



EXECUTIVE PERSPECTIVE

DIGITAL SOVEREIGNTY AS A STRATEGIC, OPERATIONAL INDUSTRIAL CAPABILITY



From controlling dependencies to building a
Sustainable Innovation Model

DIGITAL SOVEREIGNTY AS A STRATEGIC, OPERATIONAL INDUSTRIAL CAPABILITY

From controlling dependencies to building
a Sustainable Innovation Model

TABLE OF CONTENTS

Preface	3
Executive Summary	4
PART I — UNDERSTANDING THE NEW QUESTION OF CONTROL	
01 Why Digital Sovereignty matters, and why now	6
PART II — PRAGMATIC SOVEREIGNTY	
02 Beyond Data Localization	8
03 Digital Sovereignty Assurance Levels	10
PART III — BUILDING DIGITAL SOVEREIGNTY	
04 Governing Digital Sovereignty	14
05 DGS Digital Sovereign Enabler	16
06 AI & Data: Sovereign Intelligence	20
07 Physical AI: sovereignty in the physical world	23
08 Open Source and RIOS: the sovereign Stack	26
09 Cybersecurity: perimeter protection	29
CONCLUSIONS	34

FOREWORD

The freedom to choose

By Vincenzo Fiengo, Co-CEO, DGS

Digital innovation has often been portrayed as a matter of speed. Today, the central issue is freedom to choose: which assets must an organization continue to govern in order to preserve resilience, decision-making capability, and freedom to evolve?

Digital sovereignty emerges from this question. It is, first and foremost, an industrial challenge rather than a purely technological one. It means maintaining governance over the data, infrastructures, platforms, skills, models, and processes that generate value and ensure business continuity.

Artificial intelligence makes this challenge even more urgent. A pragmatic approach is required, one that distinguishes sustainable dependencies from those that must be actively governed, while preserving the capabilities that are strategic for the Italian and European ecosystem.

DGS supports enterprises and institutions through deep technological expertise and experience in critical environments, helping define practical and sustainable frameworks to protect what is strategic while continuing to innovate



Vincenzo Fiengo
Co-CEO DGS

DIGITAL SOVEREIGNTY

EXECUTIVE SUMMARY

| The Sovereignty Challenge

Digital sovereignty has moved from the geopolitical debate to the center of industrial decision-making. The concentration of cloud services, the growing importance of data, the widespread adoption of artificial intelligence, and the evolution of European regulation have made control over digital resources a key factor for **competitiveness, resilience, and operational continuity**.

Some Key Figures

85%

of the European cloud market is controlled by three U.S. hyperscalers, and 80% of EU cloud spending is directed toward U.S. providers.

80mld \$

Global sovereign cloud IaaS spending is expected to reach USD 80 billion in 2026, representing a 35.6% increase over 2025.

1,8mld €

The Italian AI market reached EUR 1.8 billion in 2025, growing by 50% in a single year, while public sector adoption rose from 6% to 19%. (Osservatorio PoliMi)

The **Cloud and AI Development Act (CADA)**, proposed by the European Commission on 3 June 2026, introduces a common European framework for assessing the sovereignty of cloud and AI services through four progressive assurance levels. The framework is intended primarily for risk assessments and public-sector procurement decisions, confirming a clear strategic direction: sovereignty must be calibrated according to criticality rather than applied uniformly.

Sovereignty should be calibrated according to the level of criticality rather than applied uniformly.

Data localization is only the starting point. The actual level of sovereignty also depends on applicable jurisdiction, control of identities and encryption keys, software supply chain transparency, provider substitutability, availability of skills, and the ability to govern models, agents, and automated decisions.

DGS translates this logic into a pragmatic framework: the industry determines the maximum level of sovereignty potentially required, while each individual workload defines the actual level needed. The same organization may adopt different sovereignty levels for administrative processes, regulated data, control systems, and mission-critical functions.

The answer does not lie in a single platform. **DGS acts as a Digital Sovereignty Enabler** by combining the ability to understand where an organization stands and where it needs to go with four interconnected capabilities: **Advisory**, to define scope, governance, compliance, and adoption; **AI & Data**, to govern data, models, and agents; **Open Source and RIOS**, to build open and sustainable technology stacks; and **Cybersecurity**, to make control effective, continuous, and verifiable.

