Alain Fiocco
afiocco@af-insights.com

Digital Sovereignty

Independence, Control
Freedom of choice

https://www.ie.edu/uncover-ie/digital-sovereignty-master-in-public-policy/ IE University Digital Policy WP

Towards a Common Understanding of EU Digital Sovereignty European Commission, JRC Publication

Digital sovereignty is the capacity to control your digital destiny:
your infrastructure, software, standards and data, including how they are governed and under which jurisdiction they operate.

For organizations, it means controlling key dependencies: hardware, software, cloud services, data storage locations, access rights, contractual exposure to external providers and exposure to Extra-territorial laws and demands.

Four key pillars

- **Data Sovereignty:** Ensuring data storage, processing, and governance comply with local laws and national jurisdictions.
  such as EU's GDPR, Data Act, IA Act…etc…
- **Legal Sovereignty:** Guaranteeing that digital services and actors answer to domestic or regional laws rather than foreign laws or extraterritorial demands
  such as US's CLOUD Act, PATRIOT Act, FISA 702 or Chinese PIPL, NIL Article 7 & 14) …)
  or Foreign Executive Orders (aka "kill swich")
- **Operational Sovereignty:** Retaining administrative control, visibility, and key-management rights over Code, Applications, Systems and Cloud environments.
- **Technical/Infrastructure Sovereignty:** Building resilience by avoiding vendor lock-in, using open standards, and maintaining alternative options for critical hardware and software stacks.

Risk Matrix

It’s about Operational Control, External Technology Dependencies and Exposure to Extra-territorial demands

No Risk : Full Control, No External dependencies , no exposure
Low Risk : Full Control, Little dependencies, some legal exposure
Med Risk : Fair Operational Control but External Dependencies
High Risk : Weak Control, External Dependencies

} Mitigations ?

	DATA	LEGAL	OPERATION	TECHNOLOGY/INFRA
Controller/Owner				
Processor (if applicable)				
Combined Risk				

One have to evaluate the level of Risk he is ready to endure, relative to its own Business, Industry regulations and Customers

The Dilemma

You’re operating in a world where your data, infrastructure and algorithms can be shaped by rules you did not write and you have never been asked to comply with.

The European Commission, the OECD, the Weizenbaum Institute and the World Economic Forum all point to the same strategic issue:

Digital power concentrates quickly,
and dependencies accumulate quietly.

These dependencies reach far beyond the legal aspect.

Vendor's (or Service Provider's) Technical Lock-in put you at risk of changes in Vendor's Commercial T&C, Pricing Model changes, Technical Support policies or Product/Service End of Life

Vendor's or Service Provider's strategy evolution Examples

- Broadcom acquisition of VMware led to dramatic changes in product offering, forcing many customers to migrate to alternative solutions
- Microsoft Exchange Server perpetual license model EOS, led to mandatory migration to Subscription Edition or equivalent Cloud offering.
- Microsoft Skype perpetual on-prem license for business phased out, and has never been replaced by an on-prem equivalent, rather it forced migration to Team which is a cloud only service.
- Oracle Database perpetual license model evolved to include a mandatory support service of ~ 20% of the product price annually. Or a migration to OCP based DB service.

Specific Cloud issues

- Predicting montly cloud costs ?
  - Storage ; egress fees – API calls
  - Usage based services (Serverless, Auth/Directoy, Databases)
  - Observability – monitoring – Logs
- Cloud Stickiness = long term dependencies / balloning bills
  - Proprietary tools and services, Creating operational dependencies
  - Cloud Credits
  - Egress fee = “pay as you shrink” Business model

Are European Cloud the solution ?

Nowadays most public cloud services are available from EU alternatives

ex: OVHcloud, Scaleway, DT Cloud, IONOS, StackIT, ExoScale, UpCloud, InfoManiak …

- Balance between Service richness and velocity vs European Sovereignty
  - Unless specific needs, Service parity is always higher priority
- Local vs Global footprint can be a strong driver.
- Scale & Elasticity
  - Public Cloud promise of unlimited scale and elasticity (commission and decommission at will) require huge scalability of Cloud infrastructure.
- Are theses clouds really Technology independent ?
  - Underlying software infrastructure (Opensource DIY vs Buy)
  - Supply chain

Is Opensource the solution ?

Opensource is definitly key to the solution but there are several caveats

- Is the software independent of distribution/support
  (ie; Redhat, Suze, Canonical …) or in other words "can it be swapped"
- Are you not recreating dependencies on proprietary tools/features built around the opensource piece of code ?

"Free/Vanilla" opensource software can be complex to deploy, scale and maintain as it requires the deep technical expertize and capability.

However it would be my recommendation for EU Cloud providers, to fully control the software supply chain. as it is key to guarantee Sovereignty status.

- Some European cloud providers go one step further and do contribute in Opensource communities (OVHcloud Openstack, CNCF, IAM KeyClock), and even opensource their own specific code (ie; Manager, Bastion…) .
- That is generally a good sign of expertize and cloud operationnal control

Is Hybrid or Multi Cloud the solution ?

- This potentially includes an “on prem” or “Private” cloud component to the global enterprise cloud architecture.
- This provides a much better Operational control over data and applications, but add complexity
- The software infrastructure (ie; open or closed source) must be able to run in both public and private cloud environment.
- Remaining risk of Technology/Product dependencies

Call for action

Do NOT put your head in the sand ! This is too important

- Do your Risk assessment – put in place mitigation measures
- Evaluate (again ?) European Clouds alternatives
- Evaluate Multicloud with a European Cloud component and/or an on-prem component for the most critical data/processes

One have to evaluate the level of Risk he is ready to endure, relative to its own Business, Industry regulations and Customers