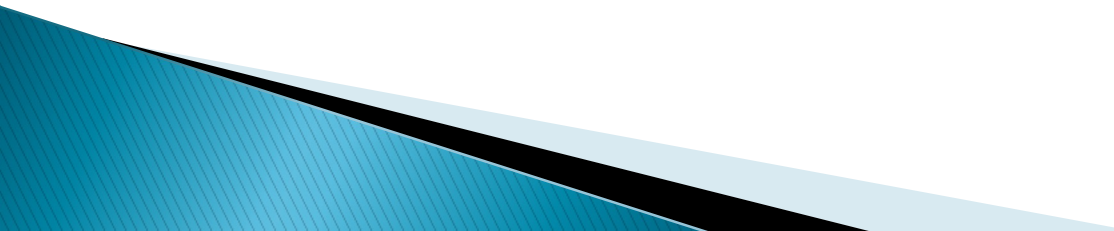


Harmonising Open–Science Principles with Data Sovereignty and the Mitigation of Ecological and Security Threats

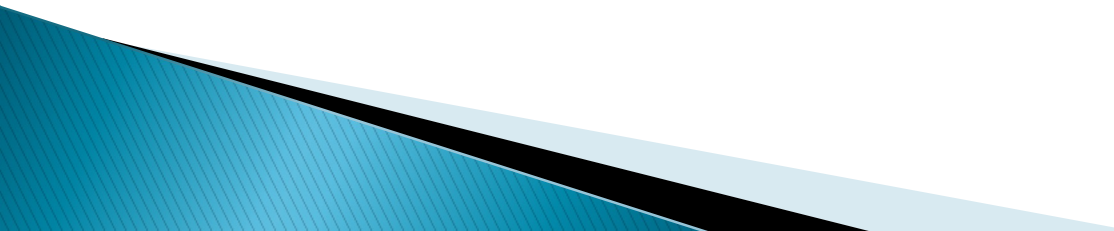
Stavroula Tsinorema
University of Crete

ENVRI–Hub NEXT webinar: Ethical Challenges in
Data Reuse, Aggregation and Sustainable Storage
Thursday, 3rd September, 2026

- ▶ **Open science**: accessibility, knowledge– and data–sharing, reproducibility.
 - ▶ **Data sovereignty**: control over data, subjects' rights, legal restrictions over storage & processing, **responsible stewardship**.
- 

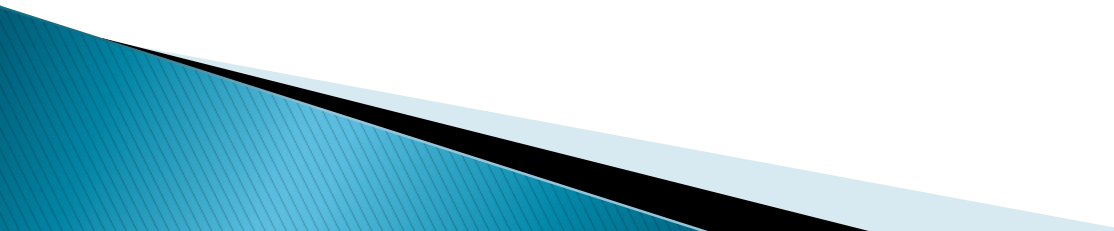
- ▶ **Security threats:** misuse, privacy violations, cybersecurity issues, strategic vulnerabilities.
 - ▶ **Ecological sustainability risks:** Environmental costs of data infrastructures, research systems, AI.
- 

Competing normative claims?

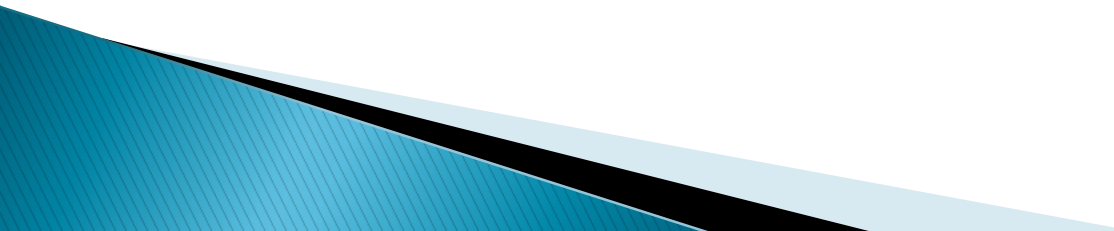
- ▶ **Openness vs. sovereignty?** Here approached not as a technical data management issue, but primarily as a conceptual and normative one.
 - ▶ Openness a core scientific value related to the guiding principle of freedom of research (pursuing knowledge as a scientific and social/ public good).
 - ▶ However, openness *as a scientific value* differs from unconstrained accessibility as a *policy standard*.
- 

A central tension?

