N°	Appendix 2: CISPE Resilient Cloud Service Requirements
1	**Legal requirements**
1.A.	**Jurisdictional immunity of the service provider**
1.A.1 bis	The service provider must be legally established in the Defined Geographical Area of Sovereignty.
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.A.2	If in the course of providing the services, one or more non-Critical Assets are located outside the Defined Geographical Area of Sovereignty, the service provider shall obtain prior written consent of the client and set up at least one redundant asset in the Defined Geographical Area of Sovereignty. The redundant asset shall be equivalent to the non-critical asset which is located outside the defined geographic area of sovereignty, notably present equivalent functionalities, technical characteristics, security measures and service levels according to the service provider contractual commitments to the customer.
2.C	**Support operation**
2.C.1	When support operations are performed from a State located outside the Defined Geographical Area of Sovereignty, the service provider must: (a) document and keep up to date the exhaustive list of operations concerned; (b) obtain the customer's prior approval; (c) implement access control and oversight mechanisms ensuring the traceability, security, and governance of these operations from the Defined Geographical Area of Sovereignty; (d) guarantee that these operations do not in any way compromise the requirements of this framework and operational autonomy of the service provider.
2.D	**Interoperability and no lock-in features**
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.
2.D.2	The service provider shall notify to the customer without delay any event impacting the continuity of the service in order to enable the customer to activate its service continuity plan notably through third party

2.D.3	The Service Provider must ensure back-ups can be done autonomously by the customer using third party tools in formats restorable outside of the service providers infrastructure (i.e. back-ups of virtual machines, databases, files, and other services, including both data and configurations).
2.E	**Control and right of access to data**
2.E.1	The service provider must guarantee the customer full, continuous, and secure access to the customer's data, Technical Data and Users data contemplated into this framework.
2.E.2	The service provider must provide documentation detailing the procedures, formats, and interfaces made available to the customer to access the data. The service provider must provide the customer with the technical means to access customer's data autonomously, without exclusive dependence on the service provider. The conditions to access Users Data and Technical Data must be expressly provided into the service
2.E.3	Access to data must be available for the entire duration of the contract. The condition of availability of the data after the end of the contract, must be clearly provided into the service agreement.
2.E.4	Access to data must be implemented through secure mechanisms guaranteeing the confidentiality, integrity, and traceability of access.
3.	**Technological requirements**
3.A	**Hardware management**
3.A.1	Appropriate level of stock of key hardware equipment and components shall be defined and maintained in order to ensure the continuity of the service, taking into account the following circumstances: (a) the growth orientation of service provider's activities, (b) the availability of the components and equipment on the market, in particular in the Defined Geographical Area of Sovereignty, (c) their life cycle, (d) the country where they are designed and manufactured, (e) the jurisdiction and the law applicable to the manufacturer and vendor, (f) if hardware equipment or component is designed and manufactured outside of the Defined Geographical Area of Sovereignty, the availability of alternative equipment or components designed and manufactured within the Defined Geographical Area of Sovereignty.
3.A.2	Stock of key hardware equipment and components shall be: (a) continuously monitored and (b) periodically reassessed, at predefined intervals and in case of material change of circumstances.

3.A.3	The service provider shall notify to the customers without delay any event such as supply chain or transportation issue, or foreign authority export restriction, resulting in an unavailability of key hardware equipment or components in the Defined Geographical Area of Sovereignty, impacting the continuity of the service.
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
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.
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, notably control plane and data plane equipment, components and software, must not include any remote 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 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.
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
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.B.3	Only the customers, not the service provider, has effective control over cryptographic means to decrypt and access to their data.
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).