Digital Sovereignty in Europe

CRONOS EUROPA

Table of content

Introduction

Digital sovereignty is rapidly becoming a defining theme for organisations across Europe.

Driven by regulatory pressure, geopolitical shifts, and an increasing need for control over data and technology, it is moving from an abstract concept to a practical priority. Yet in many cases, the conversation remains fragmented, often reduced to infrastructure choices or cloud providers.

At Cronos Europa, we see this differently.

For over 20 years, we have been supporting European institutions at the crossroads of communication, IT and digital services. As a privately owned organisation and part of De Cronos Groep, we combine local expertise with a broad ecosystem of specialised companies to address complex digital challenges in a European context.

We believe sovereignty is not a single decision, but a layered and evolving discipline. It spans how data is managed, how systems are operated, which technologies are used, and how organisations build the capabilities to remain in control over time.

In this magazine, we bring together a series of perspectives that explore this topic from different angles. From infrastructure and cloud architecture to information management, AI, security, and governance, each article highlights how sovereignty can be translated into concrete, operational choices.

This is not a closed or exhaustive view.

Digital sovereignty is a dynamic and continuously evolving domain. We will continue to share new insights and perspectives in the coming months, and we remain available to support you in navigating this journey.

Digital Sovereignty in Europe: why control requires more than infrastructure

As Europe accelerates its push towards digital sovereignty, the conversation is moving from ambition to execution.

Sovereign Tech Europe, organised by Forum Europe, brings together policymakers, industry leaders, and technology experts to explore how sovereignty can be operationalised across the European landscape.

As a partner of the event, Cronos Europa actively contributes to this conversation, with multiple experts engaged across different domains and areas of expertise.

This broader dialogue reflects the growing need to translate sovereignty into practical, operational choices across organisations.

In this context, we take a step back to look at a fundamental question.

What does digital sovereignty really mean in practice?

"Sovereignty is not a single checkbox. Most organisations are further from control than they realise."

What does digital sovereignty mean in practice?

Digital sovereignty is the ability of an organisation to retain control over its data, systems, technology choices, and digital capabilities.

In practice, this goes beyond infrastructure. It requires organisations to understand where control sits across their entire technology stack and how dependencies affect their ability to act.

A key misconception is that sovereignty can be achieved through a single decision. In reality, it is a layered discipline.

Ruben describes it as a four-layer model:

- control over data
- control over operations
- control over technology
- control over internal digital capabilities

Each of these layers addresses a different dimension of sovereignty. Focusing on only one creates an incomplete and potentially misleading sense of control.

Why is infrastructure-only sovereignty not enough?

Many vendors position "European hosting" as a solution to sovereignty.

While data residency is important, it is also the most visible and often the easiest layer to address. It does not automatically guarantee control over how systems operate, how technology evolves, or how decisions are made.

For example, organisations may store their data in Europe while still relying on external providers for operations, proprietary platforms for core functionality, or external expertise for critical decisions.

In such cases, sovereignty is partial.

True sovereignty requires organisations to understand and manage dependencies across all layers, not only where data is stored.

Why is portability becoming a first principle for European organisations?

As organisations become more aware of their dependencies, portability is emerging as a key principle.

Portability means the ability to move workloads, data, and systems across environments without being locked into a single provider or ecosystem.

This is particularly relevant in a European context, where organisations need to balance regulatory requirements, operational resilience, and long-term flexibility.

Without portability, even well-designed architectures can become constrained over time. Decisions that optimise for short-term efficiency may limit future options.

Portability therefore becomes a way to maintain strategic control, even in complex and evolving environments.

Where do organisations struggle today?

One of the main challenges is what Ruben describes as the integration gap.

European organisations have access to a growing ecosystem of sovereign technologies. However, these solutions are often fragmented.

Bringing them together into a coherent, operational stack remains difficult.

As a result, organisations may have individual components that support sovereignty, but lack an integrated approach that connects data, operations, technology, and capabilities.

This gap is not primarily technical. It is architectural and organisational. It requires clear choices, alignment across teams, and a long-term view on how systems evolve.

How can organisations move from fragmented initiatives to real sovereignty?

Moving towards digital sovereignty requires a structured and deliberate approach.

It starts with understanding which layer of sovereignty matters most for the organisation. For some, this may be data jurisdiction. For others, operational independence or control over technology choices.

From there, organisations need to define how the different layers interact and where dependencies exist.

This often involves reassessing existing architectures, identifying critical dependencies, introducing portability, and building internal capabilities over time.

> **"The organisations that will succeed are those that understand which layer matters most to them, while maintaining a clear plan across all four."**

Why the window for European sovereignty is now

The current European landscape creates a unique moment.

Regulatory frameworks, public sector initiatives, and market dynamics are aligning around the need for greater control, transparency, and resilience.

At the same time, organisations are increasingly aware of the limitations of existing dependency models.

This combination creates an opportunity.

Organisations that act now can shape their architecture, capabilities, and partnerships in a way that supports long-term control. Those that delay may find themselves constrained by decisions that are difficult to reverse.