**Digital
Sovereignty is the
ability to choose,
intervene,
replace, and
evolve while
maintaining
control over what
is strategic,
without
necessarily
owning every
technology.**

PART I

Understanding the new question of choice

WHY DIGITAL SOVEREIGNTY MATTERS, AND WHY NOW

01

Digital Technology as **critical** infrastructure

The progressive digitalization of the economy has transformed the role of technology within organizations. Application systems, cloud platforms, and collaboration tools no longer merely support business operations; in many cases, they have become an integral part of the business process itself, determining its continuity and shaping its capacity for growth and evolution.

A **power grid** depends on **monitoring and dispatching systems**; a hospital relies on interconnected ecosystems of data and applications; a bank depends on platforms that coordinate **processes, controls, and decision-making**.

This transformation makes technological dependencies an integral component of strategic risk. The unavailability of a service, a supply chain vulnerability, or a legal constraint affecting a provider can generate consequences that extend far beyond the IT domain, impacting operational continuity, reputation, regulatory compliance, and decision-making capabilities.

| National Security, **resilience** and economic autonomy

Healthcare, defense, justice, taxation, energy, telecommunications, and finance all rely on complex and interconnected digital infrastructures. Digital resilience has therefore become an essential component of economic and institutional resilience: protecting operational continuity and recovery capabilities means safeguarding critical services while reducing exposure to market concentration, geopolitical crises, and non-substitutable dependencies.

The economic dimension is equally significant. In the age of AI, an increasing share of value is concentrated in the hands of those who control data, models, and computing capabilities. Digital sovereignty is therefore also about the ability to retain expertise, intellectual property, and innovation capacity, ensuring that technology adoption does not result in an irreversible loss of control.

| **Regulatory Evolution**

The European Union is increasingly linking competitiveness, security, and technological autonomy. The AI Act, Data Act, Data Governance Act, NIS2 Directive, DORA, Cyber Resilience Act, and Chips Act address different domains, yet converge around a common set of principles: accountability, portability, resilience, supply chain transparency, and verifiability.

The proposed Cloud and AI Development Act further reinforces this direction by combining investments in infrastructure capacity, research and innovation, and a common European framework for assessing the sovereignty of cloud and AI services. As a result, digital sovereignty is becoming a key factor in vendor selection, public procurement processes, and the design of services intended for critical sectors.

| The turning Point of **Artificial Intelligence**

Artificial intelligence expands the boundaries of control. Generative AI systems create content and generate knowledge; AI agents can invoke tools and interact with applications; Physical AI connects digital intelligence with machines, industrial systems, and critical infrastructure.

As a result, sovereignty is no longer concerned solely with where data resides. It also encompasses who governs the model, which tools an agent is authorized to use, what actions it is permitted to perform, and how human oversight and intervention can be maintained when needed.

PART II

Pragmatic Sovereignty

BEYOND DATA LOCALIZATION

02

Why data residency is not enough

The location of data within the European Union is an important requirement, but it does not fully address the issue. Data may be stored in a European data center and still remain subject to non-European jurisdictions, operational procedures controlled by external entities, or platforms that are difficult to replace.

Geography describes where a resource is located; sovereignty defines who can exercise control over that resource and under what conditions.

The six dimensions of control

Jurisdictional Data

Which legal framework applies to data, infrastructure, and providers?

Who controls access, encryption keys, retention, lineage, and data usage?

Operational

Who monitors, administers, restores, and manages exceptions?

Technologic

Can components, formats, and services be replaced or migrated?

Industrial

Where do expertise, intellectual property, and innovation capabilities reside?

Cognitive

Who governs the objectives, decision-making criteria, autonomy, and oversight of AI systems?

Taken together, these dimensions make it possible to distinguish mere formal compliance from the actual ability to maintain control over critical dependencies. Sovereignty therefore becomes a property of the entire ecosystem: data, identities, infrastructure, software, providers, skills, and processes must be viewed as links in a single integrated chain.

From geography to governance capability

The key question for decision-makers is not whether an organization is sovereign in an absolute sense.

