euralarm

Guidance document on Criteria for European Sovereign Cloud

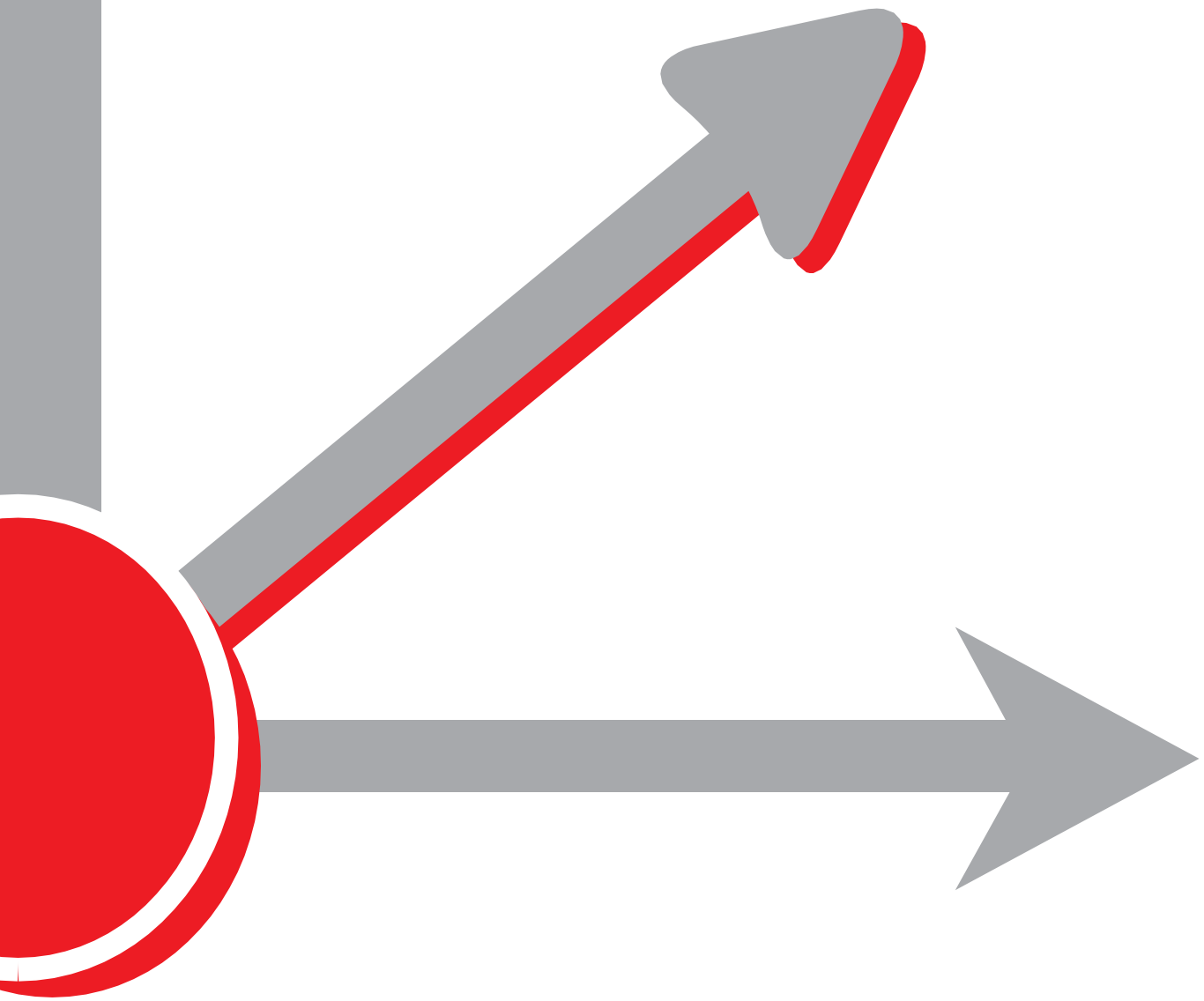

Table of Contents

Foreword

Body

Changes revision table			
Date	**Rev #**	**Paragraph / Page**	**Change**
6/2026			1st publication

DISCLAIMER

This document is intended solely for guidance of Euralarm members, and, where applicable, their members, on the state of affairs concerning its subject. Whilst every effort has been made to ensure its accuracy, readers should not rely upon its completeness or correctness, nor rely on it as legal interpretation. Euralarm will not be liable for the provision of any incorrect or incomplete information.

