CISPE Digital Sovereignty Principles for Cloud Infrastructure Services

Background at EU level

In her 2020 State of Union, European Commission President Ursula von der Leyen announced that Europe should secure digital sovereignty with a common vision of the EU in 2030, based on clear goals and principles. According to Commissioner Thierry Breton "digital sovereignty 'rests on three inseparable pillars: computing power, control over our data and secure connectivity" [1].

The Digital Compass 2030 published by the EU Commission (EC) in March 2021 stressed the EC's ambition to bolster digital transformation for EU's resilience with the clear target of having 75% of European enterprises in the cloud by 2030[2]. By contrast, the Commission also identified issues both on the supply side and on the demand side which need to be fixed: 1/ data produced in Europe is often stored and processed outside Europe, and its value may be extracted outside Europe; 2/ Evolving EU rules and standards, particularly on data protection, have created uncertainty for EU customers regarding the use of cloud service providers (CSPs); 3/ CSPs operating in the EU may also be subject to legislation of third countries conflicting with EU laws and values; 4/ micro-enterprises, start-ups and SMEs suffer economic detriment because of contract-related problems (e.g. unfair contract terms); 5/ European businesses may suffer economic detriment due to the lack of interoperability and portability of some providers' solutions.

CISPE and Digital Sovereignty

If Digital Sovereignty is key for Europe, it is key as well for any economic area in the world. Therefore, addressing the topic widely should be considered, and we believe that European values of Data Protection, Security, Portability and Transparency shall be the driver to develop principles that could be largely supported and operated worldwide, while answering the expectations of European stakeholders.

CISPE believes in continuous innovation, particularly for SMEs by creating an ecosystem of trust for businesses of all sizes to scale up and compete. Cloud infrastructures are the catalyst for such genuine digital and environmental transformation as they provide the underlying IT infrastructure tools for organizations and individuals: the processing, storage, networks and other fundamental computing resources necessary to deploy and run essential software and systems.

CISPE supports the priority in Europe given to technological and digital sovereignty as an enabler of trust in cloud services for EU businesses and Governments. However, we observe that there is a lack of definition of what digital sovereignty actually means, particularly for the cloud industry.

Overall, when using cloud services, many customers want more clarity and legal certainty from CSPs so that they can trust the technology and focus on innovation to grow their business and compete. In its unique position of being the voice of EU CSPs, CISPE recommends defining concrete customer-centric attributes of digital sovereignty in the cloud that will not only ensure the uptake of cloud computing in Europe but also create a "leading role model for a society empowered by data to make better decisions – in business and the

[1] https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en
[2] https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

public sector"[3], including outside of Europe. **CISPE has also been constantly supporting a greater harmonization of applicable rules in Europe, including cybersecurity attributes and other relevant** attributes **regarding Digital Sovereignty like data protection and portability of data.**

CISPE's suggested approach to digital sovereignty in the cloud

To successfully achieve its digital transformation goal while maintaining sovereignty, the EU should support the right tools and mechanisms that ensure trust in cloud infrastructure services as well as the freedom of choice for cloud customers. In this context, CISPE has identified the four attributes of digital sovereignty in the cloud representing core EU values that customers should be able to control:

- Freedom of technological choice
- Control of data protection
- Control of security and resilience
- Control of legal protection and applicable jurisdictions

1/ Freedom of technological choice

Principle: Customers should be able to choose the best technology available in terms of functionality, security and availability to build services quickly and securely and deploy them where required in order to grow their business and compete. Customers should be free to choose at any time the CSPs, services, features and the deployment model that best fits their needs without being hindered by unfair license terms.

Recommended measures:

a. CSP shall provide the necessary technical capabilities to support the customer portability activities

b. CSP shall provide transparency about such capabilities, in compliance with the IaaS Switching and Porting (SWIPO IaaS) Code of Conduct or any other alternatives.

c. CSP shall comply with the Ten Principles of Fair Software Licensing for Cloud Customers supported by a variety of customers and providers trade associations.

2/ Control of data protection

Principle: Customers should be able to ensure that their CSPs fully comply with their obligations as a processor under EU privacy laws. Based on their choice, customers should be able to choose to store and processor their data in the EEA only or to use cloud services either to transfer their data outside of the European Economic Area (EEA) in accordance with the General Data Protection Regulation (GDPR), the EUCJ Schrems II ruling and Standard Contractual Clauses (Commission implementing decision (EU) 2021/914).

Recommended measures:

a. CSPs shall design its services to offer the possibility to store customer data in one or multiple locations, including the option to store and process their data exclusively in EEA.