Rather, it is which functions must remain governable, what level of autonomy they require, and which dependencies can be considered acceptable.

FUNCTIONS

Which functions must remain under effective control?



AUTONOMY

What degree of autonomy is required?



DEPENDENCIES

Which dependencies are acceptable?

This approach avoids two extremes

GOVERNANCE CAPABILITY

Unmanaged dependency

Reduces freedom of choice and resilience.

Indiscriminate self-sufficiency

Increases costs and complexity without necessarily delivering greater value.

PART II

Pragmatic Sovereignty

DIGITAL SOVEREIGNTY ASSURANCE LEVELS

03

The framework proposed by the Cloud and AI Development Act (CADA)

The European Commission adopted the proposal for the **Cloud and AI Development Act (CADA)** on 3 June 2026, with the objective of strengthening the European cloud and artificial intelligence ecosystem. The proposal focuses on three key pillars: **research and innovation**, the **development of infrastructure capacity**, and **technological autonomy**. Within this latter area, it introduces a common European framework for assessing the sovereignty of cloud and AI services, supported by an adoption mechanism designed for the public sector.⁶

CADA is currently a proposed regulation and may be amended during the legislative process before its final adoption.

However, the framework already represents a significant milestone, as it defines four progressive assurance levels to be applied on the basis of risk assessment.

This classification does not correspond to the DGS deck's previous editorial taxonomy and therefore requires terminology and descriptions aligned with the official framework.



| The 4 CADA levels

Livel 1

EU DATA LOCALIZATION

Suitable for non-critical business processes or routine support activities (e.g., information portals or non-sensitive data processing), where the primary risk is mitigated through the storage and processing of data within the borders of the European Union.

Livel 2

OPERATIONAL INDEPENDENCE AND SUPPLY CHAIN TRANSPARENCY

Required for medium- to high-criticality processes, where a service disruption or the suspension of cloud/AI services by the provider could result in significant operational impacts. This level requires operational autonomy as well as transparency across the supply chain, including visibility into subcontractors and critical dependencies.

Livel 3

EUROPEAN OWNERSHIP AND CONTROL

Designed for core and strategic processes (e.g., regulated sectors, financial services, healthcare, and NIS2-designated critical infrastructures), where operational continuity and confidentiality cannot depend on entities owned or controlled by third countries.

Livel 4

FULL SOVEREIGNTY AND SOFTWARE SUPPLY CHAIN CONTROL

Reserved for processes with the highest levels of criticality and national security requirements (e.g., defense, intelligence, and essential judicial functions), where the risk of external interference must be eliminated across the entire technology stack, including software code, infrastructure, and maintenance activities.

The European framework therefore moves beyond the assumption that data localization alone is sufficient to guarantee sovereignty. As the assurance level increases, so do the requirements related to independence from third countries, European ownership and control, transparency, and governance of the software supply chain.

The DGS contribution: applying the levels to workloads

The sovereignty assurance levels defined by CADA characterize the attributes of the service and the provider. DGS's contribution is to translate these levels into the organization's specific operating context, taking into account factors such as sector criticality, data sensitivity, the impact of service disruption, regulatory requirements, and the substitutability of key components.

The sector establishes the ceiling; the individual workload determines the level actually required within that ceiling.

The same organization may legitimately adopt different sovereignty levels across its operations. An administrative portal or a development environment may require lower assurance levels than a control system, a critical financial platform, or an infrastructure responsible for managing classified data.

Pragmatic sovereignty concentrates the most stringent controls where risk and business value justify them, while preserving economic sustainability and access to innovation in less critical contexts.

CONTEXT		HIGH-LEVEL GUIDANCE
GENERIC ENTERPRISE		Baseline assurance levels for standard workloads, with selective escalation for sensitive data or critical business processes.
REGULATED INDUSTRIES		Assurance levels tailored to intellectual property protection, cybersecurity requirements, and high-risk operational scenarios.
FINANCIAL SERVICES AND INSURANCE		High assurance levels for regulated data, decision-making processes, and essential services.
CRITICAL INFRASTRUCTURE		Higher assurance levels for control and dispatch systems, with differentiated approaches for administrative and support functions.
DEFENCE AND NATIONAL SECURITY		The highest assurance level for classified infrastructures, intelligence operations, and data protected by national security restrictions.

| Key factors to consider in the assessment

01

Nature and sensitivity of the data processed

For example, personal, financial, healthcare, or strategically important industrial data.

