
Designing Europe's Digital Future

The foundations for a European cloud
and AI infrastructure.

aruba.it

Si-
c
o
n
a

Aruba's European Positioning

This paper was written with a clear purpose: to explain how Aruba understands its role within the European digital ecosystem.

The company's positioning is built around the concept of a European operator, not an independent one: an identity that reflects a concrete geographic, regulatory, and institutional affiliation, rather than an aspiration to technological isolation, a concept often associated with the idea of self-sufficiency. While this notion carries real weight in political and regulatory debate, it brings with it implications of autonomy, self-reliance, and independence that do not reflect Aruba's vision.

Choosing Aruba means operating within a European ecosystem by choice:

infrastructure rooted in EU territory, governance aligned with the Community regulatory framework, and personnel subject exclusively to Italian and European law.

This is not about shutting the door on global innovation, but about integrating it on foundations that are transparent, governable, and resilient. This is the difference between a European positioning , one that speaks of **belonging, responsibility, and trust**, and a self-sufficiency-driven positioning, which speaks of exclusive control and independence from external systems.

The pages that follow examine the infrastructural, regulatory, and architectural foundations of this model.

When cloud computing first entered the enterprise landscape, organizations approached it with a mixture of enthusiasm and caution. The promise was compelling: scalable infrastructure, rapid deployment of services, and the ability to innovate without the constraints of traditional IT environments. Yet even in those early stages, most organizations did not immediately migrate their entire digital estate to the cloud.

Instead, a pragmatic architectural model emerged. Core systems, those supporting sensitive data, critical processes, or strategic intellectual property, typically remained on-premise, within infrastructures fully controlled by the organization. At the same time, more peripheral workloads such as development environments, testing platforms, collaboration tools, and non-critical applications began moving to public cloud environments to benefit from their agility and scalability.

This balance between control and flexibility became one of the defining characteristics of the first phase of cloud adoption.

Today, a similar dynamic is re-emerging as organizations integrate artificial intelligence into their operational environments. After several years dominated by experimentation and proof-of-concept initiatives, AI technologies are now moving into production, beginning to influence core processes across enterprises and public administrations. As this transition unfolds, the question is no longer simply which models or tools to adopt. Organizations are now reassessing the infrastructural foundations on which these technologies operate.

Sensitive data, strategic applications, and critical decision-making processes increasingly require environments that can guarantee governance, jurisdictional clarity, and operational transparency. At the same time, hyperscale platforms continue to provide unmatched capabilities in terms of computational power, advanced AI services, and global scalability.

What is emerging is a renewed search for balance, echoing the early cloud era but within a far more complex digital landscape. Concepts such as **digital governance**, **data residency**, and **workload repatriation** are not signs of retreat from the cloud model. They reflect a growing need to balance the agility of hyperscale infrastructures with the governance, control and long-term technological agency required for strategic digital assets.

Organizations are also adopting pragmatic frameworks such as minimum viable sovereignty, focusing on the most critical controls across infrastructure, data, and applications in order to balance governance requirements with operational feasibility.

For European enterprises and public administrations, this is no longer a purely technical or legal debate. **"Data localization" is becoming part of digital strategy itself**, shaping how organizations approach competitiveness, resilience, sourcing choices, operational continuity, and the adoption of AI at scale.

As digital systems become more central to business and public value creation, the question of who governs the underlying foundations becomes inseparable from how organizations **innovate** and **evolve** over time.

Summary

01 The foundations of Europe's Digital Future	3
02 Compliance: the Regulatory Backbone	6
03 Resilience, interoperability and open infrastructure	10
04 Strategic Control and the Compute–Compliance Paradox	13

CHAPTER 01

The foundations of Europe's Digital Future

Digital data governance is often framed as a political objective, yet in practice it is first and foremost an architectural condition. It emerges from a layered system of controls that determines who governs digital infrastructure, where data resides, and how technological systems evolve over time. Rather than an abstract principle or a policy slogan, sovereignty is the outcome of concrete design choices across multiple levels of the digital stack.