Within Cronos Europa, we see digital sovereignty as a practical discipline. Together with our ecosystem, we support organisations in translating strategy into operational reality across all layers of their stack.

Sovereign AI in Europe: how organisations can balance innovation, control and compliance

Artificial intelligence is rapidly becoming a central pillar of digital transformation across Europe.

From public sector organisations to private enterprises, AI is being deployed to improve decision-making, automate processes, and unlock new value from data.

At the same time, the rise of AI introduces new questions around control.

Where is data processed?

Who has access to models and outputs?

And how can organisations ensure that AI systems remain compliant with European regulations?

Within Cronos Europa's Sovereign Tech series, AI represents one of the most dynamic and complex domains where innovation and sovereignty intersect.

We spoke with Jorge De Corte, Managing Partner at ReBatch, a sister company within De Cronos Groep, to explore what sovereign AI means in practice.

> "AI creates value through data and models. Sovereignty determines who remains in control of both."

What is sovereign AI and why does it matter in Europe?

Sovereign AI refers to the ability of organisations to develop, deploy, and operate AI systems while retaining control over their data, models, and infrastructure.

This includes where data is stored and processed, how models are accessed, which providers and platforms are involved, and how systems comply with regulatory frameworks.

In a European context, this is particularly relevant.

Organisations must navigate a complex regulatory landscape, including GDPR and the EU AI Act, while ensuring that sensitive data and intellectual property remain protected.

At the same time, reliance on external AI providers can introduce new dependencies, particularly when models are accessed through proprietary APIs or hosted outside European jurisdictions.

Sovereign AI therefore becomes a way to balance innovation with control.

How can organisations adopt AI without losing control?

One of the main challenges in AI adoption is the speed at which organisations move from experimentation to production.

Many teams start with easily accessible tools and APIs, often provided by large hyperscalers.

While this accelerates development, it can also introduce dependencies early in the process.

Over time, these dependencies become harder to reverse.

A more deliberate approach starts with understanding where data flows, which models are used, and how systems are integrated into existing architectures.

This allows organisations to make conscious choices about where control is required and where flexibility is acceptable.

In practice, this often leads to hybrid approaches.

Some AI workloads may rely on external services, while others are deployed in more controlled environments, depending on sensitivity, compliance requirements, and strategic importance.

How do data, models and infrastructure shape AI sovereignty?

AI sovereignty is not defined by a single component.

It emerges from the combination of data, models, and infrastructure.

Data sovereignty ensures that sensitive information remains within controlled environments and complies with European regulations.

Model sovereignty focuses on control over how models are trained, accessed, and adapted. This includes avoiding lock-in through proprietary APIs and ensuring transparency in how models operate.

Infrastructure sovereignty determines where AI workloads run and under which conditions they are managed.

Organisations that align these three layers are better positioned to retain control while still benefiting from AI capabilities.

What are the main challenges organisations face today?

One of the main challenges is the trade-off between speed and control.

AI tools are becoming increasingly accessible, making it easy to build prototypes and deploy solutions quickly.

However, this ease of use can obscure underlying dependencies.

Another challenge is regulatory complexity.

European organisations must ensure that AI systems comply with evolving frameworks, which requires a clear understanding of how data and models are used.

Finally, there is the challenge of capability.

Building sovereign AI requires not only technology, but also expertise in data management, model governance, and infrastructure design.

How to get started with sovereign AI in practice

For organisations looking to take the first steps towards sovereign AI, the key is to start in a structured and pragmatic way.

This typically begins with mapping existing AI use cases, understanding where data flows, and identifying which workloads fall within regulatory scope.

From there, organisations can define their sovereignty requirements, select appropriate models and infrastructure, and gradually build governance and monitoring capabilities.

Rather than aiming for a complete transformation, most organisations benefit from a phased approach.

Starting with a limited number of use cases allows teams to validate choices, build internal expertise, and scale with confidence.

It does not have to be expensive either.

Sovereign AI does not require a large budget or a dedicated infrastructure team. Open-source models can run locally or on European cloud platforms without licence fees. European cloud providers offer pay-as-you-go pricing comparable to the large hyperscalers. And through the EU's AI Factories initiative, compute capacity is now accessible to startups and SMEs at reduced cost. A practical first step is often as simple as moving one workload to a European hosting environment, or replacing a proprietary API with an open-source alternative. The investment is minimal. The control you gain is significant.

From strategy to execution

Sovereign AI is not about limiting innovation.

It is about ensuring that innovation remains aligned with control, compliance, and long-term flexibility.

Organisations that take a structured approach to AI, understand their dependencies, and design for control from the start are better positioned to scale sustainably.

