Annex: Assessment framework for the award criterion digital sovereignty

Level of Sovereignty: Dimension and aspects	1	2	3	4	5
Legal **1.1 Location**	**1. No EU establishment** – No legal establishment or head office within the EU	**2. EU branch establishment –** Only a branch or subsidiary in the EU; parent company and head office outside the EU	**3. EU parent company establishment –** Parent company legally established in the EU, head office outside the EU	**4. Fully EU-based –** Parent company legally established in the EU, head office within the EU	**5. Fully EU-based and local (NL) –** Parent company legally established in the EU, and head office within the EU. Also a branch or subsidiary in the Netherlands
Legal **1.2 Control and ownership**	**1. Full non-EU control** - Non-EU entity has decisive control	**2. Blocking non-EU influence –** Non-EU party holds a blocking minority interest or comparable rights	**3. Shared EU/non-EU control -** Control shared between EU and non-EU entities	4. **Predominantly EU control** – Majority of voting rights held by the EU, limited external influence	**5. Full EU control –** All voting rights and de facto influence exclusively European
Legal **1.3 Applicable law**	**1. Non-EU jurisdiction**				**5. EU jurisdiction**
Data & AI **2.1 Data residency**	**1. No guarantee of EU storage –** No guarantee whatsoever that data, backups, metadata or logs are stored or processed within the EU	**2. Partial EU storage –** Main data is stored in the EU, but backups, metadata or logs may be located or processed outside the EU. Data may be transferred outside the EU	**3. EU storage with exceptions –** Primary data and backups are stored within the EU, but system-generated data (such as metadata and logs) may be stored or processed outside the EU. Data transfer for analytics/training purposes is possible outside the EU for this system data	**4. EU storage and processing –** All data, including backups, metadata and logs, is physically and logically stored and processed within the EU. No form of data transfer outside the EU, not even for analytics or training	**5. Local/EU storage and processing –** All data, including backups, metadata and logs, is physically and logically stored and processed within the EU. No data transfer of any kind takes place outside the EU, not even for analytics or training. There are also options to store data locally (e.g. nationally or on-premises) as desired
Data & AI **2.2 Technical Access Security**	**1. No technical protection –** Contractor has full access to data; no encryption or key management by the customer	**2. Basic encryption (Platform Managed Keys) –** Data is encrypted, but the contractor manages all keys and can gain access	**3. Shared key management (BYOK/CMK) –** Customer provides or manages keys (Bring Your Own Key/Customer Managed Key), but the contractor can modify permissions or gain access via the cloud platform	**4. Customer-controlled key management (External Key Management/Managed HSM) -** Key management is entirely under the customer's control via an external HSM or Cloud HSM; the contractor has no or very limited access to key management	**5. Full cryptographic isolation (HYOK + Confidential Computing) -** The customer retains their own keys (Hold Your Own Key) and data remains cryptographically isolated, even during processing; the contractor has no access to unencrypted data at any time
Data & AI **2.3 Legal Access Safeguards**	**1. No obligation –** Contractor complies with foreign requests without objection	**2. Voluntary notification –** Contractor informs the customer voluntarily and/or on request, but does not challenge requests	**3. Contractual notification –** Contractor is obliged to report requests, but does not challenge them	**4. Active legal challenge –** Contractor is obliged to report requests and does not comply with the request; always attempts to refer the matter to the customer	**5. Full legal protection –** Contractor is obliged to report requests, does not comply with the request and refers the matter to international legal mechanisms such as the MLAT (Mutual Legal Assistance Treaty)

Technology **3.1 Interoperability & Portability**	**1. Complete lock-in –** Services are entirely proprietary; migrating data and workloads is not possible without significant effort or cost. No portability or interoperability	**2. Partial openness –** Open standards are used, but core components are proprietary; migration is possible to a limited extent and often requires extra effort; portability and interoperability are low	**3. Open standards with limitations -** Open standards are widely used, but not all components comply with them or use less common standards; portability and interoperability are partially limited	**4. All services based on open standards –** All components use open standards, but not always the most common variants. Portability and interoperability are high, but not fully optimised	**5. All services based on the most widely used open standards –** All components use the most common and widely accepted open standards. Portability and interoperability are maximised; migration and integration are simple and cost-effective
Technology **3.2 Open-source**	**1. Proprietary –** It is unclear whether and where open-source software is used; migrating workloads is not possible without significant effort or cost	**2. Proprietary with open-source components –** The service is primarily proprietary, but contains some open-source components; migration of workloads remains complex due to dependency on proprietary core components	**3. Open source with limitations –** Key components of the service are partly built on open-source software, but feature unique customisations, are one-of-a-kind and/or linked to proprietary integrations. Migrating workloads is no simple task and costs can mount up	**4. Fully open-source –** The service is fully open-source; workloads are easy to migrate. The chosen open-source software has large and active support communities	**5. Open-source evangelist -** The service is fully open source; data and workloads are easy to migrate. The chosen open-source software has large and active support communities. The contractor is also a major contributor to the development of (in-house) open-source software
Technology **3.3 Operational reversibility**	**1. No reversibility –** The service is not transferable; continuity in the event of the provider's failure is not guaranteed	**2. Limited reversibility –** Documentation is available to a limited extent, but transfer to a third party is complex and not fully possible	**3. Contractual reversibility –** The service is largely transferable; documentation and design are readily available, enabling a third party to operate the service independently in the long term	**4. Active reversibility –** The service is fully transferable; documentation and design are sufficiently detailed to enable a third party to operate the service independently	**5. Full operational reversibility –** The service is fully transferable; documentation and design are sufficiently detailed and tested to enable a third party to operate the service independently
Operational **4.1 EU-Infrastructuur en Control Plane**	**1. Fully non-EU operation –** The physical infrastructure (data centres, network) and control plane are located entirely outside the EU and are managed entirely by non-European parties	**2. EU infrastructure and non-EU control plane –** The physical infrastructure (data centres, network) is located within the EU, but the control plane is managed externally and is located outside the EU	**3. EU infrastructure and control plane –** The physical infrastructure (data centres, network) and control plane are located within the EU, but the control plane is (partly) managed externally	**4. Fully EU-based operation –** The physical infrastructure (data centres, network) and the control plane are guaranteed to be entirely within the EU	**5. Fully EU-based operation guaranteed –** The physical infrastructure (data centres, network) and the control plane are guaranteed to be entirely within the EU. Periodically audited by a recognised EU partner
Operational **4.2 Supply Chain Resilience**	**1. Absent –** No strategy outlined for dealing with supply chain disruption	**2. Ad-hoc –** The contractor has an initial or partial strategy (data centres/ infrastructure or services) to limit reliance on non-EU hardware and critical software, thereby ensuring service continuity in the event of geopolitical sanctions or supply chain disruptions	**3. Repeatably documented –** The contractor must have a comprehensive (data centres, infrastructure and services) documented strategy that is repeatable and auditable to limit dependence on non-EU hardware and critical software, thereby ensuring service continuity in the event of geopolitical sanctions or supply chain disruptions	**4. Systematic –** The contractor must have a comprehensive (data centres, infrastructure and services) documented strategy that is regularly audited by a recognised European body to limit dependence on non-EU hardware and critical software, thereby ensuring service continuity in the event of geopolitical sanctions or supply chain disruptions	**5. Leading –** The contractor must have a comprehensive, documented strategy (covering data centres, infrastructure and services) that has been audited to limit reliance on non-EU hardware and critical software, thereby demonstrably ensuring service continuity for a minimum agreed period in the event of geopolitical sanctions or supply chain disruptions