Are we far from a solid EU Digital Regulation protecting Sovereignty and creating cloud service immunity from foreign jurisdictions?

Francisco Mingorance, Executive Secretary
CISPE.cloud
07/11/2022
CISPE & your speaker – Francisco Mingorance, Executive Secretary

**Board Member**
Climate Neutral Data Center Pact (www.climateneutraldatacentre.net)
Mar 2022 - Present · 2 mos

**Gaia-X Board Member representing CISPE**
Gaia-X Association for Data and Cloud (AISBL)
Jun 2021 - Present · 11 mos
Brussels Region, Belgium

**Executive Secretary**
CISPE (Cloud Infrastructure Services Provide)
Oct 2016 - Present · 5 yrs 7 mos
Brussels, Brussels Region, Belgium

**CISPE.cloud**
- Created in 2016. Developed first GDPR (data protection) Code of conduct to encourage storage and processing of personal data in Europe
- 24 members ranging from SMEs to multinationals – with shared values
- Founding members of the Gaia-X European Cloud Initiative
- Convener of the Climate Neutral Data Centre Pact
- Co-developer of 10 Fair Software Licensing Principles with Cigref and CIOs organisations
Overview and short answer…

**Question:** Are we far from a solid EU Digital Regulation protecting Sovereignty and creating cloud service immunity from foreign jurisdictions?

**Answer:** at least 18 months, or more.

1. EU Regulatory landscape for Cloud Sovereignty: EUCS, NIS2, GDPR, Data Act…
2. Industry responses: Bleu, S3NS, Delos, VMware, Gaia-X
3. CISPE definition of Digital Sovereignty for cloud: 4 Attributes and 20 Measures
4. Forward-looking perspectives
EU Regulatory landscape for Cloud Sovereignty
EUCS - European Union Cybersecurity Certification Scheme on Cloud Services

*Demand:* private and public sector services immune to third countries jurisdictions

- October 26 letter by four leading EU CIOs customer organisations: DE, FR, BE and NL

Customer *concerns:* loosing access to business-critical cloud services and applications

Cloud Providers *opportunities:* new sovereign cloud offerings; new industry partnerships

Member States views and arbitrage on jurisdiction immunity for cloud services:

- Technical security certification (leveraging on NIS2) or ad-hoc (political) legislation?
- An EUCS fourth level for immunity? Ongoing Review and Decision in 2024?

What other EU Regulations?
EU Regulatory landscape for Cloud Sovereignty (2)

Data Act, GDPR

**GDPR** Article 47 - Chapter 5 on Transfers or disclosures not authorised by Union law - and adequacy decisions

Adequacy decision: The European Commission has so far recognised Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.

**New US-EU Privacy Shield:** Mid-2023; Legal challenge?

**European strategy for data** and **Data Act Article 27** International access: 2024 entry into force
Industry responses and customers needs
VMware, Gaia-X, Bleu, Delos, etc… CISPE definition of Digital Sovereignty for cloud

Plethora of industry initiatives:

1. S3NS: Google and Thales: 2023 – 2024
2. Bleu: Orange, Microsoft, CapGemini: : 2024 ?
3. Atos and AWS toward SecNumCloud certification: 2024
4. Dassault 3DS Outscale, Bouygues and La Poste: 2023
5. Delos : SAP, Microsoft and Arvato for German public sector: 2024
6. Gaia-X Federated Services and Trust Framework Level 3 Label for jurisdiction immunity
   – Gaia-X Summit Catalogue Demo – what are the current sovereign cloud market offerings ?
Industry responses to regulatory initiatives and customers needs (2)
CISPE definition of Digital Sovereignty for cloud

Plethora of initiatives, but lack of definition. What does digital sovereignty mean, for the cloud?

4 Attributes and 20 Recommended Measures (+/-)
https://cispe.cloud/cispe-digital-sovereignty-principles-for-cloud-infrastructure-services/

1. Freedom of technological choice: *freedom to choose the best technology available in terms of functionality, security and availability, features and the deployment model that best fits their needs*

2. Control of data protection: *ensure fully compliance with EU privacy laws and enable full EEA storage/processing*

3. Control of security and resilience: *demonstrate compliance with state-of-the-art of cloud security*

4. Control of legal protection and applicable jurisdictions: *customers shielded against unlawful third countries law enforcement data access requests*
Industry responses to regulatory initiatives and customers needs (3)
CISPE definition of Digital Sovereignty for cloud