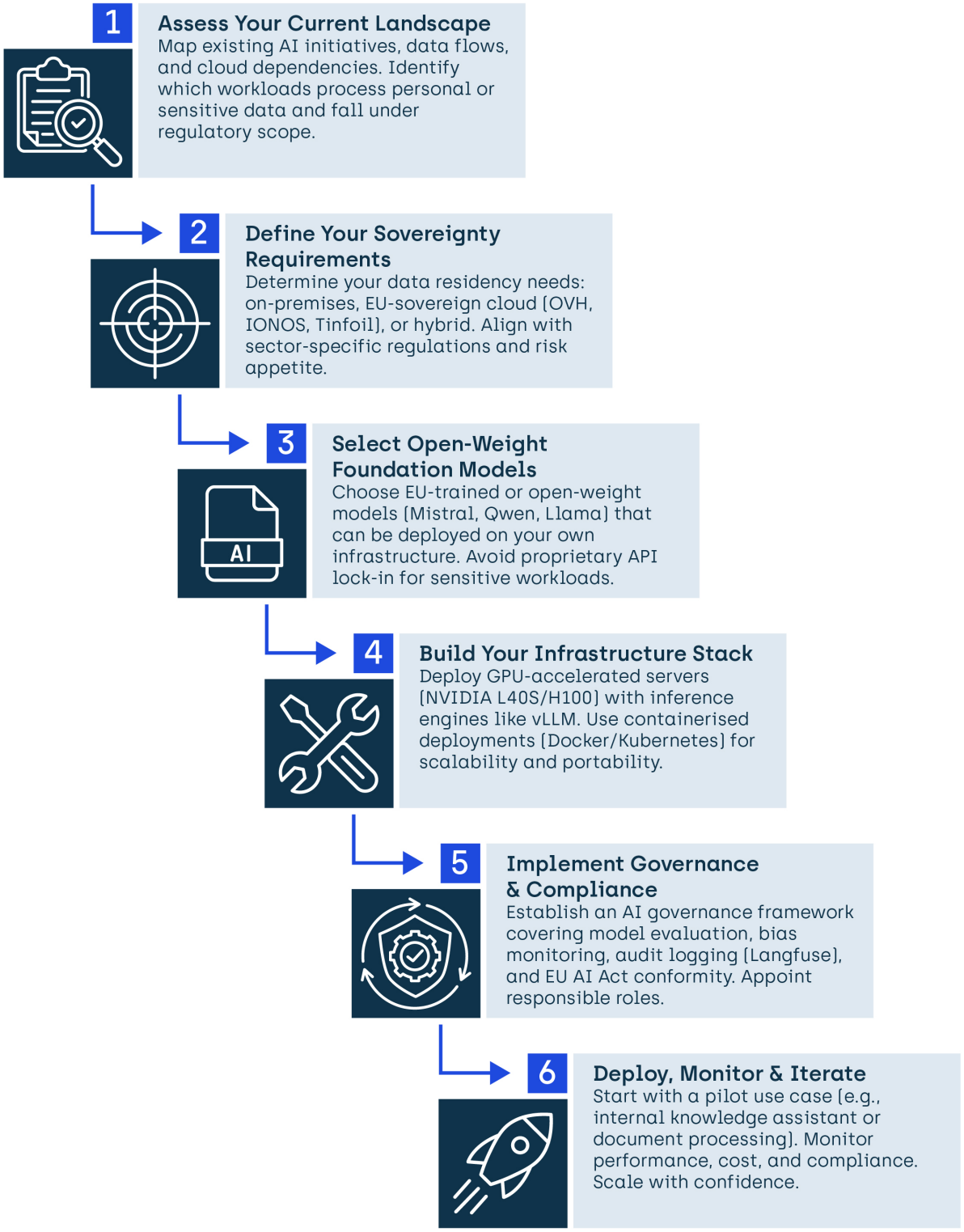
To support this transition, we have summarised a practical step-by-step approach in the accompanying overview.

Within Cronos Europa, we see sovereign AI as a key component of digital sovereignty. Together with partners such as Rebatch, we support organisations in designing AI strategies that balance innovation with control.

WHY SOVEREIGN AI?

European organisations face increasing pressure to maintain control over their data, comply with evolving regulations (GDPR, EU AI Act, NIS2), and reduce dependency on non-EU cloud providers. Sovereign AI ensures your data never leaves European jurisdiction, your AI systems meet regulatory requirements by design, and your organisation retains full control over models, infrastructure, and intellectual property.

6 STEPS TO GET STARTED



6 STEPS TO GET STARTED

	GDPR	EU AI Act	NIS2 Directive	Data Act
Impact on AI Deployment	Personal data must remain within EU boundaries. Data processing agreements with non-EU providers carry transfer risks.	Risk-based classification of AI systems. High-risk systems require transparency, human oversight, and conformity assessments.	Critical infrastructure and essential services must meet strict cybersecurity requirements, including AI systems in scope.	Rules on data access and sharing. Organisations must ensure data portability and interoperability without vendor lock-in.

COMMON PITFALLS TO AVOID

Treating sovereignty as just a hosting decision
It encompasses models, data pipelines, governance, and vendor agreements – not only where servers are located.

Ignoring model selection until deployment
Not all open models support your languages or meet your quality bar. Benchmark early with your actual data.

Defaulting to US hyperscaler APIs for convenience
Even with EU regions, CLOUD Act and FISA 702 create legal exposure. Evaluate the full legal chain.