Note: The English version of this document is the approved Euralarm reference document.

About Euralarm

Euralarm represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm members are national associations and individual companies from across Europe.

Euralarm • Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

Criteria for European Sovereign Cloud

1. Introduction

Recourse to cloud technologies has dramatically increased in the last decade in all sectors of the society. Fire safety and physical security applications also make increasing use of that technology to improve the efficiency, performance and reliability of existing services and to offer new services to the users: alarm transmission using IP technology, remote access to the systems by the end-user and remote services on the systems for remote diagnostics, operations, updates and maintenance. Beyond those services, the computational power of cloud servers being by far higher than the one of microcontrollers and microprocessors used in the installed systems on site allows for sophisticated processing of large datasets with the objective of increasing the detection probability, reducing the false alarm rate and analysing large sets of video images.

In most cases, implementation of cloud computing requires contracting with an external cloud service provider (CSP). The affordable choices for such providers are limited to some hyperscalers allowing a worldwide deployment of the solutions. Proper contracting with a CSP needs careful assessment of the needed cloud environment (IaaS, PaaS, SaaS…), the legal criteria for the location of the servers and the distribution of the roles and responsibilities, including cybersecurity. Those aspects are dealt with in the Euralarm "Guideline on Contracting cloud services for secure remote access to alarm systems and for secure alarm transmission" published during the first quarter of 2025 in several languages.

Fire safety and physical security applications may imply the processing of data and images that are critical to the resilience of infrastructures or to the security of entities, governmental institutions or states. Such high-demanding users require reliable, high-performance and cybersecure applications and may also need the guarantee that the generated data are not accessible by foreign governments or actors. This is a challenge when using the cloud services of hyperscalers available on the market and so limits the opportunities of development of high-performance fire safety and physical security applications for institutional entities.

The keyword circulating over the last years and particularly in the today complex geopolitical context is "Sovereignty". The present fact sheet intends to guide the reader through the different facets of cloud sovereignty and guides the reader for his own risk assessment for identifying the sovereignty facets that can be expected by a customer. The result of the risk assessment should be that sovereignty requirements become traceable to business impact and compliance obligations, easier to justify to stakeholders and auditors, and—crucially—avoid locking the organization into costly architectures where the added sovereignty measures do not meaningfully reduce risk.

2. Abbreviations

CSP	cloud service provider
IaaS	infrastructure as a service
PaaS	platform as a service
SaaS	software as a service
SOC	security operations centre
GDPR	general data protection regulation
TOMS	technical and operational measures´ specification
ISO	international standardisation organisation
PAM	privileged access management
JIT	just in time

DNS	domain name system
PKI	public key infrastructure
HSM	hardware security module
HYOK	hold your own key
CA	certificate authority

3. Facets of cloud sovereignty

3.1 Introduction

Cloud sovereignty is usually described through several complementary facets that together capture who controls digital technologies, data and infrastructures, and to what end. The exact list varies by author. The present document makes the elaborates on the facets described in[1] and the sovereignty objectives of the Cloud Sovereignty Framework from the European Commission. More detailed descriptions can be found in the above-mentioned sources and in the C3A scheme developed by the German BSI and complementing the framework from the European Commission. This guidance intends to allow for better understanding of the key concepts.

3.2 Technological sovereignty

Technological Sovereignty is the independency to technologies preventing migration or reducing the availability. It is divided in 2 sub-parts:

- independency to non-European proprietary technologies: evaluation of the degree of openness, transparency, and independence in the underlying technological stack, ensuring European actors can interoperate, audit, and evolve solutions without lock-in to foreign proprietary systems; full independency is based on open source, open industry standards or generally available standardized technology (non-proprietary) and enables transparency and traceability of data processing and the software components used;
- European survivability: dependency on the availability of the connectivity.

