EUROPÄISCHE KOMMISSION

GENERALDIREKTION DIGITALE DIENSTE

Luxemburg

Rahmenwerk für Cloud-Souveränität

Version 1.2.1 – Oktober 2025

INHALT

1. EINLEITUNG

Dieses Dokument definiert **die Souveränitätsziele,** die für die Bereitstellung der in diesem Verfahren angeforderten Cloud-Dienste relevant sind. Sie stützen sich auf europäische Initiativen wie das Trusted Cloud Referential v2 von CIGREF, die Richtlinien und Architektur von Gaia-X und den Europäischen Rahmen für die Zertifizierung der Cybersicherheit (ENISA, NIS2, DORA). Darüber hinaus spiegeln sie die Erfahrungen aus nationalen Cloud-Souveränitätsstrategien (z. B. „Cloud de Confiance" in Frankreich, „Souveräne Cloud" in Deutschland) sowie internationale Praktiken in den Bereichen Exportkontrolle, Widerstandsfähigkeit der Lieferkette und Sicherheitsüberprüfbarkeit wider. Das Ergebnis ist eine Reihe von Zielen, die die Anforderungen an die Sicherheitsgewährleistung durch souveränitätsspezifische Schutzmaßnahmen ergänzen, die klar definieren, was Souveränität bedeutet.

Die Bewertung erfolgt auf der Grundlage offener oder geschlossener Fragen an die Bieter, von den Bietern vorgelegter Belege und/oder der öffentlichen Dokumentation der Dienstleistung, wie in den Ausschreibungsunterlagen erläutert. Die Bewertung erfolgt in zwei Schritten:

- Der öffentliche Auftraggeber bewertet den vom Bieter für jedes der Souveränitätsziele angebotenen Sicherheitsgrad anhand eines **Souveränitäts-Effektivitäts-Sicherheitsgrades** (**SEAL**). Der SEAL-Wert wird als **Mindestgarantiewert** verwendet. In den Ausschreibungsunterlagen ist ein Mindest-SEAL-Wert angegeben, den der Cloud-Dienstleister für jedes Souveränitätsziel erreichen muss. Angebote, die nicht für alle Ziele durchgehend die erforderlichen (Mindest-)Garantiewerte bieten, werden abgelehnt.

- Der öffentliche Auftraggeber berechnet zusätzlich zur SEAL-Bewertung einen **Souveränitätswert** für Cloud-Dienste, um diese entsprechend ihrer jeweiligen Souveränitätsmerkmale zu sortieren. Die Formel zur Berechnung des Souveränitätswerts ist in *Abschnitt 5* angegeben. Der Souveränitätswert fließt als **Zuschlagskriterium** in die Qualitätsbewertung des Angebots ein.

Die Ergebnisse der Souveränitätsbewertung können auch von den technischen Diensten des öffentlichen Auftraggebers während der Ausführung der aus diesem Verfahren resultierenden Verträge verwendet werden, um die Art der Systeme zu bestimmen, die bei einem bestimmten Anbieter eingesetzt werden können, wobei unterschiedliche Risikoprofile unterschiedliche Sicherheitsniveaus erfordern.

2. SOUVERÄNITÄTSZIELE

Die Liste der Souveränitätsziele des Verfahrens ist in der folgenden Tabelle aufgeführt:

#	Souveränitätsziele	Beschreibung der Souveränitätsziele
SOV-1	**Strategische Souveränität**	Die strategische Souveränität erfasst den Grad, in dem die Dienste eines Cloud-Anbieters (oder Technologieakteurs) im rechtlichen, finanziellen und industriellen Ökosystem der Europäischen Union verankert sind. Sie bewertet **die Stabilität der Eigentumsverhältnisse, den Einfluss der Governance und die Übereinstimmung mit den strategischen Prioritäten der EU**.
SOV-2	**Rechtliche und jurisdiktionelle Souveränität**	Die rechtliche und jurisdiktionelle Souveränität bewertet das **rechtliche Umfeld, die Abhängigkeit von ausländischen Behörden und die Durchsetzbarkeit von Rechten**, die die Dienste eines Technologieanbieters regeln. Sie bestimmt, inwieweit die Dienste in der europäischen Gerichtsbarkeit verankert und vor externen Rechtsansprüchen geschützt sind.
SOV-3	**Daten- und KI-Souveränität**	Die Daten- und KI-Souveränität konzentriert sich auf den **Schutz, die Kontrolle und die Unabhängigkeit von Datenbeständen und KI-Diensten** innerhalb der EU. Sie befasst sich mit
#	Ziele der Souveränität	Beschreibung der Souveränitätsziele