► Open science:

- accessibility of research outcomes and data
 - transparency
 - reproducibility and verification
 - collaboration and knowledge exchange
 - reuse of data and scientific infrastructures
- 

Data sovereignty

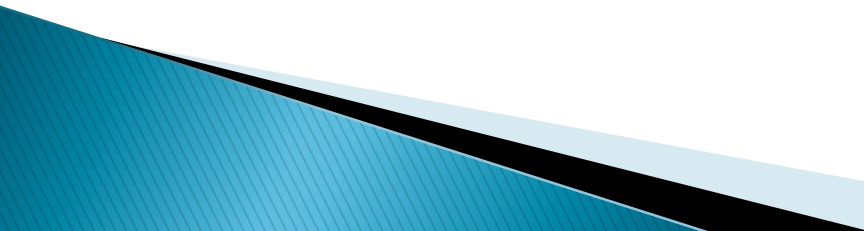
- legitimate control over data,
 - the rights and interests of data subjects, communities and institutions,
 - jurisdictional power over data storage and processing,
 - protection against exploitation or unauthorised secondary use,
 - security and accountability,
 - in special contexts, national or collective control over strategically important datasets.
- 

- ▶ How much openness is ethically justified, for which types of data, accessible to whom, for what purposes, and under whose authority?

i. What is “openness”?

- ▶ Neither unbounded nor unconditional.
- ▶ Diverse domains:
 - open publications
 - open metadata
 - open methods
 - open software
 - open research data
 - unrestricted reuse of data
- ▶ Diverse ethical challenges. Differentiated openness, requiring *distinct justification* (but also avoiding ethically illegitimate secrecy).

FAIR data principles

- ▶ Findable, Accessible, Interoperable, Reusable (focusing on technical usability of data).
Scientific data, data services, workflows– and the knowledge they represent – remain accessible, verifiable and secure.
 - ▶ Ensuring that (European) science remains **open, innovative, and resilient** in the face of the evolving global challenges.
 - ▶ Risks and challenges. Global research dependencies, geopolitical challenges.
- 

European Open Science Cloud (EOSC) Steering Board Opinion

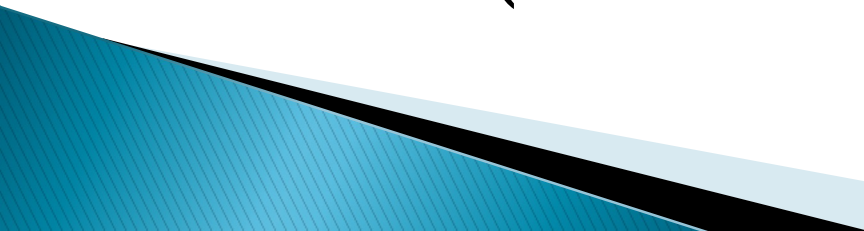
- ▶ Scientific data and data services remain permanently accessible, verifiable, and secure, by reinforcing the EOSC Federation, *aligning national and EU initiatives*, and embedding legal and operational clarity.
- ▶ Objectives. European sovereignty in research data requires the ability to maintain **open, fair, and trustworthy scientific collaboration**, grounded in resilience, interoperability, and *shared values*.

Principles for European Data Sovereignty

- ▶ Openness with responsibility
- ▶ (Local) Autonomy (of substructures) through federation
- ▶ Control of data and workflow quality
- ▶ Portability and interoperability
- ▶ Accountability and trust
- ▶ Resilience and preparedness

Data sovereignty by design

(EOSC Steering Board expert group)

