EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR DIGITAL SERVICES

Luxembourg

Cloud Sovereignty Framework

Version 1.2.1 – Oct. 2025

CONTENTS

1. Introduction 2
2. Sovereignty Objectives....2
3. Sovereignty Effective Assurance Levels....3
4. Assessment of Sovereignty Effectiveness....4
5. Computation of Sovereignty Score 6

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË – Tel. +32 22991111

Commission européenne, 2920 Luxembourg, LUXEMBOURG – Tel. +352 43011
Tel. direct line +352 4301-32243

1. INTRODUCTION

This document defines **Sovereignty Objectives** relevant for the provision of Cloud services requested in this procedure. They draw on European initiatives such as CIGREF's Trusted Cloud Referential v2, Gaia-X policy rules and architecture, and the European Cybersecurity Certification Framework (ENISA, NIS2, DORA). In addition, they echo lessons from national cloud sovereignty strategies (e.g., France's "Cloud de Confiance", Germany's "Souveräner Cloud"), as well as international practices in export controls, supply chain resilience, and security auditability. The result is a set of objectives that supplement security assurance requirements with sovereignty-specific safeguards defining clearly what sovereignty means.

The assessment will be conducted on the basis of open or closed questions asked to the tenderers, of supporting evidence provided by the tenderers and/or of the public documentation of the service, as explained in the tender specifications. The assessment is twofold:

- The contracting authority will assess the level of assurance provided by the tenderer for each of the Sovereignty Objectives, through a **Sovereignty Effectiveness Assurance Level** (**SEAL**). The SEAL level is used as a **Minimum Assurance Level**. The tender specifications indicate a minimum SEAL level that the cloud service provider must reach for each Sovereignty Objective. Tenders that do not offer the required (minimum) levels of assurance consistently across all objectives will be rejected.

- The contracting authority will also compute a **Sovereignty Score** for cloud services, complementary to the SEAL assessment, to sort the cloud services according to their respective sovereignty features. The formula used to compute the Sovereignty Score is provided in *Section 5*. The Sovereignty Score contributes to the quality score of the tender, as an **Award Criterion**.

The results of the sovereignty assessment, may also be used by the contracting authorities's technical services during the performance of the contract(s) resulting from this procedure, to determine the nature of systems that can be deployed at a specific provider, different risk profiles requiring different assurance levels.

2. SOVEREIGNTY OBJECTIVES

The list of Sovereignty Objectives of the procedure is provided in the following table:

#	Sovereignty Objectives	Sovereignty Objectives Descriptions
SOV-1	**Strategic Sovereignty**	Strategic sovereignty captures the degree to which the services of a cloud provider (or technology actor) are anchored within the European Union legal, financial, and industrial ecosystem. It assesses **ownership stability, governance influence, and alignment with EU strategic priorities**.
SOV-2	**Legal & Jurisdictional Sovereignty**	Legal & Jurisdictional sovereignty evaluates the **legal environment, exposure to foreign authority, and enforceability of rights** that govern the services of a technology provider. It determines the extent to which the services are anchored in European jurisdiction and insulated from external legal claims.
SOV-3	**Data & AI Sovereignty**	Data & AI sovereignty focuses on the **protection, control, and independence of data assets and AI services** within the EU. It addresses

#	Sovereignty Objectives	Sovereignty Objectives Descriptions
		how data is secured, where it is processed, and the degree of autonomy customers retain over AI capabilities.
SOV-4	**Operational Sovereignty**	Operational sovereignty measures the **practical ability of EU actors to run, support, and evolve a technology independently of foreign control**. It focuses on continuity of operations, skill availability, and resilience against external dependencies.
SOV-5	**Supply Chain Sovereignty**	Supply chain sovereignty evaluates the **geographic origin, transparency, and resilience of the technology supply chain**, focusing on the extent to which critical components and processes remain under EU control or exposed to non-EU dependencies.
SOV-6	**Technology Sovereignty**	Technology sovereignty evaluates the **degree of openness, transparency, and independence in the underlying technological stack**, ensuring EU actors can interoperate, audit, and evolve solutions without lock-in to foreign proprietary systems.
SOV-7	**Security & Compliance Sovereignty**	Security & Compliance sovereignty measures the **extent to which security operations, compliance obligations, and resilience measures are controlled within the EU**, ensuring independence from foreign jurisdictions and long-term operational assurance.
SOV-8	**Environmental Sustainability**	Environmental sustainability assesses **autonomy and resilience** of cloud services over the long term in relation to **energy usage, dependency and raw material scarcity**.