		wie Daten gesichert werden, wo sie verarbeitet werden und inwieweit Kunden die Kontrolle über KI-Funktionen behalten.
SOV-4	**Operative Souveränität**	Die operative Souveränität misst die **praktische Fähigkeit von EU-Akteuren, eine Technologie unabhängig von ausländischer Kontrolle zu betreiben, zu unterstützen und weiterzuentwickeln**. Der Schwerpunkt liegt auf der Kontinuität des Betriebs, der Verfügbarkeit von Fachkräften und der Widerstandsfähigkeit gegenüber externen Abhängigkeiten.
SOV-5	**Souveränität der Lieferkette**	Die Souveränität der Lieferkette bewertet die **geografische Herkunft, Transparenz und Widerstandsfähigkeit der Technologie-Lieferkette** und konzentriert sich dabei auf das Ausmaß, in dem kritische Komponenten und Prozesse unter der Kontrolle der EU bleiben oder Abhängigkeiten außerhalb der EU ausgesetzt sind.
SOV-6	**Technologiesouveränität**	Die Technologiesouveränität bewertet den **Grad der Offenheit, Transparenz und Unabhängigkeit der zugrunde liegenden Technologieplattform** und stellt sicher, dass EU-Akteure Lösungen interoperabel einsetzen, prüfen und weiterentwickeln können, ohne an ausländische proprietäre Systeme gebunden zu sein.
SOV-7	**Souveränität in Bezug auf Sicherheit und Compliance**	Die Souveränität in Bezug auf Sicherheit und Compliance misst, **inwieweit Sicherheitsmaßnahmen, Compliance-Verpflichtungen und Resilienzmaßnahmen innerhalb der EU kontrolliert werden**, um die Unabhängigkeit von ausländischen Rechtsordnungen und die langfristige Betriebssicherheit zu gewährleisten.
SOV-8	**Ökologische Nachhaltigkeit**	Die ökologische Nachhaltigkeit bewertet **die** langfristige **Autonomie und Widerstandsfähigkeit** von Cloud-Diensten in Bezug auf **Energieverbrauch, Abhängigkeit und Rohstoffknappheit**.

3. SOUVERÄNITÄTS-EFFEKTIVITÄTS-SICHERHEITSSTUFEN

Die detaillierte Liste der für das Verfahren relevanten **Souveränitätswirksamkeits-Sicherheitsstufen** (**SEAL**) ist in der folgenden Tabelle aufgeführt:

Souveränitätswirksamkeits-Sicherheitsstufen	Beschreibungen der Wirksamkeitsgarantien für Souveränität
SEAL-0	*Keine Souveränität*: Dienstleistungen, Technologien oder Operationen unter **der ausschließlichen Kontrolle von Nicht-EU-Dritten**, die vollständig in **Nicht-EU-Rechtsordnungen** geregelt sind.
SEAL-1	*Gerichtsbarkeitssouveränität*: **Das EU-Recht gilt formal**, ist jedoch **in der Praxis** nur **begrenzt durchsetzbar**; Dienstleistungen, Technologien oder Tätigkeiten unterliegen der ausschließlichen Kontrolle von Nicht-EU-Drittländern.
SEAL-2	*Datenhoheit*: **EU-Recht anwendbar und durchsetzbar**, wobei **wesentliche Abhängigkeiten von Nicht-EU-Ländern bestehen bleiben**; Dienstleistungen, Technologien oder Operationen unter indirekter Kontrolle von Nicht-EU-Dritten.
SEAL-3	*Digitale Resilienz*: **EU-Recht anwendbar und durchsetzbar**, EU-Akteure üben **bedeutenden, aber nicht vollständigen Einfluss** aus; Dienstleistungen, Technologien oder Operationen unter marginaler Kontrolle von Nicht-EU-Dritten.
SEAL-4	*Volle digitale Souveränität*: Technologie und Betrieb unter **vollständiger Kontrolle der EU**, unterliegen ausschließlich **EU-Recht**, **keine kritischen Abhängigkeiten** von **Nicht-EU-Ländern**.

4. BEWERTUNG DER WIRKSAMKEIT DER SOUVERÄNITÄT

Der öffentliche Auftraggeber bewertet die **Souveränitätsziele** anhand der im Fragebogen der Ausschreibung gestellten Fragen. Die Fragen zur Bewertung der Wirksamkeit der Souveränitätsziele werden mit dem Verweis auf das Souveränitätsziel (d. h. SOV-0 bis SOV-8) gekennzeichnet, zu dem die Antwort beiträgt.

Die Ausschreibungsspezifikation definiert das **Mindestmaß an Souveränitätssicherung (Sovereignty Effective Assurance Level)** für **jedes Souveränitätsziel, das** im Rahmen der Ausschreibung erforderlich ist.

