CoE DSC

Defining Cloud Sovereignty: Concepts, Risks and Decision Frameworks

Sophie van Baalen, Vera Irmak, Erik Langius,

Johan van der Geest, Björn Hakansson

Introduction

Cloud sovereignty has rapidly emerged as a critical topic at the intersection of technology, law, and public policy. As public and private organisations increasingly rely on cloud services for essential operations, questions of control, compliance, and independence have become central to digital strategy and risk management.

This document is intended to serve any organization that aims to manage the risk associated with a low level of cloud sovereignty. The following topics are addressed:

- How can cloud sovereignty be defined?
- What elements relate to this definition in what way?
- How can the level of cloud sovereignty be determined?
- Which frameworks exist for assessing cloud sovereignty?

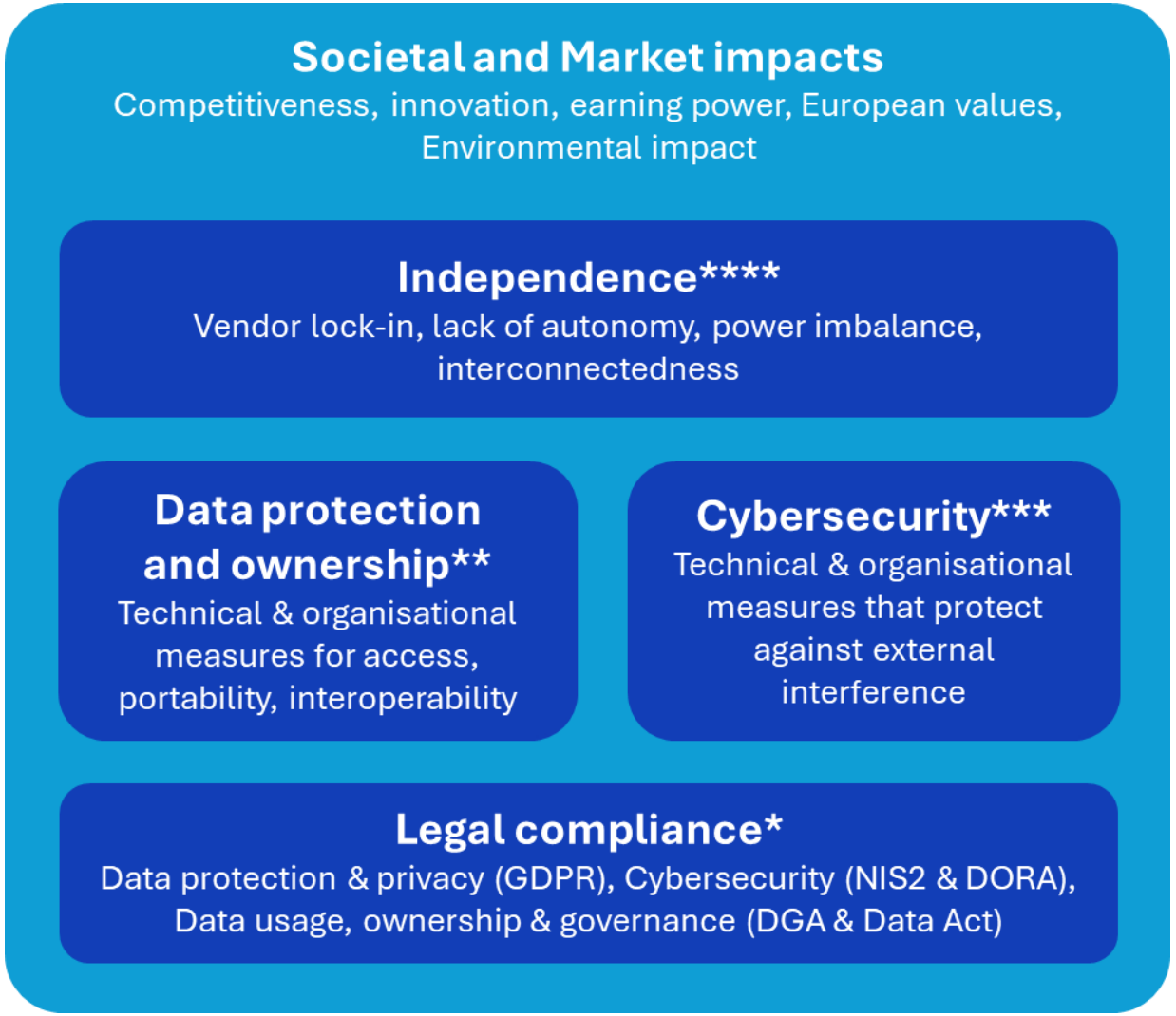
Content

CoE DSC

Elements of a definition of cloud sovereignty

In any definition of cloud sovereignty, various elements will play a key role. In this presentation we will mention some key elements and discuss the various degrees of sovereignty that are being discussed in the market.

Elements of a definition of Cloud Sovereignty



**** Under **independence** there is a need to look at several key dimensions, e.g., software independence, operational independence, supply chain independence and exclusion from foreign jurisdiction (such as, **protection from extraterritorial** (i.e. US) **laws**).

*** Technical and organizational measures regarding **cybersecurity** can be implemented as an additional layer to legal compliance. With these measures sovereignty is strengthened.

** Once Legal baseline obligations are fulfilled, organizations may implement additional technical and organizational measures related to **data protection.** These technical and organizational measures do not provide full sovereignty but provide an additional layer.