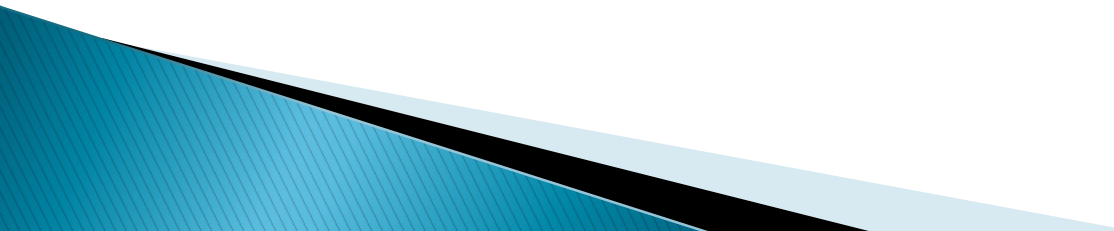


Human research data. The challenge of informed consent

- ▶ Future use. Data may be subsequently:
 - shared
 - linked to other datasets
 - processed via AI
 - reused for purposes not known at procurement time
 - subjected to automated inferences.

How **meaningful** are individual informed consent procedures in big data ecosystems?
Reconsidering informed consent in future scientific data use.

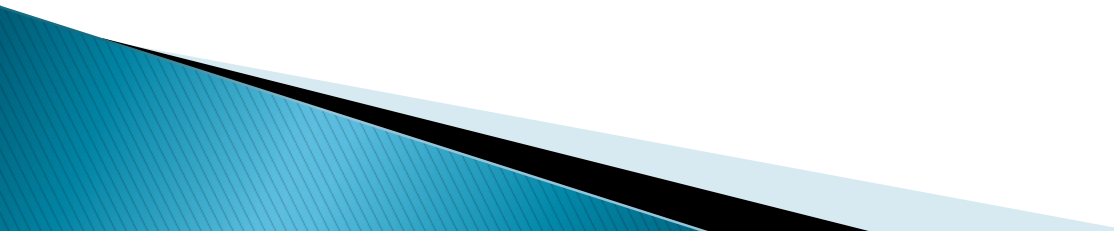
The re-identification challenge

- ▶ Anonymisation– deanonymisation challenge.
 - ▶ Datasets combined, information identifying:
The more interoperable and reusable datasets become (Open Science), the greater the possibility that *prima facie* non-identifying data acquire identifying force through linkage.
 - ▶ The anonymous/ eponymous polarity in data processing and storage needs reconsideration in complex, connected data environments.
- 

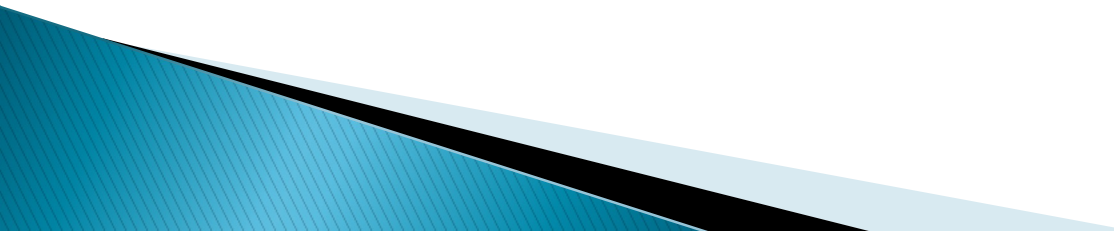
Types of data sovereignty

- ▶ Individual
- ▶ Institutional
- ▶ Community
- ▶ Jurisdictional

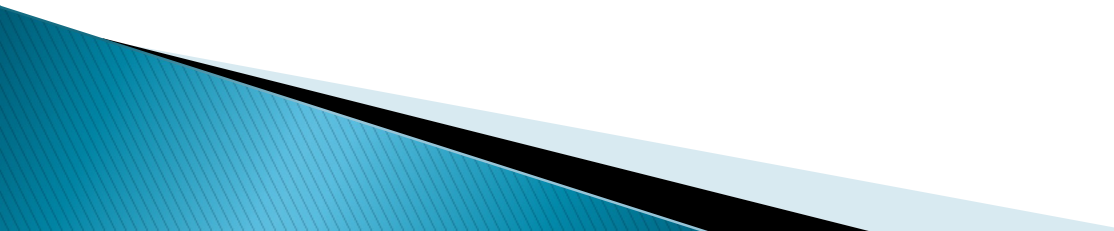
The question of “*ownership*” a misguided one.



