N°	Appendix 1: CISPE Sovereign Cloud Service Requirements
1	**Legal requirements**
1.A.	**Jurisdictional immunity of the service provider**
1.A.1.	The registered office, central administration and main establishment of the service provider must be established within a country of the Defined Geographical Area of Sovereignty.
1.A.2.	No entity which registered office, central or main establishment is established outside of the Defined Geographical Area of Sovereignty, shall whether acting individually or collectively, exercise direct and indirect control over the Service Provider whether through ultimate voting control and other controlling rights, as shareholders, beneficial owners or otherwise.
	If the capital held by these third-party entities is in the form of shares admitted to trading on a regulated market, these third-party entities are those declared in accordance with the notification and disclosure requirements as set out in the regulation applicable in the Defined Geographical Area of Sovereignty.
1.A.3.	Members of the Board and Executive team of the organisation shall not be subject, by virtue of their nationality, right of residence or domicile, to laws or regulations that may impose extraterritorial obligations conflicting with the principles of sovereignty applicable under this framework
1.B.	**Right of veto and appointment**
1.B.1	No third-party entity whose registered office, central administration or main establishment is located outside of the Defined Geographical Area of Sovereignty, nor any natural person who is a national of or has his domicile or a right of residence in a third country outside the said area of sovereignty, shall, individually or collectively, directly and indirectly: - by virtue of a contract or statutory clauses, have a right of veto over the service provider; - by virtue of a contract or statutory clauses, appoint the majority of the members of the administrative, management or supervisory bodies of the service provider.
1.C.	**Contractual Data Sovereignty requirement**
1.C.1	The service provider must contractually commit to:
	(a) subject to the paragraph C.(b), to not transfer any of customer's and user's data : (i) to any authority belonging to a country or region which is not part of the Defined Geographical Area of Sovereignty; (ii) to, or within, any third country or region that is not part of the Defined Geographical Area of Sovereignty; and, (iii) more generally, to any third-party other than subcontractors or recipients expressly authorized by the customer.
	(b) where a transfer is expressly required by a decision recognized and enforceable under the law of the country of Defined Geographical Area of Sovereignty to which the service provider is subject: (i) formaly assess of such recognition and enforceability, where necessary with the support of competent and recognized external legal counsel); (ii) inform the customer without delay, unless such notification is prohibited by the applicable law; (iii) limit the disclosure of the Customer's Data strictly to whait is expressly required by such decision.
1.C.2	The Service Provider shall keep a record of any request from a third party to obtain communication of the data covered by this framework, containing at least: (a) the request, (b) the response to the request, (c) in the case may be, the identification of any data transmitted to the requesting third-party (including the recipient(s) and the dates of communication) and (d) the legal basis under which the data has been transmitted (notably the assessment demonstrating the recognition and enforceability of the request under the law of the geographical area of sovereignty).
1.D	**Change of control notification**

1.D.1	In case of any breach to the requirements of this section 1., notably but not imited to any direct or indirect takeover or acquisition of the service provider by a third-party that does not match the said requirements, the service provider shall immediately notify in writing its customers, CISPE and the monitoring body.
1.D.2	Such written notification obligation, as described in paragraph 1, shall be expressly provided in the service agreement between the client and the service provider.
1.E	**Applicable law and jurisdiction**
1.E.1	The service agreement shall be subject to the exclusive law and jurisdiction of a country which is part of the defined geographic area of sovereignty.
1.E.2	The applicable law and jurisdiction must be clearly identified in the service agreement.
1.F	**Jurisdictional immunity of the subcontractors**
1.F.1	In the event of recourse, within the framework of the services, to the services of a direct or indirect subcontractor – all the requirements defined in this section 1 are fully applicable to such subcontractors - unless its subcontractors have no technical possibility to autonomously access, obtain, make unavailable, destroy or more broadly process critical data as defined under this framework. Where a subcontractor retains the technical capability to impact the availability of services (including, but not limited to, infrastructure or co-location providers capable of interrupting power, connectivity, or physical hosting conditions), the service provider shall implement appropriate sovereignty safeguards, including but not limited to: - real-time or near real-time mirroring of critical workloads and data to infrastructure operated under sovereign control within the defined area of Sovereignty ; or - deployment across a federated, distributed, or multi-provider infrastructure designed to prevent any single non-compliant subcontractor from unilaterally making the service unavailable. These measures must ensure that no subcontractor subject to non-compliant jurisdictions can, acting alone, effectively compromise the availability, integrity, or sovereignty of the service.