* **Legal compliance** forms the foundation of what organizations must have in place to meet the minimum requirements for cloud sovereignty. ***Compliance with applicable legal requirements represents the minimum threshold for cloud sovereignty, as a necessity but not sufficient condition for sovereignty.***

CoE DSC

Elements of cloud sovereignty

There is currently no widely supported definition of cloud sovereignty. For a definition, several elements need to be taken into account.

Legal compliance

Laws and regulations determine how data is governed, protected and accessed across jurisdictions. Compliance with laws prevent illegal exposure, regulate unauthorized access and safeguard confidentiality and integrity of data.

Data protection and ownership

Protection of data against external interference and preventing unsolicited, third-party access, beyond what is required by EU laws.

Entails control over (meta) data and being able to access and move the data when required. Concerns the data that is stored in data centres, data that is being processed and data that is being transferred from storage to be processed.

Cybersecurity

Protection of digital systems against direct threats to vital infrastructure (sabotage), theft of personal and other sensitive data or intellectual property by state actors targeting knowledge-intensive industries (economic espionage) and digital extortion, including ransomware attacks.

Economic, technical and geopolitical Independence

Can relate to sovereign states and to organisations using cloud services.

For states: protecting citizens' data and geopolitical leverage that other countries can gain when (vital) digital infrastructures depend on cloud service providers seated in other countries.

For organisations: interconnectedness between organizational processes and cloud services, vendor lock-in interruptions of services, poor interoperability, lack of freedom and transparency, business continuity.