[3] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

b. CSPs shall have services certified against a compliance tool listed in GDPR and approved by data protection authorities and the European Data Protection Board (EDPB) to demonstrate compliance with their obligations as processors under GDPR (CISPE Data Protection Code of Conduct).

c. CSPs as a processor, shall contractually commit to process the data according to customer's instructions and shall only process or use customer data to maintain or provide the service and will not use customer data for marketing or advertising purposes as processor, in compliance with the CISPE Data Protection Code of Conduct.

3/ Control of security and resilience

Principle: Customers should be able to ensure CSPs can demonstrate compliance with state-of-the-art of cloud security with respect to the infrastructure, systems and networks under the control and responsibility of the CSPs.

Recommended measures:

CSPs shall demonstrate compliance with EU Cloud Security Scheme's level "substantial" or higher, all verified by an independent third party.

4/ Control of legal protection and applicable jurisdictions

Principle: Customers should be able to control that when using cloud services, their interests and intellectual property are protected under EU laws and shielded against law enforcement access requests that would be directed to their CSPs. In particular, under all levels of assurance provided by the ENISA European Cloud Certification Scheme (EUCS).

Recommended measures:

a. The contract between customers and CSPs shall include that EU laws apply to the contract as required by applicable law and to any legal dispute between the parties. Also, the contract shall not include any transfer of customer data outside of the EEA without customer consent.

b. CSPs shall provide the choice for all customer data to be stored and processed exclusively in EEA, with options for support located in the EEA.

c. CSPs shall carry out a formal risk assessment related to applicable non-European extra-territorial regulations to its services, and if any, for specific services from certain CSP locations. This risk assessment shall be made available to customers and competent authorities and include the description of technical, organisational and legal measures in place to mitigate the risks and identify residual risks.

d. The contract between customers and CSPs shall include commitments to challenge law enforcement requests to access customer data directly from CSPs.

e. CSPs shall make publicly available, on a regular basis, transparent information about law enforcement requests received from law enforcement authorities including at least, the number of requests received, the country of origin of the requests and the number of responses provided by the CSP.

f. In the context of public procurement, CSPs shall undertake reasonable efforts to comply with the conditions set out in the CISPE Buying Cloud Services in the Public Sector handbook.

g. CSPs should put in place the contractual, operational and technical controls necessary to ensure adequate protections are enforced through their supply chain.

h. Where the "substantial" and "high" levels of the forthcoming ENISA cybersecurity scheme apply, CSPs shall provide to customers and competent authorities a risk assessment regarding the origin of software layers embedded in cloud services which may relate to export controls, restriction of use or third-party audits and/or rights. This risk assessment shall include maintenance, upgrade and support.

i. Where the "substantial" and "high" levels of the forthcoming ENISA cybersecurity scheme apply, including the EUCS, the CSP shall provide for independent assurance and audit of its security controls.

j. Where Member States law or customer request requires the level "high" of the EUCS scheme to apply to specific categories of data the CSP shall:

- (1) not give satisfaction to any unlawful access request to customer data, through any appropriate mechanisms including ownership (European control of the CSP with capital control and voting rights above 50%, no veto right outside EEA), legal (subject to exclusive European jurisdiction) and/or technical means.
- (2) ensure subcontractors, in particular colocation providers, not fulfilling the same provisions shall have no permanent, systematic and/or automated access to customer data. Access to data shall be done only upon customer instruction.

About CISPE

Cloud Infrastructure Services Providers in Europe (CISPE.cloud) is a non-profit association that focuses on developing greater understanding and promoting the use of cloud infrastructure services in Europe. Members based in 14 EU Member States range from SMEs to large multinationals. CISPE members invest billions of euros in Europe's digital infrastructure and currently provide services to millions of customers, including organisations in multiple countries and locations outside the EU.

Security and data protection are cornerstones of the CISPE constitution. It was the first association in the EU to develop a dedicated GDPR-compliant Code of Conduct for Data Protection for the sector, aligning with strict GDPR requirements to help providers comply while bringing clarity to customers to help them select providers and build trust in their services.

CISPE has always aligned with EU values: since 2016 all services declared under the CISPE GDPR Code of Conduct offer customers the ability to opt for services that securely store and process data exclusively within the EEA. CISPE also co-chaired the cloud industry working group (European Commission) to develop codes of conduct for reversibility and data portability under the Regulation on the free flow of non-personal data. In January 2021, CISPE has been a key driving force towards the creation of the Climate Neutral Data Centre Pact, supported by the European Commission, which engages the data centre and cloud infrastructure industries to be climate neutral by 2030.