Facet	General public cloud	European Technological Sovereign Cloud
independency to non-European proprietary technologies	Cloud providers usually offer proprietary technologies which are owned by non-European companies	Either: ▪ use of European proprietary technologies or which only offer better operational independence within Europe, or ▪ use of open solutions and standards, or ▪ transparency on dependency to non-European proprietary technologies (this is acknowledged as not fully technological sovereign but

[1] Katharina Cordes (plusserver) and Emmanuel Finance (CANCOM), "Sovereign cloud made in Germany", The European Sovereign Cloud Day, Brussels, June 2025.

		also almost unavoidable with the today available offer)
European survivability	Good regional and European availability, but it is part of global cloud structures	Stronger: sovereign clouds are designed to keep operating even if disconnected from the rest of the world, with European-only operations and regional separation.

3.3 Operational sovereignty

Operational Sovereignty is a measure of the practical ability of European actors to run, support, and evolve a technology independently of foreign control. It focuses on continuity of operations, skill availability, and resilience against external dependencies. It includes transparent control of operations, from provisioning and management of solutions and services to monitoring physical and digital access to infrastructure.

Facet	General public cloud	European Operational Sovereign Cloud
provisioning and management of solutions and services	Operations run as part of global cloud solutions, with potential dependencies outside of Europe.	Operations are designed to have no critical dependencies on non-European infrastructure.
monitoring physical and digital access to infrastructure	Global teams may be involved in operations and support depending on service and issue type.	Physical infrastructure is distinct and dedicated, with access restricted to qualified Europe-based staff.

3.4 Jurisdictional sovereignty

Jurisdictional Sovereignty is the evaluation of the legal environment, exposure to foreign authority, and enforceability of rights that govern the services of a technology provider. It determines the extent to which the services are anchored in European jurisdiction and insulated from external legal claims. It includes the operation in a self-chosen legal area (e.g. European Union) without the right to pass through from third legal areas (see Annex A for examples of legislations with an extraterritorial effect). The jurisdictional sovereignty facet is divided in 3 sub-parts:

- legal area where operational control of the cloud takes place;
- security model within the shared responsibility model;
- legal area where support and operations take place.

Facet	General public cloud	European Jurisdictional Sovereign Cloud
Operational control	Operated by Cloud-global teams with standard global governance	Operated under European-based governance and European personnel controls with independent governance structures

Security model	Standard Cloud-shared responsibility model with global security operations	Enhanced isolation, European-only access paths, dedicated Security Operations Centre (SOC) and stricter operational separation
Support and operations	Global support teams and global escalation paths	European-based support and operations with local leadership and personnel subject to European law

3.5 Data residency

Data residency is the requirement that data shall be stored within a specific geographical boundary, such as within a single country or region such as the European Union. For the requirement to store and process data locally, the user data needs to stay within the national boundary.

The level of requirements on data residency might be different or not applicable to data transfer if adequate protective measures are taken.

The residency requirements usually cover all kinds of data, but might be applied only to specific types of data, such as personal data (Name, location, E-Mail, IP-Addresses, images etc.)

The data residency requirements are usually defined in the ´security concept´ of the cloud-solution.

Facet	General public cloud	European Data residency Sovereign Cloud
Data residency	Data stored in chosen Cloud-Regions; metadata and operational data may cross regions depending on services.	Customer data and metadata remain located within Europe and isolated from other Cloud-Regions.

A consequence of Data residency is Data Sovereignty. It ensures complete power of disposal or self-determined control in the collection, storage, use and processing of own data.

Data sovereignty refers to the concept that data is under the control of the end-user and governed by regional or local law (e.g. EU Data Act, GDPR).

The end-user needs to be in control of his data through security and governance measures bound by the laws and general best practices of the jurisdictional location of the organisation.

Data sovereignty is achieved by administrative policies and technical controls that limit access to the data, the use, storage and retention times incl. deletion policies. This includes measures such as encryption, key management, access controls, and data governance.

While data residency ensures that data stays in a specified geographical location, data sovereignty makes sure that data adheres to the regulations of the country and region where the organisation is located.

The administrative policies and technical controls of a cloud application are usually defined in the ´Technical and Operational Measures´ specification (TOMS) including law enforcement access to data.

It is acknowledged that, due to the functioning of internet, data may flow across the borders of the designated jurisdiction, but the data are only processed within that jurisdiction. This implies that due to the way internet works, means need to be implemented to ensure that flowing critical data are protected while crossing the borders

of the designated jurisdiction.

Compliance with EU legislations (e.g. Data Act and GDPR) allows to ensure data sovereignty.