Societal and Market impacts

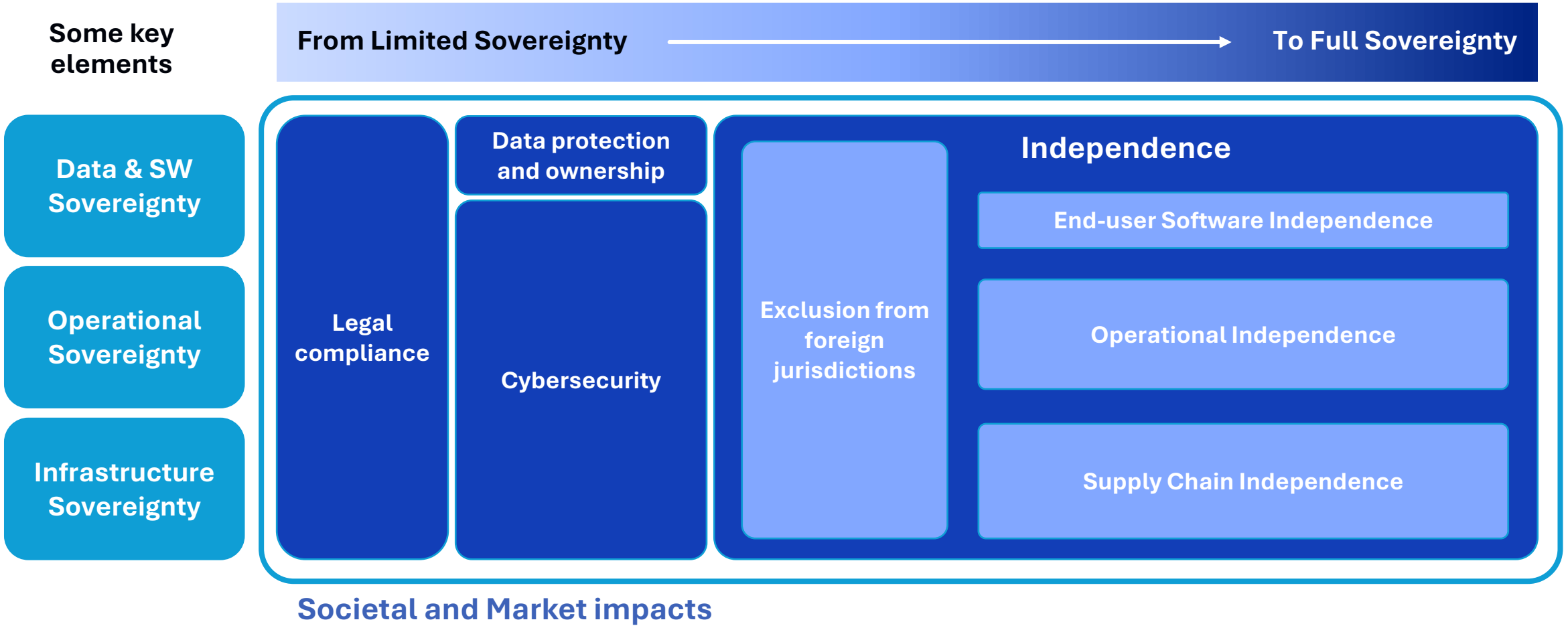
Indirect (and sometimes long term) impacts. Sovereignty increases demand for EU-based solution, increasing European competitiveness and innovation. Also increased grip on design, hence protection of European values as data protection, transparency, autonomy.

CoE DSC

Degrees of cloud sovereignty

Degrees of cloud sovereignty

The degrees of sovereignty that a user can look for in the cloud services they use or will use.



CoE DSC

Legal compliance

Plays a critical role in shaping and implementing cloud sovereignty and sets the **requirements** for *data governance, data protection* and *cross-border access.*

Five key regulations shaping how data is stored, accessed and protected in European cloud environments:

GDPR

Data protection & transfers

- Requires data protection by design: which supports sovereignty by design.
- Restricts personal data transfers outside EU/EEA.
- Enables auditability and transparency while helping to verify where and how data is processed.
- Requires technical measures to protect personal data.

Data Governance Act

Data sharing & intermediaries

- Prevents private monopolization of public data by private entities.
- Requires secure environments and controls for reuse, including restrictions on third-country access which is key for sovereignty protection.
- EU-level coordination for consistent cross-border controls.

Data Act

Portability & interoperability

- Eliminates vendor lock-in; mandates smooth migration.
- Enforces standard formats and interoperability interfaces.
- Guards against unlawful foreign data access.
- Boosts interoperability with enforcing standard data formats and interfaces.