Digital sovereignty can therefore be understood as a question of foundations. As digital environments scale, across data, applications, AI models, and interconnected services, the quality and responsiveness of those foundations become decisive. Governance, resilience, and jurisdictional clarity do not emerge at the surface of the stack; they depend on how the underlying infrastructure has been designed and governed from the outset.

The first layer is **physical infrastructure**. Data centers represent the foundational element of data residency because they determine where data and services physically reside, the starting point from which governance, oversight, and jurisdictional clarity can be established.

When infrastructures are designed, operated, and governed within the European regulatory environment, organizations gain clarity over applicable legal frameworks and operational oversight. Without this, digital autonomy risks remaining largely theoretical. Strategic control, in practical terms, begins with the infrastructure that hosts digital workloads.

From this base emerges the second layer: **cloud architecture**. Over the past decade, the dominant paradigm has shifted from centralized infrastructure models toward hybrid and multi-cloud architectures. These models allow organizations to combine the scalability and innovation of hyperscale environments with infrastructures that remain under regional or organizational governance. Hybrid architectures become the mechanism through which organizations reconcile agility with the governance requirements of strategic workloads.

A third layer concerns **data governance**: the ability to determine where data is stored, under which jurisdiction it is processed, and how it moves across infrastructures. In the European context, data residency and traceability are not merely operational considerations; they are core requirements tied to privacy protection, cybersecurity obligations, and regulatory accountability.

Artificial Intelligence adds a critical layer, AI infrastructure and governance, that elevates these strategic questions. AI systems rely on large datasets, specialized compute like GPUs, and seamless data flows across training, inference, and operations. As organizations embed AI in core processes, the supporting infrastructure shapes their technological path, with factors like data proximity, GPU capacity access, and data flow transparency determining compliance and governance success.

This layered perspective also reflects a broader transformation in how digital infrastructure is perceived. Data centers are no longer simply facilities that host servers; they have become strategic assets where multiple dimensions intersect: energy availability, high-performance connectivity, security frameworks, operational resilience and regulatory considerations.

In Aruba, the sustainability of digital infrastructure is a strategic factor. Modern European data centers increasingly rely on renewable energy sources and high-efficiency cooling systems, ensuring that the growth of AI and cloud workloads does not come at the expense of environmental responsibility. The infrastructures capable of sustaining advanced Artificial Intelligence workloads are also those that support long-term digital autonomy.

For organizations operating within the European regulatory and economic landscape, to know where your data is hosted does not imply isolation from global innovation. It reflects the ability to integrate external technological capabilities within infrastructures that remain transparent, governable, and resilient over time.

European governance, in this sense, is less about limiting choice and more about preserving the structural conditions that allow organizations to retain agency over their digital evolution.

The strategic relevance of digital infrastructure is also shaped by its energy, industrial, and regulatory dimensions. Artificial intelligence workloads are highly compute-intensive and closely tied to the availability of reliable and sustainable energy.

At the same time, control over digital infrastructure has become an element of economic competitiveness and technological resilience.

Ultimately, **European infrastructure is not only about protecting what is critical today, but about preserving the conditions that allow organizations to adapt to what will become critical tomorrow.**

Why it matters for businesses and public administrations to keep their data in Europe

The importance of a European governance becomes particularly clear when viewed from the perspective of enterprises and public administrations.

For **companies**, it is increasingly linked to the ability to retain architectural control over strategic workloads, protect sensitive data, diversify sourcing strategies, and avoid structural dependencies that could limit future choices. It also brings greater predictability across compliance, costs, operational continuity, and infrastructure evolution, especially as AI systems become embedded in core business processes.

Ultimately, digital data residency and digital governance become competitive differentiators, enabling organizations to respond more flexibly to market changes, regulatory requirements, and strategic opportunities.

For **public administrations**, the stakes are even higher. Control on digital systems involves the protection of citizen data, the continuity of essential services, and the assurance that critical digital infrastructures operate within clear jurisdictional and security frameworks.