02

Criticality of the Service for Business Continuity

The distinction between core processes, whose disruption would compromise business operations, and support or back-office functions, which are less critical.

03

Technological and governance dependency

Particularly the exposure to non-EU regulations, such as the U.S. Cloud Act, which may affect the organization's actual level of control over its data and digital assets.

04

Relevance to public order and the Security of Critical Infrastructure

A factor of particular importance for public sector organizations and for entities falling within the scope of the NIS2 Directive, where the protection of essential services and critical infrastructure is a strategic requirement.

PART III

Building Digital Sovereignty

GOVERNING DIGITAL SOVEREIGNTY

D4

From Classification to Implementation

Classification establishes the required level of assurance; governance translates that choice into an actionable program. Digital sovereignty requires decisions regarding architectures, providers, contracts, responsibilities, operational control, skills, and investments. Technology is essential, but it is not sufficient.

A digital environment may exhibit sovereign characteristics and still remain ungovernable if the necessary roles, processes, and verification capabilities are not in place.



| Scope, Governance, Compliance and Adoption

01 | SCOPE

OBJECTIVE

Classify data, processes, systems, and providers according to their criticality, risk profile, and dependency level.

02 | GOVERNANCE

OBJECTIVE

Define responsibilities, the operating model, metrics, and decision-making mechanisms.

03 | COMPLIANCE

OBJECTIVE

Translate the requirements of the AI Act, NIS2, DORA, GDPR, Data Act, and CADA into measurable and verifiable controls.

04 | ADOPTION

OBJECTIVE

Develop the skills, processes, and culture needed to govern what has been chosen.

Digital sovereignty becomes sustainable when it is embedded into everyday sourcing, development, security, operations, and change management processes. Go-live is not the finish line: dependencies, regulations, and technologies continuously evolve, and the governance model must be regularly updated through ongoing monitoring, risk reassessment, portability testing, and business continuity validation.

PART III

Building Digital Sovereignty

DGS DIGITAL SOVEREIGN ENABLER

D5

Understanding the starting point and defining the target state

DGS supports organizations in understanding their operating context, assessing their current position against digital sovereignty requirements, and defining the roadmap needed to achieve the required level of assurance. This capability precedes technology selection:

organizations must first identify what needs to be **protected**, distinguish **acceptable dependencies** from critical ones, and **ensure that every decision is aligned with risk, compliance obligations, and business objectives**

Advisory therefore plays a cross-functional role: it translates regulatory requirements and **control objectives** into scope definition, a **strategic roadmap**, an **operating model**, and an **adoption** program. DGS classifies data, processes, and systems, assesses provider dependencies, identifies the appropriate assurance level, and defines priorities, investments, responsibilities, and performance metrics.

DGS Sovereign Enabler: interconnected capabilities

Digital sovereignty is the outcome of an integrated journey that combines platforms, infrastructure, certifications, and expertise. DGS makes it tangible through the convergence of four interconnected domains of expertise that it develops, governs, and brings together:

Advisory, AI & Data, Open Source, and Cybersecurity.

ADVISORY

Scope and governance

Digital sovereignty strategy, operating model, and governance translated into actionable roadmaps, processes, roles, and measurable metrics.