Sovereignty means:

- ▶ Who has legitimate authority over the data?
 - ▶ Who should have access to them?
 - ▶ Who should determine secondary uses?
 - ▶ Who bears responsibility?
- 

Ecological aporias

- ▶ On the one hand, open science contributes to sustainability, as sharing data avoids duplication of research.
 - ▶ On the other hand, energy consuming massive infrastructures:
 - data centres
 - cloud computing
 - repositories
 - high-performance computing (HPC)
 - AI systems use
 - storage redundancy
 - continuous data preservation.
- 

Meeting the ecological paradox?

- ▶ Need for harmonising goals:

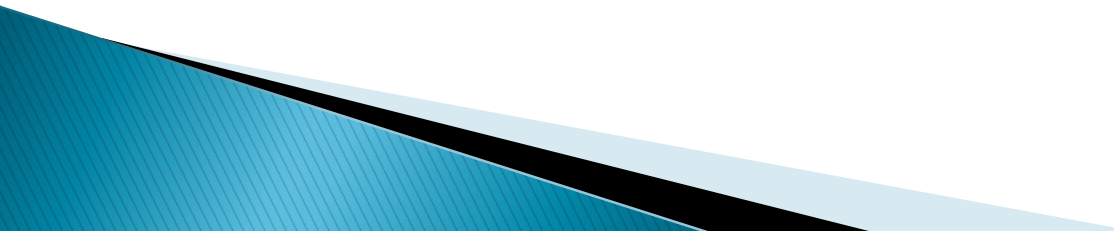
Sustainable openness

Scientific data should be preserved and shared to the extent that the expected scientific and societal value justifies the ethical, security and environmental costs involved.

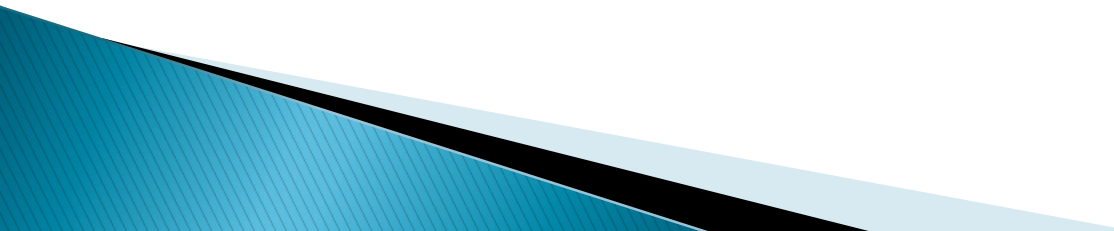
Security tensions

- ▶ **Open science's “Janus face”**. Beneficial but also research security vulnerabilities.
 - malicious/harmful use of scientific information
 - cyberattacks
 - exploitation of vulnerabilities
 - Illegitimate dual-use applications
 - exposure of critical infrastructure
 - misuse of advanced technologies
 -

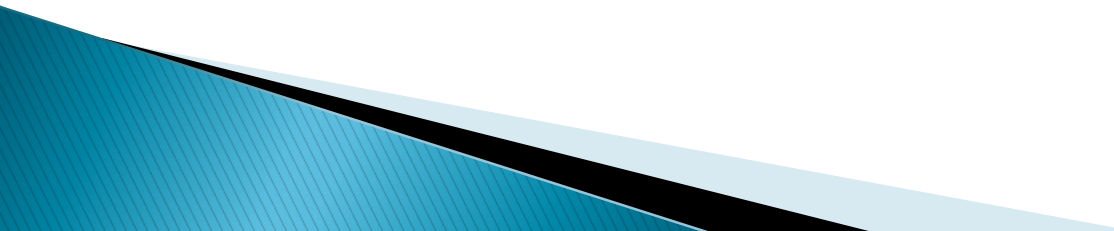
II. Environmental data. The case of ENVRI-Hub Next

- ▶ A secure integrated gateway for sharing environmental data, **structured federated system**.
 - ▶ Addressing Open Science via robust data management policies, legal requirements, and also common, shared ethical guidelines, training personnel, sharing good practices, continuous assessment of socio-ethical impacts of shared data...
- 

Challenges

- ▶ Decentralised data architectures create complex ethical and legal challenges.
 - ▶ Digital equity. Digital divide, resource disparities, geopolitical vulnerabilities, data piracy, data integrity, misuse, accuracy of automated policy decisions...
 - ▶ Ethics assessment tools and guidelines should be continuously discussed and *co-evolve* with scientific developments in environmental and data sciences.
- 