In both cases, it is not a feature to be added downstream, but a foundational condition that shapes whether innovation can be adopted with sufficient **trust, control**, and **resilience**.

For this reason, organizations increasingly look for partners able to interpret sovereignty not as an isolated compliance requirement, but as an **infrastructure model built around governable foundations**.

EU perspective: the dimensions of digital sovereignty

Jurisdictional & strategic sovereignty:

control over where infrastructure operates and under which legal frameworks digital services are governed.

Data & AI sovereignty:

ability to manage data location, access, and usage, ensuring traceability, protection, and compliant AI deployment.

Technological sovereignty:

use of open standards, interoperability, and composable architectures to avoid dependency on closed ecosystems.

Ecosystem & operational sovereignty:

resilient supply chains, trusted providers, and sustainable infrastructure supporting long-term digital autonomy.

CHAPTER 02

Compliance: the Regulatory Backbone

If data residency is ultimately an architectural question, compliance provides the regulatory framework that shapes how that architecture is designed.

Over the past decade, the European Union has built one of the most comprehensive governance systems for the digital economy, introducing rules that address data protection, cybersecurity, operational resilience, and, more recently, AI.

From this perspective, the European Union does not treat sovereignty as a single principle, but as a set of interdependent dimensions: jurisdictional control, data governance, technological transparency, operational resilience, and ecosystem-level trust.

The emerging European framework therefore extends beyond data protection alone. It connects infrastructure location, cybersecurity obligations, interoperability, and accountability into a broader model for governing digital systems.

At the foundation of this regulatory landscape lies the **General Data Protection Regulation (GDPR)**, which established a global benchmark for the protection of personal data and the accountability of organizations that process it. GDPR introduced principles such as data minimization, purpose limitation, and transparency, concepts that now influence not only legal compliance but also the design of digital infrastructures.

More recently, the **Artificial Intelligence Act** has extended this governance framework into the domain of algorithmic systems. It introduces a risk-based approach to AI deployment, imposing specific obligations on systems considered high-risk and requiring organizations to demonstrate transparency, traceability, and human oversight. As AI begins to influence operational decision-making across sectors, the infrastructure hosting these systems must support mechanisms for monitoring, auditing, and governance.

Alongside these initiatives, the **Data Act** aims to strengthen data portability and access rights across the digital ecosystem, reducing barriers between platforms and enabling organizations to retain greater control over the data they generate.

At the same time, cybersecurity frameworks such as **NIS2** and the **Cyber Resilience Act** introduce stricter obligations for the protection of digital infrastructures and connected products, while **DORA** sets specific requirements for operational resilience in the financial sector.

Taken together, these initiatives indicate that European sovereignty is not defined only by where data resides, but by whether organizations can demonstrate control over the infrastructures, standards, supply chains, and governance mechanisms on which digital services depend.

Compliance can no longer be treated as a downstream requirement; it needs to be embedded directly into the design of digital infrastructure.

Infrastructure decisions, where data is stored, how systems are interconnected, and which environments host sensitive workloads, ultimately determine whether organizations can meet regulatory obligations.

Artificial intelligence further intensifies this dynamic. AI systems rely on complex pipelines of data collection, training, and deployment, often operating across distributed environments. Ensuring compliance in these contexts requires infrastructures capable of guaranteeing traceability, security, and jurisdictional clarity from the outset. Regulatory frameworks, therefore, are not merely constraints on technological development; they increasingly shape how digital ecosystems are built to remain sustainable and trustworthy over time.

Many organizations are now moving toward risk-based European strategies, focusing first on the most sensitive layers of their digital stack.

Approaches such as **minimum viable sovereignty** reflect this shift, encouraging organizations to prioritize controls where sovereignty risks are highest, typically across infrastructure, data governance, and critical applications, while maintaining operational flexibility elsewhere.

Aruba's QC3 Qualification

A concrete example of how infrastructure control translates into operational standards can be found in the qualification framework defined by Italy's **National Cybersecurity Agency (ACN)** for cloud services used by the Public Administration.