Facet	General public cloud	European Data Sovereign Cloud
Data sovereignty	Customer content can be kept in a chosen Region, but some cloud operations and metadata may still involve global systems, not necessarily located in the region.	Customer content and customer-created metadata are designed to stay within the European boundary, with stronger sovereignty controls.

3.6 Legal compliance

Legal compliance protects against unavailability of data and disruption of the services delivered by the cloud application due to lawsuits or prosecution.

Facet	General public cloud	European Sovereign Cloud
Legal compliance	Broad compliance portfolio (ISO, SOC, GDPR readiness) for many regulated workloads	Engineered to meet EU sovereignty frameworks and public-sector regulatory requirements: ▪ cloud contracts are governed by the law of an European country ▪ only European courts and other arbitration bodies have jurisdiction for disputes related to the contracts ▪ GDPR (Data Privacy describes the protection against the improper processing of personal data and the right to informational self-determination) ▪ Data Act

4. Risk-based approach to European cloud sovereignty

Cloud Sovereignty Framework from the European Commission proposes a rating mechanism that attributes a Sovereignty Effectiveness Assurance Levels (SEAL) to a particular cloud service for each of the sovereignty objectives. This rating is then complemented by a global sovereignty score. This quantitative approach is understandable in the context of the specific procurement procedure from the European Commission.

For the purpose of the present guidance document, a risk-based approach is proposed. The following table provides for each facet the primary risk to be covered, the key requirements for satisfying that facet and typical

controls or architecture patterns satisfying the key requirements[2]. That table can then be used to identify which facets of sovereignty needs to be satisfied for a particular customer or a fire safety or security application.

Facet	Primary risk	Key requirements	Typical controls / architecture patterns
Technological Sovereignty			
— independency to non-European proprietary technologies	Sanctions/export controls, provider class outage, forced migration	reduce concentration risk, ability to exit within defined time	Portability architecture; tested exit plans; data exportability; multi-cloud/dual-stack where justified
— European survivability	Cross-border connectivity shut down (or severe international routing disruption). Provider control-plane dependency used to enforce policy or interrupt service	Cloud infrastructure should keep operating/decrypting even if provider is pressured : Data and service remain usable inside the country/region without relying on cross-border dependencies	Local endpoints - same as for Data residency; in-country DNS resolution; local break-glass; local monitoring/ops; ensure critical dependencies don't hairpin cross-border (identity, PKI, time, logging, update repos). Customer-managed keys/HSM; external key mgmt / HYOK patterns; independent identity; minimize foreign-controlled control-plane dependencies
Operational Sovereignty	Unwanted actors gain privileged access from outside jurisdiction (support, admins)	Only authorized in-region personnel can perform sensitive ops; actions are auditable	PAM + JIT; dual control; strict support residency; tamper-evident logs; customer notification/ approval for sensitive access
Jurisdictional Sovereignty			
— operational control	Extraterritorial orders (e.g., CLOUD Act) forces cloud providers to disclose EU customer data without notice to EU stakeholders	Provider/operator is structurally shielded from conflicting foreign legal compulsion (End-to-end service delivery without reliance on foreign parent control/support systems)	Dedicated sovereign cloud with separate operational model; in-region-only ops; localized core services (DNS/CA/ control plane); strict subcontractor chain; legally separated environment designed for sovereign operation; independent governance. Cloud provider independent certification /label like SecNumCloud in France
— security model	cross-region or cross-tenant spillover solution outage or data leak due to absence of adequate incident response	Operational separation which removes the risk that support, maintenance, or incident-response access is exercised from outside the EU	Enhanced isolation, EU-only access paths, dedicated Security Operations Centre (SOC) and stricter operational separation
— support and operations	Operational outage or leakage of data due to unavailability of or leakage from the support/DevOps teams due to local law enforcement	The support and operations organization ensures that key operations can be performed within county/region.	At least a minimum necessary support and operations organization is Europe-located with local leadership and personnel subject to EU law. Emergency plans are available to restore full Europe-based support in case of foreign jurisdictional action.

[2] More detailed questions can be found in section 4 of the Cloud Sovereignty Framework of the European Commission and strict criteria to satisfy those sovereignty objectives can be found in the C3A scheme from the German BSI.