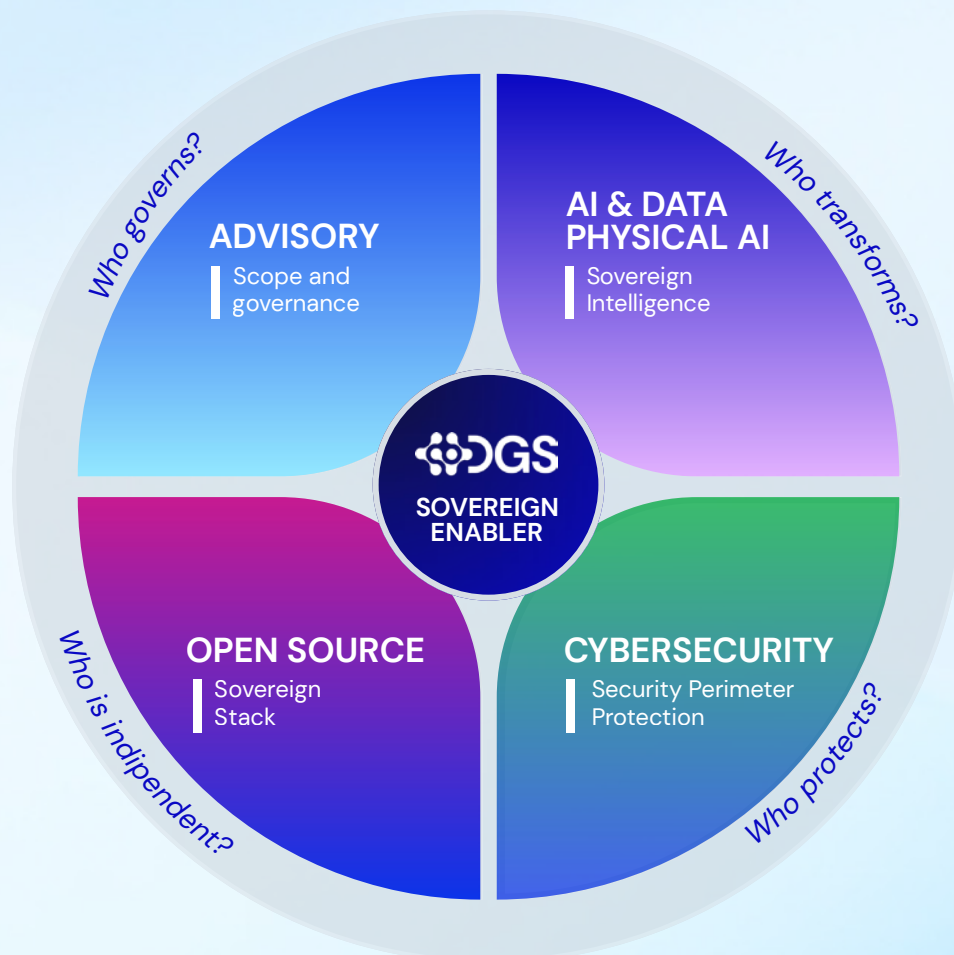
- SCOPE
- COMPLIANCE
- GOVERNANCE
- ADOPTION

AI & DATA SENSE | PHYSICAL AI

Sovereign Intelligence

Data platforms and AI solutions: from models and agents to Physical AI. Every agent has a defined identity, accountable ownership, and a verifiable audit trail.

- AI & DATA SOLUTIONS
- DATA MARKETING
- AGENTIC ORCHESTRATION
- AI ENGINEERING



OPEN SOURCE

Sovereign Stack

Infrastructure built on open technologies, ensuring transparency, portability, and independence from vendor lock-in. As a key contributor to RIOS, we are not merely users of open-source technologies, but active builders and innovators.

- RIOS (RETE ITALIANA OPEN SOURCE)
- VERTICAL AI & DATA
- ENTERPRISE SOLUTIONS

CYBERSECURITY

Perimeter Protection

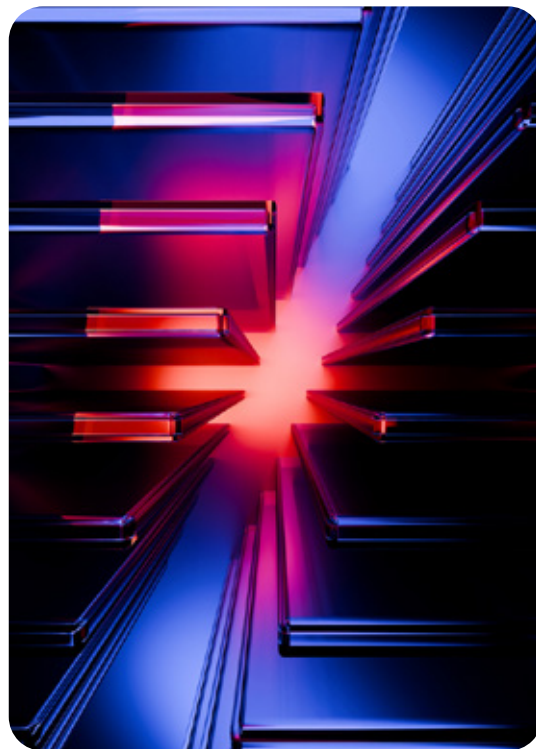
Protecting data, identities, and services through Governance & Compliance, continuous monitoring, risk management, and access control, ensuring integrity, resilience, and operational trustworthiness.