3. SOVEREIGNTY EFFECTIVE ASSURANCE LEVELS

The detailed list of **Sovereignty Effectiveness Assurance Levels** (**SEAL**) relevant for the procedure is provided in the table below:

Sovereignty Effectiveness Assurance Levels	Sovereignty Effectiveness Assurance Levels Descriptions
SEAL-0	*No Sovereignty*: Service, technology or operations under **exclusive control of non-EU third parties**, governed entirely in **non-EU jurisdictions**.
SEAL-1	*Jurisdictional Sovereignty*: **EU law formally applies** with **limited practical enforceability**; service, technology or operations under exclusive control of non-EU third parties.
SEAL-2	*Data Sovereignty*: **EU law applicable and enforceable**, with **material non-EU dependencies remaining**; service, technology or operations under indirect control of non-EU third parties.
SEAL-3	*Digital Resilience*: **EU law applicable and enforceable**, EU actors exercising **meaningful but not full influence**; service, technology or operations under marginal control of non-EU third parties.
SEAL-4	*Full Digital Sovereignty*: Technology and operations under **complete EU control**, subject only to **EU law**, with **no critical non-EU dependencies**.

4. ASSESSMENT OF SOVEREIGNTY EFFECTIVENESS

The Contracting Authority will assess the **Sovereignty Objectives** though questions asked in the questionnaire of the tender. Questions involved in the evaluation of Sovereignty Objectives effectiveness will be tagged with the reference of the Sovereignty Objective (i.e. SOV-0 to SOV-8) to which the answer contributes.

The tender specification defines the **minimum Sovereignty Effective Assurance Level** of **each Sovereignty Objective** required in the scope of the tender.

The assessment performed by the Contracting Authority will be based on the answers of the tenderer supplemented by supporting document provided in the context of the answers, and by public information made available by the tenderer.

The contributing factors involved in the assessment of each objective are described in the following table:

#	Sovereignty Objectives	Contributing factors
SOV-1	**Strategic Sovereignty**	- Ensuring that bodies having decisive authority over your services are located within EU jurisdiction, - Evaluating the assurances against change of control. - Degree to which the provider relies on financing coming from EU sources. - Extent of investment, jobs, and value creation within EU. - Involvement in EU initiatives, Consistency with digital, green, and industrial sovereignty objectives defined at EU level. - Ability to sustain secure operations against requests to cease or suspend the service, or if vendor support is withdrawn or disrupted.
SOV-2	**Legal & Jurisdictional Sovereignty**	- The national legal system governing the provider's operations and contracts. - Degree of exposure to non-EU laws with cross-border reach (e.g., US CLOUD Act, Chinese Cybersecurity Law). - Existence of legal, contractual, or technical channels through which non-EU authorities could compel access to data or systems. - Applicability of international regimes, which may restrict usage or transfer. - Location of intellectual property creation, registration, and development (EU vs. third countries), legal jurisdiction where IP is created and developed.
SOV-3	**Data & AI Sovereignty**	- Ensuring that only the customer, not the provider, has effective control over cryptographic access to their data. - Visibility into when, where, and by whom data is accessed, including auditability of AI model usage, mechanisms guaranteeing irreversible removal of data, with verifiable evidence. - Strict confinement of storage and processing to European jurisdictions, with no fallback to third countries. - Extent to which AI models and data pipelines are developed, trained, hosted, and governed under EU control, minimizing dependency on non-EU technology stacks.