Data residency and sovereignty	Violate regulatory/ contractual data location constraint, third-country data processing risk	Data at rest (incl. backups, logs/telemetry as scoped) stays in-country/region. Demonstrate where processing occurs and supplementary measures when outside of Europe.	Region pinning; residency for backups/logs; data classification & placement rules; clear location transparency Contractual "no third-country processing" where required; encryption with robust key governance; technical + contractual supplementary measures; transfer assessments, see Schrem II landmark case
Legal compliance	Risk of legal actions (lawsuits, prosecutions) due to violation of applicable EU laws	Respect of all applicable regulations from county/region - ex : GDPR, EU Data act, EU AI act ...	Regulatory compliance is integrated in the processes of the cloud solution provider in auditable way.

5. Conclusions

Digital services create substantial value for Fire Safety and Security systems operations by improving transparency, supporting faster troubleshooting, reducing false alarms, and enabling capabilities that cannot be delivered by on-premises systems alone. At the same time, these benefits require data and processes to be hosted in remote cloud environments.

As outlined in this guidance, cloud sovereignty is not an all-or-nothing question. The appropriate model should be selected through a risk-based and proportionate approach that takes into account the customer's protection needs, the business value of the service, and the additional cost and complexity of stronger sovereignty measures. For example, true immunity from extraterritorial orders and a fully cloud-vendor-agnostic architecture come with a very high price tag. These measures should therefore be carefully balanced against the business value created and the real impact and likelihood of a potential sovereignty infringement.

Annex A: US CLOUD Act and other relevant foreign acts

The most commented data legislation with an effect in Europe is the US CLOUD Act (Clarifying Lawful Overseas Use of Data Act). According to[3], it asserts that U.S. data and communication companies must provide stored data for a customer or subscriber on any server they own and operate when requested by warrant, but provides mechanisms for the companies or the courts to reject or challenge these if they believe the request violates the privacy rights of the foreign country the data is stored in. It also provides an alternative and expedited route to Mutual Legal Assistance Treaty (MLATs) through "executive agreements"; the executive branch is given the ability to enter into bi-lateral agreements with foreign countries to provide requested data related to its citizens in a streamlined manner, as long as the Attorney General, with concurrence of the Secretary of State, agree that the foreign country has sufficient protections in place to restrict access to data related to United States citizens. The first such agreement was with the United Kingdom.

Knowing that most of providers of generic cloud services, commonly named as hyperscalers, are US-based companies or subsidiaries of US-based companies, the US CLOUD Act is of primary importance when discussing the facet of jurisdictional sovereignty. However, it is also worth noting that, according to[4], data legislation with an extraterritorial effect is increasingly being introduced outside the EU and the US, from Australia and South Africa to India and China. The latter is relevant because hardware and software (as well as other digital services) increasingly come from China. One of those Chinese laws with an extra-territorial effect is the Data Security Law. The DSL is, to some extent, a response to the US CLOUD-Act and regulates the processing of data in China and data or information outside China when it is "relevant to China's national security or other social interests."

According to[4], the analysis shows that, in the case of the US CLOUD-Act alone, it is challenging for a data owner or controller to determine whether a service or service provider is subject to extraterritorial influences from non-European legislation. This is not only determined by various factors at the supplier but also by the supply chain and the companies that are active in it. This requires thorough risk analyses and realising that it is impossible to exclude extraterritorial influences completely. As the use of extraterritorial legislation continues to grow internationally – and it is expected that this will undoubtedly be the case for legislation in the digital field in the coming years – the complexity in the practical application and compliance of such (European) legislation will only increase. Organisations and companies must always ask themselves against which extraterritorial legal regimes, and therefore countries, they will and can arm themselves and what that means in terms of supplier choice and the use of additional control measures. In terms of compliance, however, it also means that companies and organisations are, in fact, less able to guarantee or ensure that the information they process is sufficiently protected against viewing by foreign, non-European, powers.

[3] Wikipedia page of the CLOUD Act
[4] "Dutch National Cyber Security Centre": How the CLOUD-Act works in data storage in Europe

Publication date: 8 June 2026

Euralarm
Gubelstrasse 22
CH-6301 Zug (Switzerland)

Swiss Commercial Registration No: CHE-222.522.503

E secretariat@euralarm.org
W www.euralarm.org