Skipping governance for "just a PoC"
PoCs with real data are in regulatory scope. Start governance from day one, even if lightweight.

QUICK-START CHECKLIST

- [ ] Inventory all AI workloads and classify by risk level (EU AI Act).
- [ ] Map personal data flows and identify GDPR exposure.
- [ ] Evaluate current cloud provider contracts for data residency clauses.
- [ ] Select 1–2 pilot use cases with clear business value.
- [ ] Choose open-weight models suited for your languages and domain.
- [ ] Provision EU-sovereign infrastructure (cloud or on-prem).
- [ ] Deploy observability stack (logging, tracing, PII detection).
- [ ] Establish AI governance roles and escalation procedures.
- [ ] Run a conformity pre-assessment against EU AI Act requirements.
- [ ] Document everything – transparency is a regulatory requirement.

Sovereign Cybersecurity in Europe: how to reduce dependency while maintaining security and interoperability

Cybersecurity is often framed as a technical challenge. In reality, it is increasingly becoming a question of dependency.

European organisations rely heavily on external platforms, tooling, and security ecosystems. While these solutions offer scale and efficiency, they also introduce a structural question.

What happens when critical security capabilities are no longer under your control?

Within Europe's broader push for digital sovereignty, cybersecurity is emerging as a key domain where dependency needs to be understood and managed.

We spoke with Wouter Decruy, Managing Partner at ACEN, a sister company within De Cronos Groep, to explore how organisations can approach this challenge in practice.

> "The challenge is not to eliminate dependency, but to understand where it matters and how to manage it."

Why is dependency on cybersecurity ecosystems becoming a concern in Europe?

Over the past decade, organisations have adopted increasingly integrated security platforms.

Detection, monitoring, identity, and response capabilities are often bundled within a limited number of ecosystems. This creates real operational value, but only when those ecosystems operate transparently, within a trusted context, and with full visibility for the organisations they serve.

Dependency can limit visibility into how systems operate. It can reduce flexibility in adapting architectures. And it can create constraints when regulatory, operational, or geopolitical conditions change.

At the same time, European initiatives are placing greater emphasis on control, resilience, and accountability. This creates a tension between efficiency and sovereignty.

How can organisations reduce dependency without compromising security?

Reducing dependency does not mean abandoning existing technologies.

Instead, organisations need to take a more deliberate approach to how security capabilities are structured.

This starts with understanding where critical dependencies exist. Not all components have the same impact. Some can be externalised without risk, while others require stronger control.

From there, organisations can introduce architectural choices that increase flexibility. This may include separating detection from response, and ensuring that data and decision-making remain accessible.

The objective is not to replace one system with another, but to regain optionality.

What role does interoperability play in sovereign cybersecurity?

Interoperability is often discussed in terms of data exchange, but it is equally relevant in cybersecurity.

Organisations need the ability to integrate different tools, platforms, and capabilities without being locked into a single vendor ecosystem.

This is particularly important in Europe, where collaboration across institutions and Member States is essential.

A sovereign approach to cybersecurity therefore requires architectures that support interoperability, both technically and operationally.

This ensures that organisations can evolve their security landscape over time, rather than being constrained by past decisions.

How sovereign cybersecurity supports resilience in Europe

Sovereign cybersecurity is not about isolation. It is about resilience.

Organisations that understand and manage their dependencies are better positioned to adapt to change, respond to incidents, and maintain control over their security posture.

Within Cronos Europa, we see cybersecurity as a strategic layer of sovereignty. Together with partners such as ACEN, we support organisations in designing security models that balance efficiency, interoperability, and control.

Sovereign Cloud in Europe: how DevOps and open architectures enable control without sacrificing innovation

Cloud adoption across Europe has largely been shaped by convenience.

Hyperscalers offer a smooth developer experience, deeply integrated services, and a low barrier to entry. For many organisations, this has enabled rapid development and faster time to market.

That convenience is real, and for many use cases, it still makes sense.

However, the trade-off is not innovation itself, but how easily organisations can build and operate their environments. European cloud approaches, based on more modular building blocks, often require a more deliberate setup, but can offer greater flexibility in how solutions are designed.

At the same time, this convenience introduces a structural dependency.

Managed services, proprietary tooling, and tightly integrated platforms make development easier, but they can also make it more difficult to move, adapt, or operate independently across environments. In a context where geopolitical dynamics and regulatory pressure are evolving, this dependency becomes an important architectural consideration.

Within Cronos Europa's Sovereign Tech series, cloud and DevOps represent a critical layer where organisations must balance ease of use with long-term control, while preserving the flexibility to design and evolve their architecture over time.

We spoke with Kilian Niemegeerts from FlowFactor, a sister company within De Cronos Groep, to explore what sovereign cloud means in practice and how organisations can design for both flexibility and autonomy.

> "The question is not whether cloud convenience is useful. It is when that convenience starts limiting your ability to choose and move across environments."

What does sovereign cloud mean in practice for European organisations?

Sovereign cloud is often associated with data residency. In practice, it is broader.