1.G	**Vendor and subcontractor clauses**
1.G.1	Absence of any contractual terms that grant the right to terminate the delivery or the right to use any critical asset whose unavailability would compromise the availability of the Service for any reason other than non-payment, abuse or material breach of the terms of use.
2.	**Operational requirements**
2.A	**Asset location and redundancy**
2.A.1	All the Critical Assets that are used in the course of providing the service - including assets managed by subcontractors - must be fully located within the Defined Geographical Area of Sovereignty .
2.C	**Support operation**
2.C.2	In no event (i) access to and process of the Critical Data nor (ii) operation (notably management, administration, supervision, configuration, intervention, etc) on Critical Assets, shall be technically possible from outside the Defined Geographical Area of Sovereignty.
2.D	**Interoperability**

2.D.1	The services shall be designed in order to ensure the customers can easily migrate to another solution/service, notably in case of any circumstance impacting the continuity or the security of the service. The service must notably: a) be cerified as compliant with EU Data ACT or similar local legislation or alternatively : b) be interoperable and easily portable to other service providers notably by using open-source solutions or solution widely used into the market of the Defined Geographical Area of Sovereignty; or alternatively, by providing its services through a federated and distributed cloud service infrastructure; c) contain no lock-in features; d) provide appropriate technical and organisational measures that ensure and facilitate their reversibility.
3.	**Technological requirements**
3.A	**Hardware management**
3.A.4	The service provider shall implement and maintain appropriate technical and organizational measures to secure critical key hardware equipment and components (notably isolation, testing and validation of non sovereign vendors-signed updates such as Firmware/BIOS updates, etc.) in order to not compromise the service provider operational autonomy, and the service availability and security.
3.B	**Software management**
3.B.1	The service provider must endeavour to obtain commitments or, at a minimum, information from the publisher of any critical software asset whose unavailability would compromise the availability of the Service regarding the duration of software maintenance in order to avoid the risk of unavailability that may result in particular from a defect or cessation of maintenance by the publisher, suspension of service, or failure on the part of the publisher; particularly when the publisher is a national of a country outside the Defined Geographical Area of Sovereignty. Where such commitments cannot be obtained, the service provider shall demonstrate technical and organisational measures ensuring continuity of service independently from the publisher, including the ability to maintain, operate, or substitute the software to ensure minimal viable functionality without reliance on the publisher’s continued support.
3.B.2	If a third party propriatory software is used or made available as part of the provision of the service, the service provider shall, in order to ensure the continuity of the service in particular in case of any defect or failure of the vendor or restriction from the foreign authority which the vendor may be subjected to: (a) identify one or several alternative software - notably if possible open source solution; (b) If an equivalent software cannot be identified - for example in edge and cybersecuirty services including WAF,DDoS, CDN, and traffic filtering services - a solution ensuring minimal viable functionality must be identified (c) implement tests and a switchover plan enabling migration to such alternative solutions. (d) Regarding SaaS software, ensure compliance of software with Data ACT or similar local regulation.
3.B.3	The service provider shall implement and maintain appropriate technical and organizational measures to secure the maintenance of critical software in order to not compromise operational autonomy.
3.C	**Operational autonomy**

3.C.1	The service provider must be in full capacity to maintain the entire service - including any software, equipment and components used to provide the service – by itself or by using the services of at least two third-party companies. This operational autonomy shall be guaranteed by any third party used by the service provider to provide the service. This too shall apply in the case of the use of subcontractors' cloud service, where such services must themselves be certified Sovereign in order for the Cloud Service to qualify as such.
3.C.2	Critical assets that are provided, owned, or licensed by a non-sovereign entity, and whose unavailability would compromise the availability of the Service, notably control plane and data plane equipment, components and software, must not include any remote or build-in disable features that may bypass the service provider's in-sovereign Zone administrative control. The service provider shall notably demonstrate it has implemented and documented appropriate controls to prevent the existence of any such remote or build-in kill-switch features (notably testing and controlling operation as part of the maintenance, firmware, bios and software up-date procedures).
3.C.3	When a key hardware equipment or proprietary component is used or made available as part of the provision of the service, the service provider shall, in order to ensure the continuity of the service in particular in case of any defect or failure from the supplier entity or restriction from a foreign authority which the supplier is subjected to: (a) Identify one or several alternative solution - notably if possible open source; (b) Implement periodical tests and a switchover plan enabling migration to such alternative solutions.