NIS2 Directive

Cybersecurity for critical sectors

- Security-by-design obligations for cloud providers.
- Ensures cloud providers critical to society and economy are designated as essential entities and subject to stricter controls.
- Mandatory risk assessments & national incident coordination.
- National strategies required to boost cybersecurity.

DORA

Financial sector ICT resilience

- EU-level oversight of critical cloud providers in finance.
- Requires contracts in place to guarantee things like data portability and termination rights, which supports sovereignty by making sure institutions can move their data or exit in a controlled way.
- ICT risk management, testing & incident reporting required.

CoE DSC

Data protection & ownership: additions

includes the protection of data against unsolicited, third-party access, beyond what is required by EU laws.

ISO/IEC standard 27001

An international standard for information security. It provides a systematic approach to managing information security, with the aim of ensuring the confidentiality, availability, and integrity of information within the organisation. It specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

Other possible and organisational measures, e.g.,

- External Key Management
- Data boundary
- External encryption
- Location of data centres and processing in EU
- Internal policies describing data handling and security measures

CoE DSC

Cybersecurity: additions

includes the protection of digital systems against external interference beyond what is required by EU laws.

European Cybersecurity (EUCC)

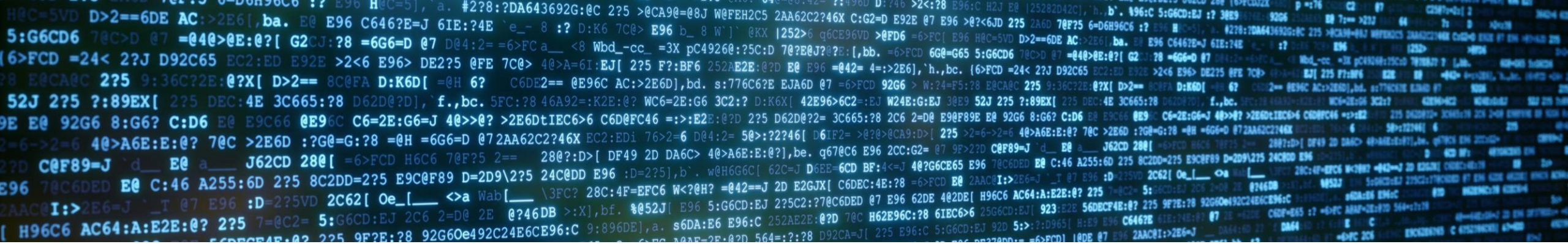
EUCC is a voluntary-based security scheme that allows ICT suppliers to go through an EU commonly understood assessment process to certify ICT products such as technological components (chips, smartcards), hardware and software.

European Cybersecurity Scheme for Cloud Services (EUCS)

EUCS looks into the of the cybersecurity of cloud services.

Other possible and organisational measures, e.g.

- National cybersecurity schemes, e.g. SecNumCloud, C5, ENS, etc.
- Trust Frameworks like e.g. Gaia-X



Independence

Includes measures on reducing critical dependencies from (non-EU) jurisdictions and companies.

Exclusion from foreign jurisdictions

Exclusion from extraterritorial laws like the US Cloud ACT or the FISA section 702.

End-user Software independence

Reducing dependencies in end-user software, e.g. by using Open-Source Software applications.

Operational independence

Reducing operational independence in e.g. personnel dependencies from non-EU actors.

Supply chain independence

Reducing dependencies in the infrastructure supply chain, e.g. from SW and HW used by non-EU providers

Independence

Exclusion from International jurisdiction

Extraterritorial laws that provide foreign access:

1. CLOUD Act

Customer data which is inquired for **law enforcement purposes**. This means that the US law enforcement has a **“probable cause”** to issue such **warrant**.

Circumstances:

A. EU company might fall under the US CLOUD Act if:
- It has a **U.S. legal presence** (subsidiary, branch, or office).
- It has “**sufficient contacts**” with the U.S.
for example, selling to U.S. customers, targeting U.S. users online, or using U.S.-based service providers.
- It is under control of a **U.S. parent company** (since the parent can compel data access).