The framework classifies public sector data and services into three levels, **Ordinary**, **Critical**, and **Strategic**, based on the potential impact of their compromise on national security, economic stability, and citizens' well-being.

Strategic data includes services linked to the **National Cybersecurity Perimeter (PSNC)**, essential national services under the NIS framework, and systems processing highly sensitive or large-scale citizen data.

Critical services, while less sensitive than strategic ones, still support key public functions such as healthcare and other essential local services.

For cloud providers, these classifications translate into progressively more stringent technical and governance requirements. Even at the ordinary level, providers must demonstrate strong guarantees in areas such as service quality, interoperability, portability, and observability.

As the classification moves toward critical and strategic levels, additional obligations emerge, including data localization within the European Union, encryption management, such as customer control over encryption keys and the integration of dedicated HSM solutions, enhanced monitoring capabilities, and more rigorous security validation processes.

Operational resilience is also a core requirement. Infrastructure supporting critical services must include redundant

backup systems and regular disaster recovery exercises, while strategic environments introduce further obligations related to software lifecycle management, supply chain security, and formal reporting procedures toward authorities.

Within this framework, **Aruba's QC3 qualification** represents the highest level of trust for infrastructure capable of hosting the most sensitive public administration workloads. While primarily designed to ensure the protection of strategic public data, this qualification also reflects a broader capability: operating infrastructures that meet some of the most demanding standards in security, resilience, and governance across Europe.

Aruba's QC3 qualification is further extended through the Consip Accordo Quadro, enabling public administrations to access European IaaS and PaaS services directly, without additional procurement procedures, and thereby accelerating digital transformation initiatives.

For enterprises navigating increasingly complex regulatory and security environments, such certifications provide a clear reference point. They demonstrate that European infrastructure is not only a policy objective but also a practical operational capability, one that allows organizations to combine regulatory compliance, technological performance, and long-term digital resilience.

Qualifications such as QC3 therefore do more than certify compliance with public sector requirements. They illustrate what it means, in practice, to build and govern digital foundations capable of supporting sovereignty by design, where security, jurisdictional control, resilience, and operational trust are embedded directly into the infrastructure.

EVIDENCE OF ARUBA'S SOVEREIGN CLOUD CREDENTIALS

ACN QC3 qualification

Aruba Cloud is qualified at ACN QC3 level under the Italian National Cybersecurity Agency's framework, enabling cloud services for strategic public-administration workloads and Consip framework access.

Open-standards leadership

Aruba is a Gaia-X Board Member and a 1st (founding) member of CISPE, and an active contributor to SECA (Sovereign European Cloud API) and open infrastructure projects such as Liqo and ArubaKube, keeping European cloud reversible and interoperable.

Italian-personnel-under-Italian-law operating model

Aruba operations are run by Italian personnel under Italian and EU law, removing extraterritorial legal exposure (US CLOUD Act, foreign discovery orders) from the trust perimeter.

+300K

ITALIAN CAMPUS
FOOTPRINT (SQM)

80MW

IT POWER CAPACITY
OF ITALIAN CAMPUSES

+16M

USERS

8

COMPANY-OWNED
DATA CENTERS ACROSS EU

evidence box

CHAPTER 03

Resilience, interoperability and open infrastructure

If control begins with infrastructure and is shaped by regulatory frameworks, its effectiveness ultimately depends on the architectural principles that guide how digital systems are built.

Among these, resilience, interoperability, and openness have become central to ensuring that digital infrastructures remain adaptable, trustworthy, and sustainable over time.

Resilience is the first of these pillars. As digital services increasingly underpin essential economic and public functions, infrastructure must be able to maintain continuity even under adverse conditions.

Multi-region architectures, where workloads operate across geographically distributed data centers, are now a fundamental design requirement. They allow organizations to implement robust disaster recovery strategies, redundancy mechanisms, and operational

failover, ensuring that critical services remain available even in the face of technical failures or external disruptions.

