

Quality, Trust, and Sovereignty of Data Task Force

Charter

1 Task Force background and scope

The new Quality, Trust, and Sovereignty of Data Task Force (2027–2028) addresses three closely related concerns — data quality, data sovereignty, and the trustworthiness of research data — that make the Federation reliable for researchers.

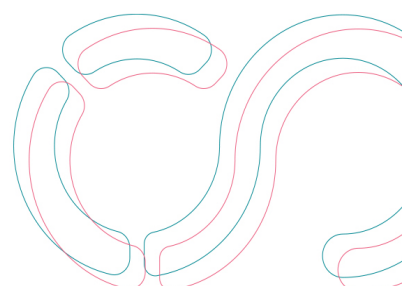
Because sovereignty cannot be effectively governed, validated or enforced without objective requirements, the Task Force (TF) will work to establish practical frameworks through which data quality can be assessed and enforced across the Federation. In addition, the TF will specify requirements for sovereign, compliant and reliable data, and contribute to alignment with the ESFRI–EOSC Task Force with respect to data sovereignty.

In line with the mandate set by the EOSC-A Board of Directors, the TF is expected to deliver, in particular: a recommended requirements document for data sovereignty to determine the compliance of Federation data; a report on data quality dimensions and requirements suitable for the Federation; a report on recommended mechanisms to review the compliance of Federation data against the standards adopted; and a shared understanding of what trust in EOSC means.

The TF is a strategic, time-bound body that works in direct service of the EOSC Federation. Its single annual output is a concise paper that identifies a specific problem, sets out possible solutions, and formulates actionable recommendations addressed to the relevant Federation Working Groups or to the EOSC Nodes more broadly, anchored wherever possible in one or more EOSC use cases, so that recommendations are grounded in real Federation needs.

2 Potential areas of work for the annual deliverable

As a new TF, this body does not build on a predecessor's deliverable. To ground its work, three bodies of existing work in the EOSC and wider European context are especially relevant: on data quality, the EOSC-A report "[Towards a Data Quality Framework for EOSC](#)"; on data sovereignty, the [Gaia-X Trust Framework](#), the European reference for compliance-by-design and sovereign data exchange; and on trust in research infrastructures, the [CoreTrustSeal Trustworthy Data Repositories Requirements](#), the international certification standard for trustworthy repositories. Together with the Board's mandate, these suggest some single-paper-sized problems for the annual deliverable. The TF is invited to select and sharpen at least one of them (or a comparably scoped problem):



a) Data sovereignty requirements and compliance

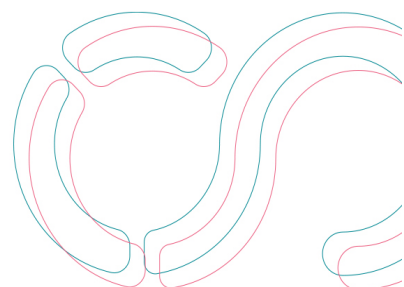
- **Requirements set for data sovereignty.** Drawing on the compliance-by-design approach of frameworks such as Gaia-X and on the European data legislation, a paper could identify the standards and objective requirements against which the sovereignty of Federation data can be defined, so that sovereignty becomes governable, validatable and enforceable rather than aspirational.
- **Mechanisms to review compliance.** A deliverable could recommend practical mechanisms – self-assessment, compliance labels, or peer review – through which Federation data and the infrastructures that hold it can be reviewed against the adopted sovereignty and quality requirements, learning from certification schemes already in use.

b) A data quality framework for the Federation

- **Quality dimensions and requirements for the Federation.** Building on the EOSC data quality framework, a paper could define the data quality dimensions and requirements most relevant to the Federation, expressed in a way that is human- and machine-readable and can be assessed at scale.
- **From dimensions to an assessable quality function.** A deliverable could propose how quality (and sovereignty) requirements are operationalised into an assessable, multi-actor quality function across data providers, Nodes and users – echoing the proof-of-concept quality function proposed by the earlier EOSC work – while remaining realistic about workforce and cost.

c) Trust and data autonomy in the Federation

- **Trustworthiness of research data hosted in infrastructures in a federated setting.** Certification schemes, such as CoreTrustSeal, were designed for individual repositories. A paper could examine what trustworthiness means when repositories operate as Federation Nodes relying on shared or outsourced functions, and how responsibility and evidence of trustworthiness should be displayed and assessed across the Federation.
- **A mutual understanding of trustworthy data.** 'Data trustworthiness' is a widely used term that is interpreted differently depending on the context and the stakeholder. It consists of many components, such as traceability, certification, sovereignty, accessibility, etc. The complexity of this concept increases when data is shared across European repositories, domains and disciplines, as is the case with the EOSC Federation. Within the scope of the TF, a deliverable could clarify the factors that make data trustworthy within the EOSC Federation. The proposed recommendations should be tested against two or three use cases to demonstrate



that the concept of data trustworthiness is feasible for the Nodes to follow and that having a shared, visible basis for trust would increase uptake of the Federation.

These areas are illustrative, not prescriptive. The elected Co-Chairs, in consultation with the relevant Federation stakeholders, will define the precise problem, scope and use-case anchor in the first month of the mandate.

3 Expected membership

We are looking for members who are willing to contribute actively to an output of the kind described above, in line with the proposed structure (problem – solutions – actionable recommendations). Concretely, prospective members should be ready to:

- Research, analyse and write specific sections of the annual deliverable, within agreed deadlines.
- Critically review and provide constructive feedback on the contributions of fellow members.
- Incorporate feedback received from reviewers and other Federation bodies into the draft.
- Engage with the relevant EOSC Federation Working Groups and bodies – including, where relevant, the ESFRI–EOSC Task Force – and wider communities on data quality, sovereignty and trust, to keep the deliverable connected to real needs.
- Commit to consistent and continuous participation throughout the mandate.

Expertise should be relevant to the chosen disciplinary scope – for example: data quality management, stewardship and assessment; data sovereignty, compliance and digital autonomy (including familiarity with frameworks such as Gaia-X and the European data legislation); trustworthy repository certification (e.g. CoreTrustSeal); the governance of research infrastructures; or the requirements engineering and conformity mechanisms that turn principles into assessable criteria.

Applicants are asked to submit a short statement of relevant expertise, a CV, and an endorsement letter from their organisation; gender balance and broad representation across the community are taken into account in the selection.