It is not only about where data is stored, but also about how systems are operated, which technologies are used, and how dependent an organisation becomes on specific providers.

Sovereignty therefore spans multiple dimensions, from data control and operational autonomy to technology choices and long-term flexibility.

For organisations, the key question is where control is critical and where flexibility can remain.

For some, the priority is regulatory compliance. For others, it is operational autonomy. In most cases, it is a combination of both.

How can organisations design a cloud strategy that balances innovation and autonomy?

Working with a European cloud provider often involves a more deliberate approach compared to pre-integrated hyperscaler environments.

Instead of relying on pre-bundled services, organisations make more explicit architectural choices: what runs where, who manages it, and how components interact.

This approach, often based on open standards, enables greater flexibility and makes it easier to move across environments. At the same time, it requires stronger platform and infrastructure expertise to design and operate these environments effectively.

A practical starting point is an impact analysis. Which services are you running today, how do they translate into a European cloud context, and where does sovereignty actually matter?

The goal is not to replace hyperscalers entirely, but to understand where a different approach adds value. A heatmap of applications helps prioritise where sovereign infrastructure makes the most impact.

How do DevOps and cloud-native architectures enable sovereign infrastructure?

Cloud-native architectures, when designed deliberately, are inherently portable.

Technologies such as Kubernetes and open source deployment tools allow workloads to run consistently across environments. This makes where workloads run a configuration choice rather than a migration challenge.

DevOps practices reinforce this.

Infrastructure as code and open tooling ensure environments remain reproducible and transferable.

However, this only works when it is intentional.

Organisations that rely heavily on proprietary services may find it more difficult to move across platforms over time.

Designing around open standards can increase flexibility and portability, but requires more deliberate architectural choices, as well as stronger platform and infrastructure expertise.

Resilience and portability are not by-products. They are the result of deliberate architectural choices.

What are the most common misconceptions about sovereign cloud?

One of the most common misconceptions is that storing data in Europe automatically guarantees sovereignty.

In reality, sovereignty is about maintaining the freedom to decide where data and workloads are placed, when they can be moved, and maintaining clear visibility and control over who has access and under which conditions.

Another misconception is that a full migration is required.

Most organisations benefit from a phased approach, starting with the workloads where sovereignty matters most.

Sovereign cloud is also often perceived as more expensive.

In practice, European cloud providers can, in certain scenarios, be more cost-effective than hyperscalers on a like-for-like basis. Even when factoring in platform expertise, total cost often remains competitive, particularly when organisations regain control over infrastructure.

How sovereign cloud supports long-term control in Europe

Sovereign cloud is not about rejecting innovation. It is about ensuring that innovation remains aligned with long-term control.

Organisations that take a deliberate approach to architecture, reduce dependency on proprietary services, and build on open standards are better positioned to adapt over time.

Within Cronos Europa, we approach sovereign cloud as part of a broader strategy. Together with partners such as FlowFactor, we support organisations in designing cloud environments that balance flexibility, cost-efficiency, and control.

Sovereign cloud with hyperscalers: understanding your options and choosing the right architecture

Within Cronos Europa's Sovereign Tech series, we explore how different approaches to cloud sovereignty can be combined in practice.

Digital sovereignty is often framed as a binary choice: commit to European infrastructure or remain dependent on hyperscalers. In reality, most organisations operate across a spectrum. In reality, most organisations operate across a spectrum.

We spoke with Michael Kelarou, Cloud Expert at Arxus, a sister company within De Cronos Groep, to understand how organisations can navigate this spectrum, from sovereign public cloud with built-in controls, to Azure Local, to fully private cloud environments.

"Sovereignty is not a destination. It's a set of deliberate choices about what you control, where you run, and whether you can move when the rules change."

Sovereignty is a spectrum, not a binary decision?

The binary framing of sovereignty actually holds organisations back. Real sovereignty looks more like a spectrum.

On one end, sovereign public cloud environments offer built-in controls: data residency, confidential computing, operator access restrictions, and EU Data Boundary compliance. On the other end, sits fully private infrastructure, operating entirely within your own or a trusted partner's environment, local or European.

Between these extremes, there are meaningful options.

Solutions such as Azure Local or sovereign private cloud environments allow organisations to apply control where it matters most, without giving up the benefits of cloud.

Most organisations don't need to choose one extreme. What they need is clarity about which workloads require which level of control, and a roadmap that can evolve as regulations and geopolitical conditions change.

Defining a sovereignty strategy in practice?

A sovereign cloud strategy starts with understanding workloads.

Not every system requires the same level of control, and applying sovereign infrastructure everywhere introduces unnecessary cost and complexity.

Start by identifying genuinely sensitive workloads: those subject to strict regulation, carrying real operational or reputational risk, or needing to function even if connectivity to public cloud is disrupted.

From there, assess three dimensions:

- where data must reside
- who can access it (and who must never access it)
- and what happens to business continuity if that environment becomes unavailable

This last dimension has become critical. Business continuity planning now needs to account for geopolitical disruption, not just technical failure or natural disaster.