- AI SECURITY
- CUSTOMIZED SOLUTIONS
- MANAGED SECURITY SERVICES

Composing, integrating, building

DGS acts as a **sovereign orchestrator**, assembling the most appropriate architecture by combining dedicated environments, open technologies, and available computing capabilities. The objective is neither to replicate the infrastructure of hyperscale providers nor to lock customers into a single technology stack.

In this perspective, **sovereignty** becomes a **property of the architecture** and the operating model, rather than a label attached to a single product or technology.



Where DGS Creates **value** across the sovereign value chain

The digital sovereignty value chain spans a wide range of layers. Silicon, energy, data centers, and computing capacity require significant infrastructure investments and are primarily controlled by large global providers. DGS focuses its value creation on the layers where selection, composition, integration, and risk governance make the greatest difference, combining available capabilities according to the required balance of cost, performance, and control.

Value is concentrated in the layers where domain expertise, trust, integration, and governance capabilities are critical: platforms and orchestration, vertical applications, governance, compliance, and adoption. This is where broad principles and regulatory requirements are translated into solutions that align with the operational realities of public administration, defense, finance, energy, healthcare, and other regulated industries.

LAYER

Governance, compliance and adoption

DGS ROLE

Translate regulatory requirements and sovereignty objectives into programs, controls, roles, and competencies.

LAYER

Sovereign vertical applications

DGS ROLE

Integrate sovereignty requirements into sector-specific processes and mission-critical systems.

LAYER

Platform and orchestration

DGS ROLE

Coordinate data, models, AI agents, identities, audit mechanisms, and workloads across heterogeneous environments.

LAYER

Cloud and computing capacity

DGS ROLE

Select and combine European providers, dedicated environments, and governed global services.

The challenge is not simply selecting technologies, but turning complexity into informed choices: deciding which components to use, which dependencies can be accepted, which controls are required, and how long-term governance can be preserved.

DGS addresses this challenge by combining technical expertise, business process knowledge, delivery capabilities, and ecosystem relationships, ensuring that architectures remain aligned with risk levels, organizational objectives, and operational realities.

PART III

Building Digital Sovereignty

AI & DATA: SOVEREIGN INTELLIGENCE

06

Data, models and agents across the entire stack

For DGS, sovereign intelligence is the ability to govern the entire system that transforms data, models, and AI agents into operational outcomes.

This scope spans the entire technology stack, including the business layer, applications, data, software, and infrastructure. It encompasses strategy and adoption, use case development, data governance, AI engineering, deployment, and security.

Data is the foundation of this system. Data quality, traceability, lineage, access policies, and conditions of use must be governed throughout the entire lifecycle to ensure trust, compliance, and operational control.

A reliable model requires reliable data and an organization capable of understanding where that data originates, how it has been transformed, and under which constraints it may be used.

Orchestrating models and platforms

Proprietary models, open-source models, cloud environments, and dedicated infrastructures each offer distinct advantages and constraints. DGS governs these dependencies through an orchestration-driven approach: selecting the most appropriate component for each use case, integrating it with the customer's systems, and preserving the ability to replace or modify it as risk profiles, performance requirements, or business needs evolve.

AI Factories, AI Engineering tools, and MLOps/LLMOps environments industrialize this process. Models, data, evaluations, controls, and security requirements are brought together within a governed and repeatable delivery chain, ensuring that rapid experimentation does not come at the expense of quality, traceability, or control.