Die Bewertung durch den öffentlichen Auftraggeber basiert auf den Antworten des Bieters, ergänzt durch im Zusammenhang mit den Antworten vorgelegte Belege und durch vom Bieter zur Verfügung gestellte öffentliche Informationen.

Die Faktoren, die bei der Bewertung jedes Ziels eine Rolle spielen, sind in der folgenden Tabelle beschrieben:

#	Souveränitätsziele	Einflussfaktoren
SOV-1	**Strategische Souveränität**	- Sicherstellen, dass die für Ihre Dienste entscheidungsbefugten Stellen innerhalb der EU-Gerichtsbarkeit angesiedelt sind. - Bewertung der Garantien gegen einen Kontrollwechsel. - Grad, in dem der Anbieter auf Finanzmittel aus EU-Quellen angewiesen ist. - Umfang der Investitionen, Arbeitsplätze und Wertschöpfung innerhalb der EU. - Beteiligung an EU-Initiativen, Übereinstimmung mit den auf EU-Ebene festgelegten Zielen in Bezug auf digitale, ökologische und industrielle Souveränität. - Fähigkeit, einen sicheren Betrieb aufrechtzuerhalten, wenn Forderungen nach Einstellung oder Aussetzung des Dienstes gestellt werden oder wenn der Support durch den Anbieter eingestellt oder unterbrochen wird.
SOV-2	**Rechtliche und gerichtliche Souveränität**	- Das nationale Rechtssystem, das die Geschäftstätigkeit und Verträge des Anbieters regelt. - Grad der Exposition gegenüber Nicht-EU-Gesetzen mit grenzüberschreitender Reichweite (z. B. US-amerikanischer CLOUD Act, chinesisches Cybersicherheitsgesetz). - Vorhandensein rechtlicher, vertraglicher oder technischer Kanäle, über die Behörden außerhalb der EU den Zugriff auf Daten oder Systeme erzwingen könnten. - Anwendbarkeit internationaler Regelungen, die die Nutzung oder Übertragung einschränken können. - Ort der Schaffung, Registrierung und Entwicklung von geistigem Eigentum (EU vs. Drittländer), Rechtshoheit, in der geistiges Eigentum geschaffen und entwickelt wird.
SOV-3	**Daten- und KI-Souveränität**	- Sicherstellung, dass nur der Kunde und nicht der Anbieter die effektive Kontrolle über den kryptografischen Zugriff auf seine Daten hat. - Transparenz darüber, wann, wo und von wem auf Daten zugegriffen wird, einschließlich der Überprüfbarkeit der Nutzung von KI-Modellen, Mechanismen, die eine irreversible Löschung von Daten garantieren, mit überprüfbaren Nachweisen. - Strikte Beschränkung der Speicherung und Verarbeitung auf europäische Gerichtsbarkeiten, ohne Rückgriff auf Drittländer. - Umfang, in dem KI-Modelle und Datenpipelines unter EU-Kontrolle entwickelt, trainiert, gehostet und verwaltet werden, wodurch die Abhängigkeit von Technologie-Stacks außerhalb der EU minimiert wird.