B. The US might have a **personal jurisdiction** over a US Company, hence CLOUD Act applies, when:
- If the EU Entity actively targets U.S. consumers;
- If the EU Entity passively offers its products or services to U.S. - consumers (for example, by hosting a website that is generally available globally.

2. FISA Section 702

Used by U.S. intelligence agencies, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). Unlike the CLOUD Act,

The US Government officials **do not need a probable cause to access information, which might result into arbitrary and warrantless search.** FISA authorizes **targeted surveillance** of **non-U.S. persons located outside the U.S.**, even if their communications are stored or pass through servers located in the U.S.

CoE DSC

Independence

Q & A on US Jurisdiction

Question: When does a company fall under US jurisdiction, even if the company is a non-US Company operating outside of the US?

Answer: U.S. surveillance and data access laws are generally company-centric, not location-centric. What matters most is control over data, not where your company is incorporated or operates.

Scenario: NovaPay, a Dutch fintech processing EU payments, servers in Amsterdam. Follow the four situations:

01 Dutch company + Dutch cloud, no US ties — NO

NovaPay hosts on a Dutch provider with no US parent, staff, or investors. US surveillance laws have no reach. Data stays entirely under EU jurisdiction.

02 NovaPay migrates to AWS Frankfurt — YES

Servers are in Germany, but AWS is a US company. Under the CLOUD Act, US authorities can compel AWS to hand over data stored anywhere in the world.

03 Switches to 'EuroCloud GmbH': a US-owned German provider — YES

The data centre is German, but the parent company is American with admin access. Corporate ownership is enough to bring data under US jurisdiction.

04 NovaPay itself is acquired by a US firm — YES

Servers, staff, and data centre all stay in Amsterdam, so nothing moves. However, a US entity now controls the data. Control, not location, is what matters.

Only Situation 1 is outside US reach. The deciding factor in every other case is not geography, "it's who owns or controls the infrastructure".

CoE DSC

Independence

End-user software independence

Degrees of dependencies in end-user software, e.g. by using Open-Source Software.

1. General

Preventing dependence on end-user-software and applications from non-EU providers that are often vertically integrated with cloud platforms. This thus especially applies to SaaS applications as these are often bound to a vendor specific cloud platform.

2. Open Standards

The end-user software used complies with open standards that supports interoperability and enables portability.

3. Open-Source Software

Using Open-Source Software is a solution that may decrease dependencies and vendor lock-ins if the governance of the open-source software is not controlled by one single entity, and the developer community is large and active enough to maintain and develop the software. Open-source is not an automatic guarantee for independence, the way the source code is controlled and maintained is crucial to prevent future lock-ins.

CoE DSC

Independence

Operational independence

Degrees of dependencies in operations, e.g. when it comes to personnel,

1. General

The degrees of operational dependencies will often depend on personnel used or e.g. contractual flexibilities for changes in the operations, allowing to switch providers in case of need. Having clear procedures in the operations on how to deal with e.g. security threats or sovereignty challenges will increase the operational independence.

2. Personnel

Ensure that all key operational roles (i.e. software designers, system administrators, security officers and enterprise, business and other architects) are filled by EU-citizens. This will decrease the risk of foreign interference and increase the available of expertise and skills to operate EU-based cloud services.

CoE DSC

Independence

Supply chain independence

Degrees of dependencies in the supply chain, where software and hardware from other companies are provided.

1. Software and services

The dependencies risks can be reduced, starting with vital functionalities such as backup of important data or communication software, followed by a basic cloud stack architecture and ultimately using cloud alternatives that offer cloud services with no or limited dependencies on non-EU software and services.

Preventing dependence on software from non-EU providers includes solutions for orchestration, virtualisation, networking, or storage. This can also include prevention of additional financial implications, technical-operational impediments or other lock-in practices. Solutions that enable audit and inspection of source code could add to the independence.