Select

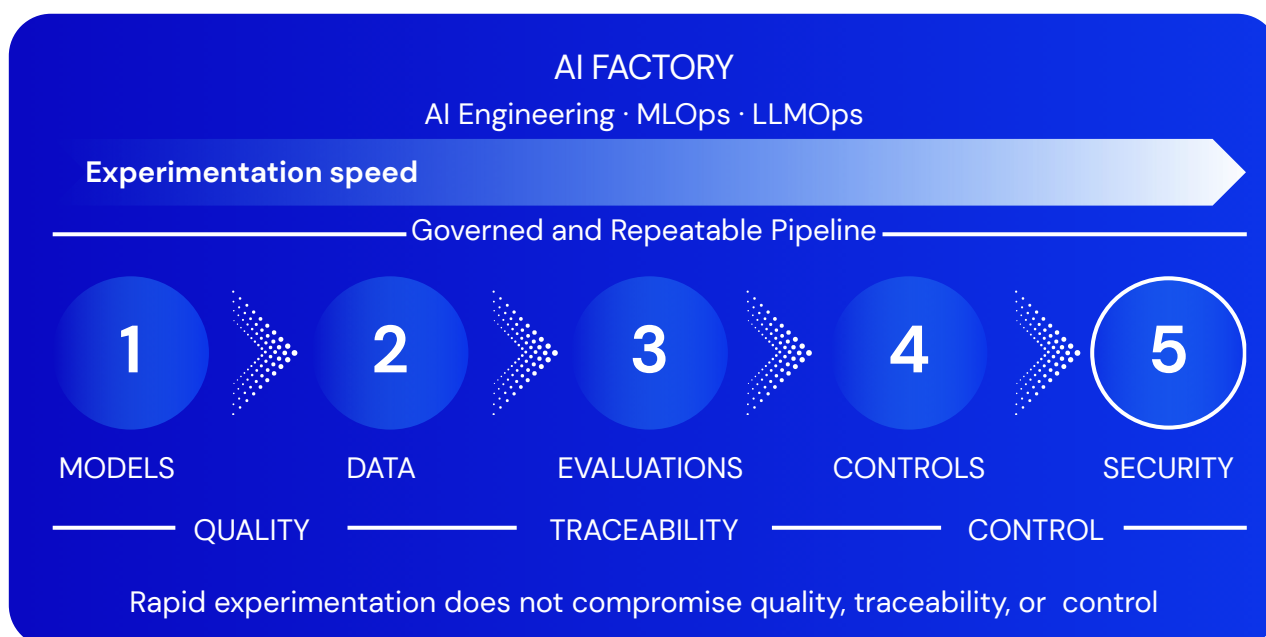
Choose the best-fit component

Integrate

Integrate with customer systems

Replace

Adapt or replace as requirements evolve



Governing the agentic paradigm

AI agents mark the transition from systems that generate responses to systems that perform actions. Sovereignty therefore shifts from the outcome to the action itself: identities, permissions, tools, memory, interactions, and levels of autonomy must all be clearly defined and continuously monitored.

Every agent must be identifiable, associated with a defined operational scope, and embedded within a verifiable chain of accountability.

DGS combines **agent orchestration, data governance, security, and application management** to ensure that oversight, traceability, and the ability to intervene are built into the architecture from the outset.

The objective is to accelerate AI adoption without separating operational autonomy from accountability.

PART III

Building Digital Sovereignty

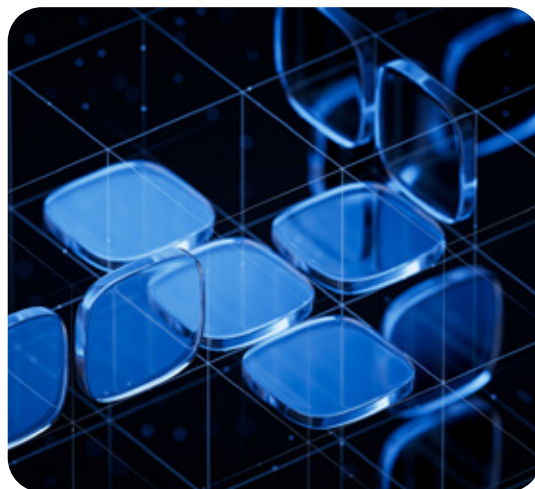
PHYSICAL AI: SOVEREIGNTY IN THE PHYSICAL WORLD

07

When control extends to behavior

Physical AI takes artificial intelligence beyond the screen. Mobile robots, autonomous systems, digital twins, computer vision, edge AI, and OT platforms create a direct link between information and action.