Where Azure Local fits within a sovereign architecture?

Azure Local is the right choice when organisations need Azure-native capabilities but have workloads that cannot or should not run in the public cloud.

This applies for:

- edge or disconnected scenarios
- environments with strict data residency requirements
- latency-sensitive environments

It allows organisations to combine familiar Azure tooling with more control over where workloads run.

A growing use case is sovereign AI, where organisations want to benefit from AI capabilities while maintaining control over data used in training and inference. Azure Local, with Foundry Local, allows organisations to run AI workloads locally, gaining productivity benefits without compromising data governance.

Architecture defines sovereignty, not platform selection?

Technology alone does not guarantee sovereignty.

Azure Local, like any platform, only contributes to sovereignty when embedded in well-designed architecture.

Sovereignty is therefore defined by architectural choices.

Portability, open standards, and infrastructure-as-code practices determine whether organisations retain the ability to adapt and move over time. The difference between genuine control and its appearance lies in design-time decisions, not in platform selection.

Common misconceptions around hyperscalers and sovereignty?

Several misconceptions still shape how organisations approach this topic.

One of the most common is the assumption that data residency automatically equals sovereignty. In practice, the key question is not only where data is stored, but who can access it, under which legal conditions, and how access is technically controlled.

Another misconception is that sovereignty requires organisations to move away from hyperscalers entirely. For many, this would mean losing access to innovation, scalability, and ecosystem integration. The objective isn't independence, but avoiding a single point of failure and retaining the ability to move when needed.

A balanced approach to sovereign cloud in Europe

Sovereign cloud is not about replacing one model with another.

It is about creating a balanced architecture that aligns with organisational priorities.

In practice, this often results in a layered approach.

Public cloud can support scalable, less sensitive workloads. Azure Local or private cloud environments can be used where additional control is required.

What matters is that these choices are deliberate, and that organisations retain visibility and control across the entire landscape.

Within Cronos Europa, we see this as part of a broader sovereignty strategy. Together with partners such as Arxus, we support organisations in designing architectures that combine innovation, flexibility, and control.

Towards sovereignty-by-design: how AI governance turns tech sovereignty from theory into reality

Digital sovereignty is often framed as a strategic objective. However, without governance, sovereignty remains largely theoretical.

Organisations may control their infrastructure or data, but without clear rules, accountability, and oversight, control cannot be enforced.

In Europe, this challenge is becoming increasingly relevant. Within Cronos Europa's Sovereign Tech series, governance represents the layer that connects strategy with execution.

We spoke with Jens Meijen, co-founder of UMANIQ, a sister company within De Cronos Groep, to explore how governance and legal frameworks turn sovereignty into an operational capability.

"You need practical, boots-on-the-ground-style AI governance to turn sovereignty from some vague idea mentioned in a strategy meeting into an operational reality."

What is sovereign AI governance and why is it critical in Europe?

Well, first of all, AI governance refers to the policies and processes you have in your organization to make sure you're using AI responsibly and safely. It's basically the backbone for how your organization handles AI. So sovereign AI governance is about setting up the right procedures to ensure you keep control over the AI systems and models you're deploying in your organization.

Think of an intake process where you assess AI model providers based on where they're headquartered, or how much an AI system would expose you to geopolitical risk. Remember when Anthropic was called a 'supply chain risk' by the US? Tons of organizations had to cut Anthropic from their supply chain immediately, which led to serious service continuity issues. Another example of sovereign AI governance is setting up a committee that evaluates key decisions in terms of how much they might increase your dependence on external, often non-EU providers.

Sovereign AI governance is essential for European organizations because we've grown so accustomed to external providers that we don't even think twice about giving away control. This will come back to bite us in the long term, and the early warning signs are already showing. We've fallen asleep at the wheel, and it's time to wake up.

Why is AI governance becoming a strategic enabler rather than a constraint?

Imagine you're playing a football game without knowing the rules. Every time you do something, the referee blows the whistle and takes the ball from you. After a while, you'll be afraid to make a move. This is what happens when you don't have proper AI governance: you don't have proper rules on what you can or can't do, which tools you can use, and how new tools can get introduced into the organization. That lack of clarity paralyzes people, which leads to low adoption. And what's the point of paying for an AI tool if no one's using it?

Another aspect is that AI governance is crucial to tackle risks, which helps maintain trust. If your AI systems discriminate, hallucinate, or leak data, people - whether employees or end customers - won't want to use or interact with your AI systems.

Again, sovereignty is crucial here: if you don't control your own data, your models, or your AI systems, you might think you're completely safe, but you may be in for a nasty surprise in the future.

Finally, you can't be compliant with the AI Act without proper AI governance. You wouldn't even know what systems you're using, let alone their risk classification or your obligations. And building compliant AI systems would be completely impossible without well-defined procedures.

How can organisations operationalise sovereign AI governance?

Our clients often come to us to embed sovereignty into their daily operations. Many already have a clearly defined AI governance strategy, with clearly defined processes, rules, roles and responsibilities. In those cases, you just weave sovereignty considerations into the fabric of the existing governance structures. There's no need to overcomplicate things with arduous overhauls of everything you've been doing. Existing governance structures offer plenty of inroads to mitigate geopolitical risk.