#	Souveränitätsziele	Beitragende Faktoren
SOV-4	**Operative Souveränität**	- Einfache Migration von Workloads oder Integration mit alternativen EU-kontrollierten Lösungen ohne Herstellerabhängigkeit. - Fähigkeit der EU-Betreiber, die Technologie zu verwalten, zu warten und zu unterstützen, ohne dass die Beteiligung von Anbietern außerhalb der EU erforderlich ist - Vorhandensein eines Talentpools in der EU mit dem Fachwissen, um den Dienst zu betreiben und aufrechtzuerhalten. - Sicherheit, dass der operative Support aus der EU heraus erfolgt und ausschließlich den rechtlichen Rahmenbedingungen der EU unterliegt. - Verfügbarkeit vollständiger technischer Dokumentation, Quellcode und operativem Know-how, die eine langfristige Autonomie ermöglichen. - Standort und rechtliche Kontrolle kritischer Lieferanten oder Subunternehmer, die an der Erbringung der Dienstleistung beteiligt sind.
SOV-5	**Souveränität der Lieferkette**	- Geografische Herkunft wichtiger physischer Teile, Fertigungsstandort – Länder, in denen Hardware hergestellt oder montiert wird - Gerichtsbarkeit und Herkunft von eingebettetem Code zur Steuerung von Hardware und Firmware - Herkunft der Software: Wo und von wem wird die Software entwickelt und programmiert, Standort und Gerichtsbarkeit, die für die Verpackung, den Vertrieb und die Aktualisierung der Software zuständig sind. - Grad der Abhängigkeit von Nicht-EU-Anbietern, -Einrichtungen oder -proprietären Technologien - Transparenz in der gesamten Lieferanten- und Unterlieferanten-Kette, einschließlich Audit-Rechten.
SOV-6	**Technologische Souveränität**	- Fähigkeit zur Integration mit anderen Technologien durch gut dokumentierte und nicht proprietäre APIs oder Protokolle, Umfang, in dem die Lösung öffentlich geregelte und weit verbreitete Standards einhält, wodurch die Abhängigkeit von einzelnen Anbietern verringert wird - Ob Software unter offenen Lizenzen mit Rechten zur Prüfung, Änderung und Weiterverbreitung zugänglich ist, wodurch Transparenz und Anpassungsfähigkeit gewährleistet werden - Transparenz hinsichtlich des Designs und der Funktionsweise des Dienstes, einschließlich Architekturdokumentation, Datenflüssen und Abhängigkeiten - Grad der Unabhängigkeit der EU in Bezug auf Hochleistungsrechnerkapazitäten, einschließlich Prozessoren, Beschleunigern und Software-Ökosystemen.
SOV-7	**Sicherheit und Compliance Souveränität**	- Erlangung von EU- und international anerkannten Zertifizierungen (z. B. ISO, ENISA-Systeme) - Einhaltung von DSGVO, NIS2, DORA und anderen EU-Rahmenwerken - Sicherheitsoperationszentren und Reaktionsteams, die ausschließlich unter EU-Gerichtsbarkeit arbeiten, Kontrolle über Sicherheitsüberwachung/Protokollierung – Möglichkeit für Kunden oder EU-Behörden, Protokolle, Warnmeldungen und Überwachungsfunktionen direkt zu überwachen. - Transparente, zeitnahe und EU-konforme Meldung von Verstößen oder Schwachstellen, Wartung Autonomie – Möglichkeit, Sicherheitspatches unabhängig von Nicht-EU-Anbietern zu entwickeln, zu testen und anzuwenden - Möglichkeit für EU-Einrichtungen, unabhängige Sicherheits- und Compliance-Audits mit uneingeschränktem Zugriff durchzuführen.
SOV-8	**Ökologische Nachhaltigkeit**	- Einführung energieeffizienter Infrastruktur (z. B. niedrige PUE) und messbarer Verbesserungsziele. - Kreislaufwirtschaftspraktiken, die die Wiederverwendung, Aufarbeitung und verantwortungsvolle Entsorgung von Hardware gewährleisten. - Transparente Messung und Offenlegung von CO2-Emissionen, Wasserverbrauch und anderen Nachhaltigkeitsindikatoren.

#	Souveränitätsziele	Beitragende Faktoren
		- Beschaffung von erneuerbarer oder kohlenstoffarmer Energie für die Stromversorgung der Infrastruktur und des Betriebs

Die Vergabebehörde legt unter Berücksichtigung aller oben genannten Faktoren das vom Bieter für jedes Ziel angegebene Sicherheitsniveau fest. Wesentliche Schwächen, die bei einem oder mehreren Faktoren festgestellt werden, führen zu einer Herabsetzung des für das Ziel anerkannten Gesamtsicherheitsniveaus.

5. BERECHNUNG DER SOUVERÄNITÄTSPUNKTZAHL

Die Vergabebehörde berechnet eine globale **Souveränitätsbewertung**, die die effektiven Souveränitätsgarantien ergänzt, wobei dieselben Fragen verwendet werden, die auch bei der Bewertung der Wirksamkeit der Souveränitätsziele zum Einsatz kommen.

Die Berechnung der Souveränitätsbewertung erfolgt anhand der Punkte, die für die in der Ausschreibung gestellte Frage vergeben wurden, gewichtet wie folgt:

#	Souveränitätsziele	Gewichtung in der Bewertung
SOV-1	**Strategische Souveränität**	**15**
SOV-2	**Rechtliche und gerichtliche Souveränität**	**10**
SOV-3	**Daten- und KI-Souveränität**	**10**
SOV-4	**Operative Souveränität**	**15**
SOV-5	**Souveränität der Lieferkette**	**20**
SOV-6	**Technologiesouveränität**	**15**
SOV-7	**Souveränität in Bezug auf Sicherheit und Compliance**	**10**
SOV-8	**Ökologische Nachhaltigkeit**	**5**
	Gesamt	**100**

Die Gewichtung berücksichtigt, dass das Beschaffungsverfahren bereits in bestimmten Bereichen wie SOV-2 (*Recht und Gerichtsbarkeit*) und SOV-7 (*Sicherheit und Compliance*) erhebliche Sicherheitsvorkehrungen enthält.

Der Souveränitätswert wird daher nach der folgenden Formel berechnet:

$$SovereigntyScore = \sum_{n=1}^{n=8} \frac{Score(SOV_n)}{Max.\ Score(SOV_n)} \times Weight(SOV_n)\ \%$$