4	**Data Sovereignty requirements**
4.A	**Information and consent**
4.A.1	The Service Provider shall undertake into the service agreement to process the customer's personal data only in accordance with (a) the applicable law in the Defined Geographical Area of Sovereignty and (b) the customer's documented instructions which may be provided in the services agreement and in writing during the utilisation of the Services. +B46
4.A.2	The service provider must keep available to the customer an up-to-date documentation specifying the exhaustive list of countries where (a) Customer's data, (b) Technical Data, (c) Users Data and (d) Administrative Data is stored and processed, including remotely. This information must be clear and easily accessible to the customer.
4.A.3	Except for Administrative Data, the service provider shall in no circumstances move the data outside the Defined Geographical Area of Sovereignty without the customer's consent.
4.B	**Data encryption**
4.B.1	Except for the customer's data, the service provider must ensure that all data is protected by appropriate and effective use of state-of-the-art encryption mechanisms. In particular: (a) Data must be encrypted in transit and at rest using protocols recognized for their robustness and security (e.g., TLS or equivalent). (b) The encryption keys used must be fully generated, stored, managed and deleted in and from the defined geographical zone of sovereignty and in accordance with key management practices aligned with international security standards. (c) The service provider must ensure that the encryption prevents unauthorized access, including by third parties involved in the network infrastructure used for the failover. (d) The service provider must document and regularly test the implemented encryption mechanisms to ensure their effectiveness and compliance with sovereignty and operational continuity requirements of this framework.
4.B.2	Concerning customer's data, the service provider shall (a) make available to the customer encryption solution as part of the services or (b) enable the customer to implement its own encryption mechanisms.
4.C	**Data and processing location**

4.C.1	The service shall be configured and organized as follow: (a) Any Critical data shall be stored and processed exclusively in and from the Defined Geographical Area of Sovereignty; (b) Third-parties that do not meet the legal sovereignty requirements described in section 1 of this framework shall in no circumstances be technically able to access, obtain, make unavailable, destroy and more generally process Critical data.
4.C.2	The transfer or processing of any customer's data to a third country shall be permitted only where the following cumulative criteria are met: (a) such transfer is authorised under the law applicable within the defined geographical zone of sovereignty (b) the law applicable within the defined geographical zone of sovereignty formally and expressly recognises the third country as ensuring a level of protection of data equivalent to that provided within the said zone (c) the law applicable in the defined geographical zone of sovereignty does not conflict with the law of the third country where the data is transfered. (d) Such transfer is expressly pre-approved by the customer in writing; (e) the service shall provide the customer the option to store and process Critical data entirely in the Defined Geographical Area of Sovereignty excluding any third country.
5	**Optional configuration of the service**
5.1	Where a cloud service is available both as a sovereign and a non-sovereign service, the option must be clearly communicated – including the applicable conditions - to the customer as part of (a) the service agreement, service description, (b) the service description and (c) the service ordering process.
5.2	Optional sovereign and resilient service configurations shall be proposed by default or be easily activable during the service ordering process and the service configuration set-up, in order to ensure that the customer can activate them when needed.
6	**Minimum additional certification requirements**
6.1	The service provider must implement appropriate technical and organizational measures to ensure that its organization and service comply with the requirements of these labels on an on going basis.
6.2	These technical and organizational measures must comply with recognized information security management standards such as ISO27001/27017, SecNumCloud or BSI C5, enabling notably but not limited to, an appropriate and secure management of the following: - Asset management; - Access rights, access control, and identity; - Data protection, location and transfer; - Changes (notably technological, operational, HR, security and third-praty changes); - Supply chain security levels, control and audit (including sub-processors); - Transparency to customers (notably about data location, data access by third-parties, security and resilience measures); - Business and service continuity and resilience; - Incident and vulnerability; - Solution development, testing, integration and maintenance.
6.3	The compliance of the service and service provider's organisation to such a recognized information security management standards, must be certified by an external monitoring body accredited to conduct such compliance assessment and provide the relevant certification. The certification shall be maintained during all the service delivery.
7	**Sustainability (Optional requirement)**
7.1	The service provider shall provide transparency on the environmental impact of the service.
7.2	The service meets the targets of a environmental standard recognized by the industry in the Defined Geographical Area of Sovereignty (such as the Climate Neutral Data Centre Pact).