Resilience alone, however, is not enough to guarantee strategic control and data governance. Interoperability is equally essential. Over the past decade, many organizations have learned that relying on a single infrastructure ecosystem can create structural dependencies that limit their ability to adapt. Interoperable environments, increasingly deployed through hybrid cloud architectures built on standardized interfaces and open APIs, allow workloads and data to move across infrastructures without excessive friction.

Initiatives such as **SECA (Sovereign European Cloud API)**, an industry-led European standard initiated by providers including Aruba, IONOS, and Dynamo to deliver open,

interoperable cloud management APIs compliant with EU regulatory frameworks, advancing EuroStack convergence and Data Act implementation, and open-source projects like Liqo illustrate how standardized orchestration layers can support multi-provider architectures, enabling organizations to combine hyperscale services with regional infrastructures while maintaining operational visibility and control.

Within this context, **ArubaKube, Aruba's center of excellence for research, development, and innovation in cloud-native technologies and open-source projects, plays a key role.**

By contributing directly to the evolution of Liqo, ArubaKube advances a practical model based on open source, interoperability, and cloud-native innovation, helping organizations design more flexible, resilient, and future-ready multi-cluster environments.

Control is shaped not only by the infrastructure an organization uses directly, but also by the standards, interfaces, supply chains, and governance models that connect providers, platforms, and partners. Composability and openness are therefore not just technical characteristics; they are essential for reducing dependency and preserving strategic optionality over time.

Closely linked to interoperability is the role of open-source technologies. Open-source components have become foundational to modern cloud environments, offering transparency into how systems function and enabling collaborative innovation across the broader technology ecosystem. For organizations focused on long-term governance,

open-source frameworks provide an additional layer of assurance: they reduce dependency on proprietary technologies and allow infrastructures to evolve without being constrained by opaque implementation models.

Artificial Intelligence further reinforces the importance of these principles. AI workloads require significant computational capacity, particularly specialized GPU resources used for training and inference tasks.

Hosting these workloads within infrastructures that remain close to sensitive datasets, and within trusted jurisdictional environments, becomes increasingly important as organizations integrate AI into operational systems.

The availability of compute capacity must therefore be balanced with governance, latency requirements, and data protection obligations.

Another concept gaining relevance in infrastructure strategy is **architectural reversibility**. Digital environments should not only be resilient and interoperable; they should also allow organizations to adjust their technological trajectory over time. The ability to migrate workloads, integrate new providers, or adapt infrastructure models without structural disruption ensures that decisions made today do not become constraints tomorrow.

Taken together, resilience, interoperability, and openness form the operational backbone of European digital infrastructure. They enable organizations to benefit from global technological innovation while preserving the flexibility, transparency, and governance needed to maintain long-term digital autonomy.

A European sovereign-by-design cloud provider

Within this evolving landscape, Aruba's role is best understood not simply as that of a cloud vendor, but as an infrastructure enabler of European digital sovereignty built into the foundations of digital environments from the outset, through infrastructure operated within European jurisdiction, resilient data center capacity, open and interoperable architectures, and governance models aligned with regulatory accountability.

This positioning is reinforced by Aruba's active role within European digital ecosystems, including initiatives such as SECA and Gaia-X, which contribute to the development of interoperable, standards-based, and trusted digital infrastructures.

This model is grounded in direct ownership and operational control of the underlying infrastructure, within a governance framework that is entirely European.

In practical terms, **a sovereign-by-design approach does not imply the creation of isolated environments. It means enabling organizations to combine innovation, compliance, resilience, and long-term control.**

Sovereignty is therefore not a feature layered on top of infrastructure, but a structural property of how that infrastructure is conceived, governed, and evolved. It also relies on operational autonomy: the ability to manage infrastructure, services, networks, and compliance processes directly, without structural dependence on third parties.

Although the reference regulatory framework is defined at the EU level, for many Italian organizations the localization of infrastructure in Italy provides an additional layer of clarity and trust, particularly in public administration and highly regulated sectors, where jurisdictional simplicity, supply-chain

control, and local qualification frameworks remain key.