#	Sovereignty Objectives	Contributing factors
SOV-4	**Operational Sovereignty**	- Ease of migrating workloads or integrating with alternative EU-controlled solutions without vendor lock-in. - Capacity for EU operators to manage, maintain, and support the technology without requiring non-EU vendor involvement - Existence of an EU-based talent pool with the expertise to operate and sustain the service. - Assurance that operational support is delivered from within the EU and subject exclusively to EU legal frameworks - Availability of full technical documentation, source code, and operational know-how enabling long-term autonomy. - Location and legal control of critical suppliers or subcontractors involved in service delivery.
SOV-5	**Supply Chain Sovereignty**	- Geographic source of key physical parts, manufacturing location - countries where hardware is manufactured or assembled - Jurisdiction and provenance of embedded code controlling hardware, firmware - Origin of Software: where and by whom software is architected and programmed, location and jurisdiction governing software packaging, distribution, and updates. - Degree of reliance on non-EU vendors, facilities, or proprietary technologies - Visibility into the entire supplier and sub-supplier chain, including audit rights.
SOV-6	**Technology Sovereignty**	- Ability to integrate with other technologies through well-documented and non-proprietary APIs or protocols, extent to which the solution adheres to publicly governed and widely adopted standards, reducing dependency on single vendors - Whether software is accessible under open licenses, with rights to audit, modify, and redistribute, ensuring transparency and adaptability - Visibility into the design and functioning of the service, including architectural documentation, data flows, and dependencies - Degree of EU independence in high-performance computing capabilities, including processors, accelerators, and software ecosystems.
SOV-7	**Security & Compliance Sovereignty**	- Attainment of EU and internationally recognized certifications (e.g., ISO, ENISA schemes) - Adherence to GDPR, NIS2, DORA, and other EU frameworks - Security Operations Centres and response teams operating exclusively under EU jurisdiction, control over security monitoring/logging - customer or EU authority ability to oversee logs, alerts, and monitoring functions directly. - Transparent, timely, and EU-compliant reporting of breaches or vulnerabilities, maintenance Autonomy - ability to develop, test, and apply security patches independently of non-EU vendors - Capacity for EU entities to perform independent security and compliance audits with full access.
SOV-8	**Environmental Sustainability**	- Adoption of energy-efficient infrastructure (e.g., low PUE) and measurable improvement targets. - Circular economy practices ensuring reuse, refurbishment, and responsible end-of-life treatment of hardware. - Transparent measurement and disclosure of carbon emissions, water usage, and other sustainability indicators.

#	Sovereignty Objectives	Contributing factors
		- Sourcing of renewable or low-carbon energy to power infrastructure and operations

The Contracting Authority will determine the assurance level given by the tenderer for each objective by taking all the above contributing factors into consideration. Material weaknesses identified in one or more contributing factor will result in lowering the overall assurance level recognized for the objective.

5. COMPUTATION OF SOVEREIGNTY SCORE

The Contracting Authority will compute a global **Sovereignty Score** complementary to the Sovereign Effective Assurance Levels, using the same questions involved in the assessment of the Sovereignty Objectives effectiveness.

The computation of the Sovereignty Score uses the points allocated to the question proposed in the tender, weighted as below:

#	Sovereignty Objectives	Weight in Scoring
SOV-1	**Strategic Sovereignty**	**15%**
SOV-2	**Legal & Jurisdictional Sovereignty**	**10%**
SOV-3	**Data & AI Sovereignty**	**10%**
SOV-4	**Operational Sovereignty**	**15%**
SOV-5	**Supply Chain Sovereignty**	**20%**
SOV-6	**Technology Sovereignty**	**15%**
SOV-7	**Security & Compliance Sovereignty**	**10%**
SOV-8	**Environmental Sustainability**	**5%**
	Total	**100%**

The weighting considers that the procurement procedure already contains significant safeguards in certain domains such as SOV-2 (*Legal and Jurisdictional*) and SOV-7 (*Security and Compliance*).

The Sovereignty Score is therefore computing according to the formula below:

$$\boldsymbol{Sovereignty\ Score} = \sum_{\boldsymbol{n=1}}^{\boldsymbol{n=8}} \frac{\boldsymbol{Score(SOV_n)}}{\boldsymbol{Max.Score(SOV_n)}} \times \boldsymbol{Weigth(SOV_n)}\ \%$$