Unconference | As open as possible, as restricted as necessary: EOSC sensitive data exchange

Questions posted on Slido

- Thanks so much for making this session available in stream! Very thankful for that :-)!
- Could each of the projects explain how theirs connects to the others - a clear simple picture of which project does / doesn't do what?
- Core difference and interconnect between titan and siesta. Seems pretty similar
- How interconnected and interoperable are these three projects intended to be with each other?
- Who do you want to use your output (beyond project partners) and how do you plan/hope to engage with them/us?
- Assisted/Automated anonymization and re-identifications assessment, can be consistent the not off-the-shelf architecture components. Do you focus on them first?
- Integration with EU dataspaces - are you collaborating with _ALL_ EU DS groups so that science could smoothly get sensitive real life data from every sector?
- With what blockchain infrastructure does TITAN intend to work with? Is there already something in place?
- Thoughts on disclosure control of results? Reproducibility of performed experiments?
- What will a simple user / researcher need to do to access the services you will build?
- Integration with ELIXIR, eg by implementing/joining with LifeScience Login (former ELIXIR AAI)
- Does using DTL for contracts involve the transmission of personal data to the ledger? If so, how are GDPR rights exercised when the record is immutable?
- Crypto Agility: How much work will it be to move to post-quantum cryptography for the frameworks that rely on current public key crypto?
- How do the projects presented interact in terms of strategy / roadmaps with the established HDABs at the national levels, about the provisioning of SPEs/TREs?
- Legal - are you developing a sufficient framework so that data holders feel comfortable to process data on EOSC infra? EU-wide? (regulation) National? Sectoral?
- Would it make sense to describe the challenge in terms of the 4 interop layers (technical, semantic, legal, organisational)? If so, who is addressing what?
- Heidi (ENTRUST) mentioned using RO-Crate for tracking data provenance and access. How will TITAN and SIESTA approach this? With RO-Crate or something else?
- How are you in your project separating different types of "end users"? Like researchers or companies, or citizens?
- In the EOSC-RAISE project we are running both static and dynamic analysers to check security and performance
- Is sbom a technology for software accountability

- But, if there is no out disclousure, there is no data issue at all. Have you identified technologies to assist the data disclousure step? AI-based?