Other clients aren't as mature in their current AI governance practices, and that's totally fine. In those cases, we set up everything they need while automatically taking sovereignty into account as a basic principle. Our "sovereignty-by-design" approach ensures that the turbulent world 'out there' doesn't interfere with your organization's ability to deliver value.

Either way, you need practical, boots-on-the-ground-style AI governance to turn sovereignty from some vague idea mentioned in a strategy meeting into an operational reality. One tip I can give is to perform regular geopolitical risk audits to assess your organization's dependence on external, non-EU technologies, even beyond cloud services, AI models, or systems. You can start from that baseline to plug potential sovereignty leaks.

AI governance, and especially sovereign AI governance, allows you to scale with confidence. You can innovate faster while preserving the hard-earned trust you've built up. When we set up sovereign AI governance structures, clients immediately notice that this clarity really brings a renewed momentum to their AI projects.

Within Cronos Europa, governance is approached as a key layer of sovereign technology. Together with partners such as UMANIQ, we support organisations in designing governance models that enable both compliance and innovation.

We are part of De Cronos Groep, a privately owned Belgian tech and innovation group with a long-term vision and a European presence. For over 20 years, we have been supporting European institutions at the crossroads of communication, IT and digital services.
Independent by design.
Collaborative by nature.

CRONOS EUROPA

100% European at our core and our roots

Sovereign Information Platforms in Europe: how Mediahaven enables control and interoperability

Digital sovereignty in Europe is often discussed in terms of infrastructure, cloud, and data control.

In practice, many organisations face a more immediate challenge.

How can information be managed, structured, and shared across complex environments while maintaining control?

In European institutions, information flows across systems, agencies, and Member States. It is continuously enriched, transformed, and redistributed. Without a structured approach, this leads to fragmentation, inconsistencies, and reduced visibility.

Sovereignty therefore depends not only on where systems are hosted, but on how information is organised and shared across them.

We spoke with Nick Vercammen, Managing Partner at Zeticon, a sister company within De Cronos Groep, to explore how this can be addressed in practice.

> "Sovereignty is not only about controlling infrastructure. It is about controlling how information is structured, accessed and shared across systems."

What is a sovereign information platform?

A sovereign information platform provides a structured environment where information can be centralised, organised, and distributed in a controlled way.

Mediahaven is an example of such a platform, enabling organisations to structure and manage content across complex environments.

It acts as a coordination layer between systems, ensuring that information remains consistent, accessible, and governed throughout its lifecycle.

The focus is not only on storing data, but on maintaining context and consistency across its lifecycle.

This includes how information is described, how it can be retrieved, and how it is shared across different stakeholders.

A key aspect of sovereignty at this level is that control remains with the organisation.

This spans several dimensions: where information is stored, how long it is retained, who can access it, and how easily it can be integrated with other systems.

In a European context, where information frequently moves across institutional and national boundaries, this structured approach becomes essential to maintain consistency and control.

How do sovereign information platforms enable control in practice?

Managing information in complex environments requires more than centralisation.

Information needs to remain usable, traceable, and governed throughout its lifecycle.

Structured platforms enable this by combining organisation, control, and openness.

Information is enriched with metadata, making it searchable and consistent across systems. At the same time, governance mechanisms ensure that retention policies and access rights are applied consistently, rather than relying on manual processes.

Retention, access, and compliance are not separate concerns, but embedded into how the platform operates.

Openness is equally important.

By enabling integration with existing systems and workflows, organisations can maintain flexibility and avoid creating new dependencies. This allows them to adapt their information landscape over time without being constrained by a single platform.

How do sovereign information platforms support information integrity and decision-making?

Sovereign information platforms play a key role in enabling information integrity.

By structuring and centralising information, they provide visibility into how information is created, transformed, and used. This makes it possible to ensure consistency, maintain traceability, and reduce ambiguity.

This includes ensuring that information remains usable over time, even as formats evolve, and that organisations are not constrained by the limitations of a single system.

Auditability is an important part of this.

Being able to demonstrate how information has been handled over time is increasingly required in regulated environments, where compliance frameworks such as GDPR and NIS2 demand not only control, but evidence of that control.

This structured foundation is essential for decision-making.

When information is fragmented or inconsistent, decisions are based on incomplete data. When it is structured and accessible, organisations can act with confidence.

How do sovereign information platforms enable interoperability across European environments?

Control and interoperability are closely linked.

In a European context, where information moves across institutions, systems, and borders, interoperability is essential to maintain consistency and coordination.

Structured platforms enable this by providing a stable layer between systems.

They allow organisations to connect workflows, exchange information, and adapt to new requirements over time, without losing control over how information is structured and governed.

At the same time, organisations retain ownership of their information, including the ability to retrieve and transfer it when needed.

This is what turns information management into an operational capability, rather than a technical constraint.

How do sovereign information platforms translate into sovereignty in practice?