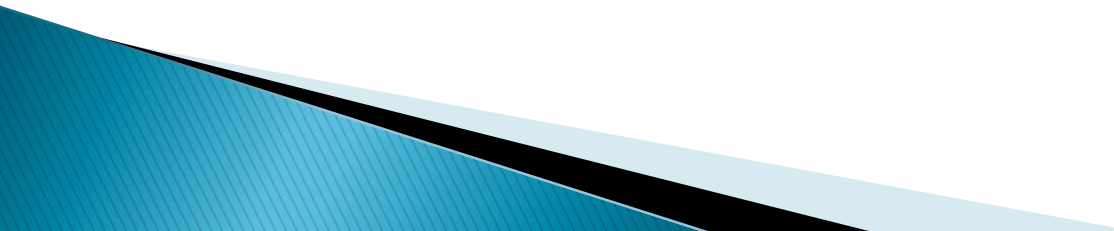
III. Mitigation strategies

- ▶ Data Governance frameworks.
 - Responsible and sustainable open access: Sharing knowledge with protection of vulnerable ecosystems, species, communities, individuals.
 - **CARE** principles (addressing human and social concerns).
- 

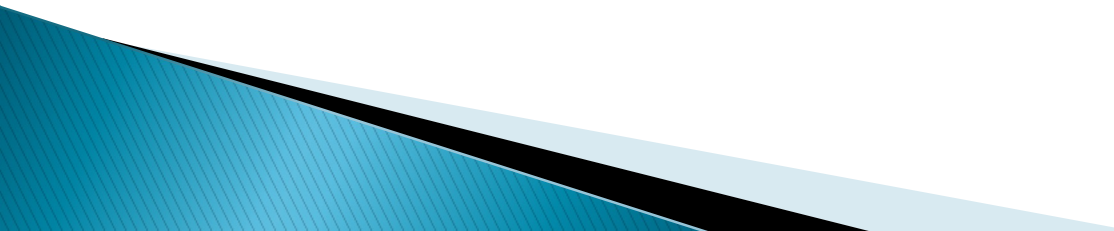
CARE principles

- ▶ **Collective Benefit:** Data ecosystems must design processes that provide tangible benefits, prioritising local communities.
- ▶ **Authority to Control:** local populations and communities retain the right to determine how their data are used.
- ▶ **Responsibility:** Researchers must actively demonstrate how their projects support regional ecosystems and livelihoods.
- ▶ **[Further] Ethical requirements:** The rights of individuals, the self-determination and well-being of communities take precedence at all stages of data usage.
- ▶ Tiered and embargoed data access (geospatial masking, credentialed access, data embargoes...)

IV. Governance framework

- ▶ Open Science objectives require **risk-sensitive governance**.
 - ▶ Openness has rigorous, ethically structured boundaries, ethically sensitive decision-making architectures and graduated access.
 - ▶ *“As open as possible, as restricted as ethically required and as sustainable as reasonably possible”*.
- 

Graduated access

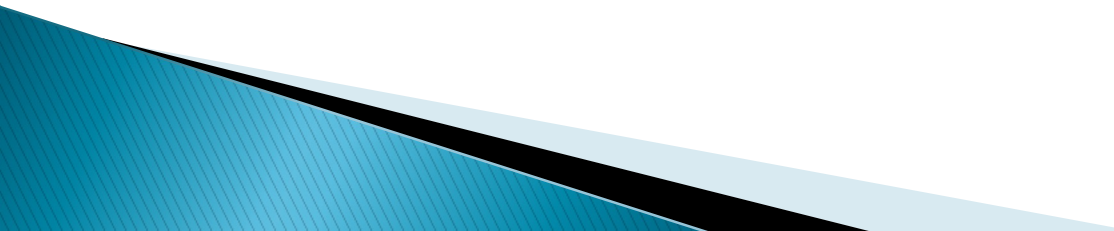
- ▶ Fully open (eg. publications, metadata)
 - ▶ Conditional openness (non-sensitive data sets)
 - ▶ Controlled access (eg. human/health data)
 - ▶ Restricted access (high-risk data)
 - ▶ Non-disclosable data (if disclosed, serious, unacceptable harm is generated)
- 