2. Hardware and chips

Using non-EU hardware or chips is almost inevitable, but there are things you can do to reduce sovereignty risks; e.g. securing supply, service and maintenance from EU suppliers.

3. Other possible supply chain dependencies

Energy, water, etc. could also be subjects in the supply chain, but critical non-EU dependencies here are more unlikely.

CoE DSC

From Limited Sovereignty → **To Full Sovereignty**

Legal compliance, no additional measures	Legal compliance + data protection and cybersecurity measures	Legal compliance + data protection and cybersecurity measures + no foreign jurisdiction	Legal compliance + data protection and cybersecurity measures + no foreign jurisdiction + independency measures
Compliance to EU and national laws.	Compliance to EU and national laws.	Compliance to EU and national laws.	Compliance to EU and national laws.
	Additional security measures, e.g. • Compliance to ISO/IEC standard 27001 • External Key Management • Data boundary • External encryption • Location of data centres + data processing in EU	Additional security measures	Additional security measures
		Exclusion from foreign jurisdiction access.	Exclusion from foreign jurisdiction access.
			Exclusion from critical dependencies: • Interoperability • No critical dependencies on non-EU suppliers

Other sovereignty definitions and frameworks

Some examples

Some often-referred frameworks for cloud sovereignty

	DG-Digit 'Cloud Sovereignty Framework'	Dutch Cloud Community (DCC)	EuroStack 'buy European Framework'	DICTU	Gartner
Objective (as stated)	Framework for procurement of cloud for EU institutions, bodies, offices and agencies	Framework for accreditation on Digital Autonomy, especially on the cloud services.	Framework for procurement paradigm for digital services. Blueprint for EU regulations to decrease dependencies.	Instrument to systematically assess the sovereignty of cloud services for the national government (NL)	Defining three pillars of sovereignty to be used in dependency audits.
Number of criteria	Eight objectives, including strategic, legal, operational, and environmental, supply chain transparency, technological openness, security, and compliance to EU laws.	Three dimensions; Legal, Technical and Organisational, with in total 13 different criteria.	Four dimensions: Jurisdiction & Governance, Technical, Operational, Data & Economic sovereignty	Fifteen criteria over five dimensions: Juridical, Data&AI, Operational, Technological and Human	Three Aspects: Data sovereignty, Operational sovereignty and Technological sovereignty.
Weighting criteria or pass/ fail criteria	No pass/fail criterium; a weighted score will be calculated.	The basis level is defined by compliance with only the Legal criteria.	Minimal requirements and pass/fail criteria. Economic sovereignty is the final differentiator.	For each criterium a 1-5 soevereignty level with explicit definitions for each level	Sovereignty as a spectrum that typically involves trade-offs in cost, scalability, data survivability and functional depth.
Final outcome	Results in a Sovereignty Effectiveness Assurance Levels (SEALs), that weighs all objectives into a single score.	The result will be an audited accreditation based on the DCC criteria to offer full transparency.	Allows further comparison between cloud services that meet minimal sovereignty requirements.	1-5 score for each criteria. The highest score for each criteria in each dimension is the definition of "sovereign cloud provider".	Risk assessment scores as input to various business strategies.

Note: Other frameworks in the making are expected to be published soon from; European Alliance for Industrial Data, Edge and Cloud 'Cloud Sovereignty Profiler', Cloud Infrastructure Service Providers in Europe (CISPE), European Sovereign Tech Industry Alliance (ESTIA) and probably others.

Cloud and AI Development Act (CADA)

In June 2026 the European Commission adopted a proposal Cloud and AI Development Act (CADA)
It includes a four-tier sovereignty model that includes four Union Assurances levels, based on exposure to foreign interference and degree of EU control.