This jurisdictional proximity extends to the human layer of infrastructure management.

Operational control is also a function of who manages the systems: personnel subject exclusively to Italian and European law ensures that legal accountability and technical control remain fully aligned, closing a gap that purely technical governance measures cannot address.

For organizations, this translates into practical advantages: greater control over infrastructure choices, clearer compliance conditions, stronger portability, more predictable operating models, and a partner able to support European requirements across the broader IT supply chain.

CHAPTER 04

Strategic Control and the Compute–Compliance Paradox

As Artificial Intelligence moves from experimentation to operational deployment, organizations are discovering that the real challenge of AI adoption lies not only in algorithms or models, but in the infrastructures that support them.

The transition from proof-of-concept initiatives to production systems raises deeper questions about governance, control, and long-term sustainability. Artificial Intelligence is becoming a revealing test of the digital architectures on which modern economies increasingly depend.

At the heart of this transformation is the concept of **digital agency**. For enterprises and public institutions alike, the ability to adopt advanced technologies must be matched by the capacity to govern them, to determine where data resides, how systems evolve, and under which jurisdiction critical workloads operate.

Digital agency reflects the ability to integrate global technological innovation while maintaining control over the structural conditions that enable it.

This challenge is particularly evident in what can be described as the **Compute-Compliance paradox**.

On one side, Artificial Intelligence requires unprecedented levels of computational capacity. Training and operating modern AI models demands specialized infrastructure, high-performance connectivity, and increasingly energy-intensive data center environments.

On the other, the European regulatory landscape places growing emphasis on data protection, cybersecurity, algorithmic transparency, and operational accountability.

If these two forces evolve independently, organizations risk being caught between competing imperatives: access to large-scale compute resources and the need to comply with demanding governance frameworks. Resolving this tension requires infrastructures capable of aligning both dimensions, providing the performance needed for advanced AI systems while operating within environments that ensure transparency, security, and jurisdictional clarity.

This is where sovereign digital infrastructure becomes critical. Infrastructure rooted within the European ecosystem can turn regulatory requirements into a design principle. By embedding compliance, resilience, and governance directly into digital architectures, organizations can innovate without losing control over their technological trajectory.

Artificial intelligence is more than a technological breakthrough; it is the first large-scale stress test of Europe's digital infrastructure model. The infrastructures that support AI, data centers, cloud architectures, data governance frameworks, and compliance mechanisms, will determine whether organizations can harness innovation while retaining the ability to shape their own digital future.

For many organizations, build a European digital infrastructure will not mean redesigning their entire digital estate from scratch. It will mean identifying the **minimum set of controls** needed to preserve control across the most strategic layers of their infrastructure. When these foundations are established early, they reduce the long-term uncertainty associated with technological dependence, regulatory change, and infrastructure lock-in, minimizing the need for future workload repatriation down the line. Sovereignty, in this sense, does not only mitigate risk; it expands the room for maneuver, allowing organizations to adopt future innovations without being constrained by past decisions.

Ultimately, control in the digital age is not about limiting technological choice. It is about building the foundations that preserve the ability to choose and to adapt over time. When designed around control, resilience, interoperability, and compliance from the outset, these foundations reduce uncertainty and turn sovereignty into an enabling condition for future innovation.

Digital governance, in this sense, is not a constraint on transformation, but one of its most important preconditions.

About Aruba

Aruba, founded in 1994, is Italy's Cloud Champion and one of Europe's leading providers of digital infrastructures and platforms based on proprietary assets. The company designs and manages the entire technology stack: from the design and construction of data centers to cloud platforms, from trust and cybersecurity services to connectivity and software solutions that support digital strategies and AI-based applications.

With entirely Italian capital, Aruba serves 16 million users from over 100 countries and operates an infrastructure distributed across 8 data centers, hosting thousands of customers' IT infrastructures.



Copyright © Aruba. All rights reserved.

Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it