The guiding ethical principles

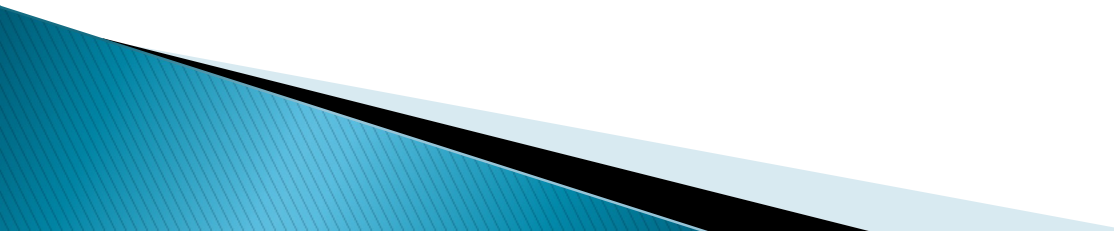
- ▶ Scientific openness is constrained by:
 - respect for personal autonomy, privacy,
 - the no harm principle, non-maleficence, harm minimisation & prevention security,
 - justice & equity
 - solidarity, public good, collective care
 - environmental sustainability.

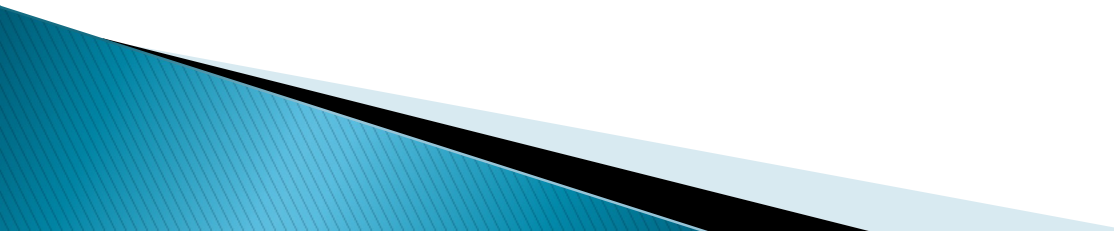
AND – the principles of **scientific integrity** (cf. ALLEA Code).

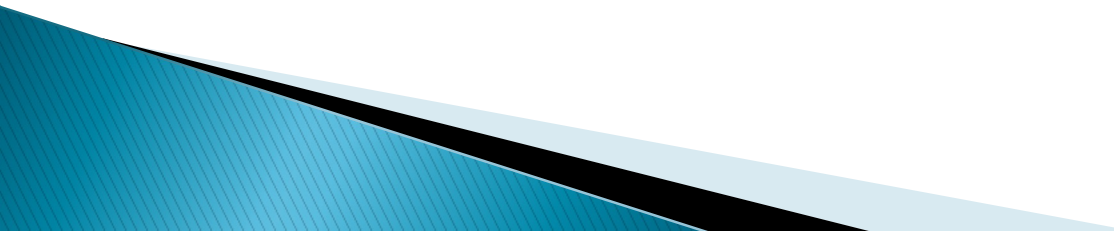
In a nutshell,

- ▶ Data sovereignty, security and ecological sustainability are not external constraints, “added-on” Open Science, but core components, “built-in” its normative structure, guaranteeing its **ethical legitimacy, institutional trustworthiness and social acceptability.**
- 

Pathways

- ▶ Engaging research communities in the active monitoring, improvement and curation of data accessibility.
 - ▶ Identifying trustworthy FAIR datasets for AI training.
 - ▶ Safeguarding long-term autonomy in the governance of scientific knowledge.
 - ▶ Public funding must never translate into political control or arbitrary restrictions.
- 

- ▶ ***Investing in infrastructure and skills.*** Investing in secure, interoperable repositories and in capacity building for data management, cybersecurity, and FAIR (and CARE) principles. Creating data management and curation training open services.
 - ▶ ***Implementing accountable governance frameworks.*** Research centres, infrastructures, Universities, should adopt transparent governance models for ethically sensitive data management, ensuring accountability, community oversight and adherence to scientific and ethical standards.
- 

- ▶ Governance frameworks should be shaped through ongoing, situated, sharable practices of (local) autonomy, equitable access and collective care/stewardship.
 - ▶ **Open science is inclusive, equitable and sustainable science.**
- 

Thank you for your attention