Level	Core idea	Key requirements
Level 1	EU-based cloud	EU provider, EU data by default, basic safeguards. Data is processed and stored in infrastructure located in the Union
Level 2	EU-operated cloud	Full EU data + operations, no external access, cybersecurity ≥ substantial. Providers must demonstrate independence from third countries and transparency over their software supply chain.
Level 3	EU-controlled cloud	All of the above + EU personnel, + limits on third-country ownership/control. The commission can recognize third-country providers
Level 4	Fully autonomous cloud	No third-country interference, EU-only stack, highest security (≥ high). Providers must have full transparency and control over their software supply chain.

Cybersecurity:
More details on frameworks and schemes

ENISA EUCC & EUCS

- **European Cybersecurity (EUCC)** is a voluntary-based security scheme.
  - Allows ICT suppliers to go through an EU commonly understood assessment process to certify ICT products such as technological components (chips, smartcards), hardware and software.
- **European Cybersecurity Scheme for Cloud Services (EUCS)** looks into the of the cybersecurity of cloud services.
  - ENISA and Commission initiative (started in March 2020) to create a harmonized cloud (instead of country specific → SecNumCloud, C5 and .
  - Could embed technical and organizational requirements relevant to “sovereign” cloud procurement.

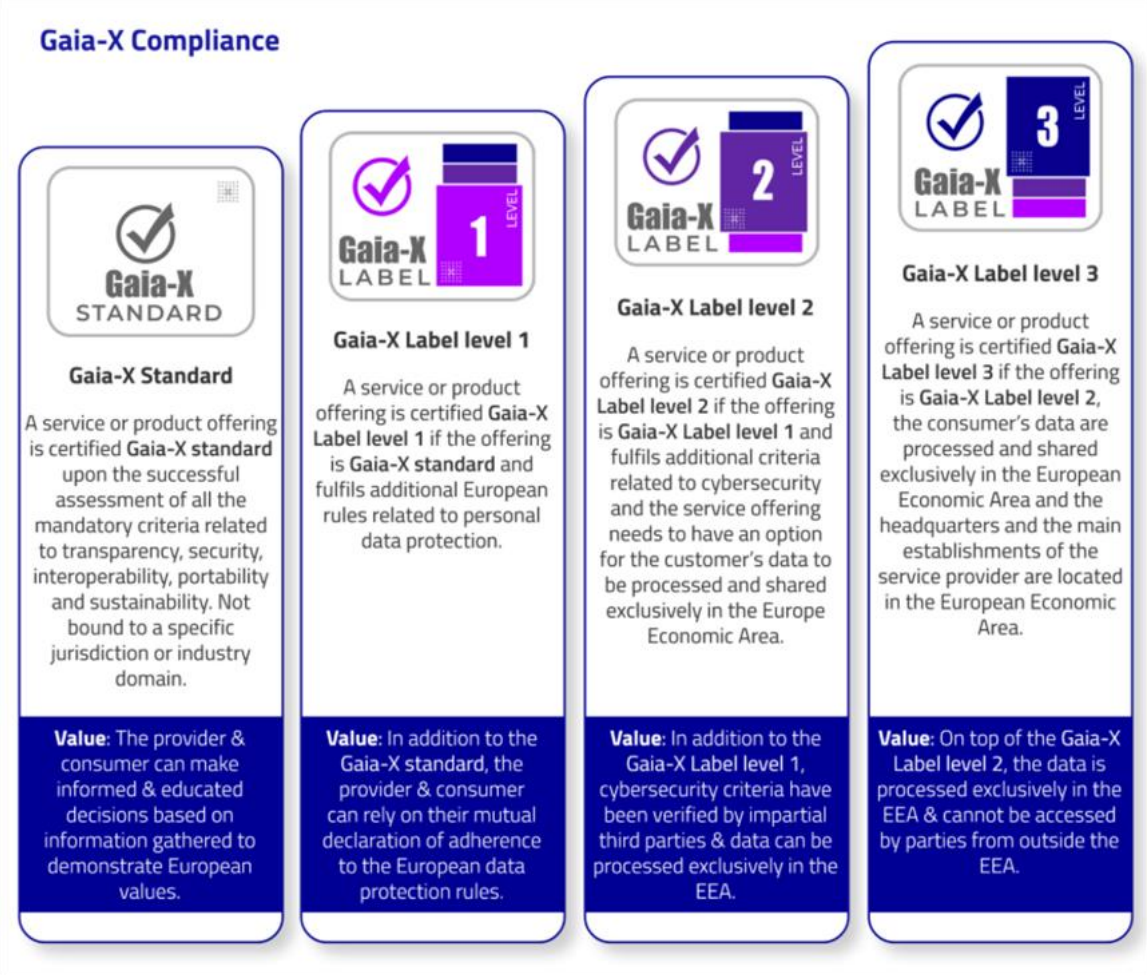
The EUCS scheme contains three (in an earlier draft it was four) different levels:

- **CS-EL1 Basic:** with a typical attack profile of one hacker with limited skills.
- **CS-EL2 Substantial:** for more business-critical data and systems.
- **CS-EL3 High:** for business-critical data and systems, or certain sectors like financial. Contains measurements against state-of-the-art cyber-attacks, including automated monitoring systems.
- The **CS-EL4 High+** was removed in later drafts.
  - Contained more specific requirements on where the data is geographically located (EU-only), comparable to the SecNumCloud requirements.

CoE DSC

Gaia-X

- In today's interconnected digital landscape, the secure, trustful and transparent exchange of data is essential for industries, innovation and growth. Trust is the prerequisite for the data economy and for the promise of data sovereignty, transparency and interoperability. Governments, organisations and individuals only share their data if they can expect the other participants to respect the policies and the rules.
- Gaia-X is creating the de facto standard aligned with EU values by developing a set of policies, rules, specifications and a verification framework
- With the innovative concept of Gaia-X Digital Clearing Houses (GXDCHs), the Gaia-X Framework is operationalised promoting decentralised data and cloud infrastructure, avoiding reliance on single points of control and avoiding vendor lock-in.
- At their core, GXDCHs serve as trusted intermediaries within the Gaia-X community, facilitating the seamless and secure flow of data between different entities.
- Gaia-X has defined a number of standard requirements at different levels that can be verified by the GXDCHs. On top of that, digital ecosystems may define their own additional labels, representing requirements that are specific to their particular ecosystem.



CoE DSC

National frameworks: SecNumCloud , C5, ENS

SecNumCloud (France), C5 (Germany) and ENS (Spain) are **national cybersecurity schemes for cloud services.**

Similarities between these schemes are that all three:

- Focus on data protection & cybersecurity (not primarily on sovereignty)
- Aligned with ISO 27001 standards (SecNumCloud and C5 require full ISO 27001 alignment) and focus on data protection and cybersecurity.
- Explicitly integrate GDPR compliance and are mandatory for public government use.

The scope of C5 and SecNumCloud is cloud services, while ENS is Public sector IT.

Differences are:

- **SecNumCloud** is the strictest on legal sovereignty and EU data residency.
- **C5** is the most modular, audit-focused, and explicit about customer responsibilities.
- **ENS** is the most prescriptive and mandatory for Spanish public sector (and its private suppliers), has tiered approach with three assurance levels (low, medium and high) depending on system sensitivity and a strong focus on traceability and authenticity.

This document is written by the following authors:
Sophie van Baalen, Vera Irmak, Johan van der Geest, Erik Langius and Bjorn Hakansson

We thank Claire Stolwijk and Peter Verkoulen for their support

For more information or requests, please contact:

info@CoE-DSC.nl

Sophie van Baalen
sophie.vanbaalen@tno.nl

Bjorn Hakansson
Bjorn.Hakansson@CoE-DSC.nl