→ Multiple Overlaps with VMware Sovereign Cloud Provider Initiative Requirements

<table>
<thead>
<tr>
<th>Section</th>
<th>CISPE Digital Sovereignty</th>
<th>VMware Sovereign Cloud</th>
<th>Gaia-X Criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contractual governance</td>
<td>X</td>
<td>X</td>
<td>Criterion 1 to 4: The provider shall offer the ability to establish a legally binding act. This legally binding act shall be documented; governed by EUIEA/Member State law; legally binding for all</td>
</tr>
<tr>
<td>Transparency</td>
<td>X</td>
<td>X</td>
<td>Criterion 5: recovery, service interruptions and business continuity (e.g., by means of a service level agreement)</td>
</tr>
<tr>
<td>Transparency</td>
<td>X</td>
<td>X</td>
<td>Criterion 6 to 12: The provider shall ensure there are provisions governing the rights of the parties to use the service and any data therein, predictability of contracts; location of physical resources; subcontractors location; applicable jurisdictions</td>
</tr>
<tr>
<td>Transparency</td>
<td></td>
<td></td>
<td>Criterion 13: The provider shall adopt the Gaia-X trust framework, by which customers may verify provider’s compliance</td>
</tr>
<tr>
<td>European Control</td>
<td>X</td>
<td>X</td>
<td>Criterion 54: For label level 2, the provider shall provide the OPTION that all data are processed and stored exclusively in EU/EEA</td>
</tr>
<tr>
<td>European Control</td>
<td></td>
<td>X</td>
<td>Criterion 55: For label level 3, the provider shall Process AND STORE all data exclusively in the EU/EEA.</td>
</tr>
<tr>
<td>European Control</td>
<td></td>
<td>X</td>
<td>Criterion 56: If subcontractor is subject to legal obligations to transmit or disclose data based on a non-EU/EEA statutory order, the provider shall have verified safeguards in place to ensure that any access request is compliant with EU/EEA/Member State law</td>
</tr>
<tr>
<td>European Control</td>
<td></td>
<td>X</td>
<td>Criterion 58: For label level 3, shareholders in the provider not established in the EU shall not, directly, or indirectly, hold control of the CSP</td>
</tr>
<tr>
<td>European Control</td>
<td></td>
<td>X</td>
<td>Criterion 59: For label level 3, subcontractor owned or controlled directly or indirectly by non EU third-party shall push back any data access request other than per Article 47/48 GDPR</td>
</tr>
<tr>
<td>European Control</td>
<td></td>
<td>X</td>
<td>Criterion 60: For label level 3, the provider must guarantee continuous autonomy for all or part of the services it provides.</td>
</tr>
<tr>
<td>European Control</td>
<td></td>
<td>X</td>
<td>Criterion 61: The provider shall not access customer data unless authorised by the customer or when the access is in accordance with EU/EEA/member state law</td>
</tr>
<tr>
<td>Data Security and Compliance</td>
<td>X</td>
<td>X</td>
<td>Third Party Certifications ISO 27017, ISO 27018, CSA STAR, Cyber SecNumCloud, ENISA, IRAP, ISMAP, HIPAA, PCI, etc.</td>
</tr>
</tbody>
</table>
Industry responses to regulatory initiatives and customers needs (4)

CISPE definition of Digital Sovereignty for cloud: two key control specifications

1. Freedom of technological choice: to prevent Software lock-in, Cloud Providers shall comply with the Ten Principles of Fair Software Licensing (best practices) for Cloud Customers supported by a variety of customers and providers trade associations.

   **5 examples of unfair licensing practices**
   - Obligation to repurchase software applications when migrating to the cloud (Bring Your Own License - BYOL)
   - Repurchasing (additional) licenses and technical restrictions to move to a competing cloud infrastructure
   - Restrictions imposed on Virtual Desktop Infrastructure solutions

2. Control of resilience: Energy dependency - post Ukraine invasion

   - Technical tying between Microsoft 365 (Office) and OneDrive
   - Technical tying between Azure AD and Microsoft 365 and refusal to disclose interoperability information

**Climate Neutrality by 2030 with clear metrics and KPIs to deliver** -
- Improved Energy efficiency
- Use of Clean, Renewable energy
- Water conservation, Circular economy and Circular energy systems
Forward-looking perspectives

1. Legislative and Regulatory: Let the Dust Settle and anticipate new Legal Framework
2. Industry initiatives and customer demand: new market offerings; different needs
3. Drivers for change, incl. VMware sovereignty offering and Gaia-X Trust Framework
Thank You