Sovereign information platforms are a practical enabler of digital sovereignty in Europe.

They allow organisations to structure and control their information flows, support interoperability across systems and institutions, and create a reliable basis for decision-making.

Within Cronos Europa, we see these platforms as a key layer between infrastructure and operations. Together with partners such as Zeticon, we support European institutions in translating sovereignty into concrete, operational capabilities.

Sovereign Information Integrity in Europe: how to ensure trusted decision-making in complex information environments

European organisations are making concrete moves toward digital sovereignty.

Much of the focus is on infrastructure, cloud, and data. There is one more layer that deserves equal attention.

Information integrity, the ability to understand, validate, and protect the information that flows through European systems, strengthens the foundations that sovereign infrastructure is being built on.

We spoke with Baris Kirdemir, Head of Information Integrity Services at Cronos Europa, to explore why information integrity is not a monitoring function but a strategic capability at the core of Europe's sovereignty agenda.

"You can build a fully sovereign technology stack, but if the information circulating within it is unreliable or manipulated, your decisions are compromised. Sovereignty that does not extend to the cognitive layer is sovereignty with a blind spot."

What is sovereign information integrity, and why should it be part of the tech sovereignty conversation?

Sovereign information integrity is the ability to understand, validate, and act on information with confidence across its full lifecycle. It means seeing where information comes from, how narratives are shaped and amplified, whether coordinated manipulation is taking place, and what impact those dynamics have on your organisation, your institution, your stakeholders.

This goes beyond data accuracy. It requires visibility across platforms, languages, and audiences, structured methods to detect Foreign Information Manipulation and Interference (FIMI), and an understanding of the information environment itself: the actors, the platforms, the feedback loops, and the cognitive vulnerabilities that make manipulation threats effective.

Europe is investing heavily in the infrastructure layer. But without structured visibility into what flows through that infrastructure, the investment remains incomplete.

What has changed in the threat landscape that makes this urgent now?

The threat has industrialised. The EEAS 4th FIMI Threat Report, released in March 2026, documents the scale: more than 100 countries targeted by Foreign Information Manipulation and Interference in 2025, over 100 heads of state targeted, and close to 200 organisations affected, including NATO.

State actors are committing significant resources to information operations at scale, producing AI-generated content, innovative techniques, and tailored narrative campaigns timed to election cycles and policy windows.

Simultaneously, the European regulatory environment is maturing. The Digital Services Act, the NIS2 Directive, and the AI Act (broader enforcement from August 2026) are converging, creating both obligations and opportunities for organisations that understand how to navigate them.

The information integrity challenge is now operational, regulatory, and strategic all at once.

How does Cronos Europa approach this operationally?

Information integrity, done well, is an operational discipline. Cronos Europa brings a four-pillar model: persistent detection across platforms and open sources; deep analysis that goes beyond identifying a problem to understanding intent, attribution, and impact; structured assessment of how information environments affect decisions; and strategic response, including capability building and decision support.

Critically, this is not a dashboard. Monitoring tools are widely available. The value lies in understanding.

Cronos operates in more than 100 languages and maintains expertise across European institutional contexts, defence environments, and multilingual audiences. We build a structured picture of the information environment: not only what is being said, but why particular narratives resonate, who is driving them, and what vulnerabilities they exploit.

What are the biggest gaps you see in how organisations handle information integrity today?

Many organisations suffer from fragmentation. Monitoring sits in one team, analysis in another, communications strategy in a third, and decision-making authority in a fourth. Signals are detected without being understood. Insights are produced without translating into action.

A second pattern is the technology-only approach: organisations invest in tools, run them at scale, and find themselves overwhelmed by alerts. Without expert interpretation, technology might produce noise rather than insight.

Third, many organisations engage with the information environment only during a crisis: an election, a policy decision, a reputational incident. By that point, the window for effective response has already narrowed. Structured, persistent information integrity is a preparedness discipline, not only a crisis management function.

What role does information integrity play in Europe's broader sovereignty ambitions?

In the current context, sovereignty is incomplete without it. European defence policy is evolving to recognise that the cognitive dimension is inseparable from traditional capability areas. A sovereign European technology stack delivers its full value only when organisations have the capability to understand and act within the information environment. Without that capability, trust erodes, decision-making becomes reactive, and European capacity to act coherently is weakened.

Information integrity is not a supplementary feature of sovereignty. It is a prerequisite. Building structured, persistent capability in this domain is a strategic investment.

Within Cronos Europa, we approach information integrity as an operational discipline that connects detection, analysis, and response in a structured and sustainable way, aligned with European institutional contexts.

Stay connected

Digital sovereignty is an evolving domain.

We will continue to share new insights and perspectives as part of our Sovereign Tech series.

To stay informed:
Follow Cronos Europa on LinkedIn
Visit our website for upcoming articles

Get in touch

contact@cronoseuropa.com
+32 2 548 12 10

Cronos Europa HQ

Avenue des Arts 46
1000 Brussels
Belgium

Sovereignty is an ongoing journey. Explore more insights:

Website

LinkedIn