In this environment, **sovereignty is no longer concerned solely with who controls the data.** It is also about who governs system behavior, under which safeguards, and through which supply chain.



Four dimensions of Sovereign Physical AI

01 | DATA

CONTROL

Data originates at the edge: edge inference, OT data governance, and data retention within the controlled perimeter.

02 | MODELS

CONTROL

Simulation, digital twins, and sim-to-real environments that are controllable, transparent, and auditable.

03 | ACTIONS

CONTROL

Agent identity, authorization of critical commands, verifiable audit trails, and safe-stop mechanisms.

04 | SUPPLY CHAIN

CONTROL

Hardware, firmware, sensors, Software Bill of Materials (SBOM), portability, and supply chain governance criteria.

Trieste: An ecosystem for sim-to-real experimentation

DGS is committed to developing controlled physical and digital environments where digital twins, AI agents, and robotic systems can be trained, tested, and validated through sim-to-real simulations before their deployment in operational processes.

A collaborative path involving the regional scientific and industrial ecosystem, aimed at turning Physical AI into secure, verifiable, and sovereign-by-design operational solutions.

Trieste provides a **natural environment** for developing this vision, thanks to the convergence of **scientific research, port operations, logistics, shipbuilding, and maritime observation.**

As part of its strategic vision for 2028, the ambition is to progressively evolve toward what could become Europe's first sovereign training ground for Physical AI: an environment in which data, models, telemetry, and intellectual property remain within a governed perimeter, with OT security, traceability, and oversight embedded by design.



PART III

Building Digital Sovereignty

OPEN SOURCE AND RIOS: THE SOVEREIGNTY STACK

08

From technological openness to industrial capability

Open Source is a powerful enabler of digital sovereignty because it promotes transparency, open standards, interoperability, portability, and freedom to evolve. However, access to source code alone does not automatically deliver autonomy. Without governance, expertise, maintenance, security, and enterprise-grade support, an open platform can simply create a different form of dependency.

For DGS, Open Source is not just about using software. It means actively maintaining and contributing to the codebase, securing the software supply chain, ensuring support and business continuity, participating in institutional and industry initiatives, and anticipating evolving European requirements and strategic directions.

The **sovereign stack** extends across infrastructure, enabling platforms, and industry-specific solutions, underpinned by governance, support capabilities, and an ecosystem able **to ensure continuous innovation, maintenance, and evolution.**

DGS and RIOS: not users, but builders of the ecosystem

RIOS (**Rete Italiana Open Source**), of which DGS is a co-founder and a member of APELL (The European Open Source Software Business Association), provides organizations with an ecosystem of expertise and technologies that makes Open Source a sustainable choice even in complex and highly regulated environments. The network brings together specialized Italian companies and a distributed set of capabilities, including:

- more than 400 technical specialists**

- 27 official vendor and community partners**

- 80 technical certifications**

- dedicated trainers**

- A broad portfolio of products, frameworks, and technologies**

For customers, this translates into access to a distributed network of development, integration, training, and support capabilities, reducing the risk that adopting open technologies creates a new operational dependency.

The value of RIOS goes beyond technology. Digital dependency is frequently a dependency on skills and expertise: access to code is of limited value without the capabilities needed to understand, adapt, secure, and maintain it. By combining complementary competencies,

RIOS provides an ecosystem capable of sustaining complex architectures and large-scale transformation initiatives over time.

From national capability to the European dimension

RIOS's membership in **APELL** connects Italian Open Source expertise to the European dialogue on digital sovereignty and open technologies. This presence enables participation in the development of standards, engagement with institutional initiatives, and representation of the needs of organizations that build and adopt Open Source solutions.

Digital sovereignty is not achieved through isolation, but through the combination of strong national capabilities and active participation in European ecosystems.

Many organizations use **Open Source**. **DGS**, through **RIOS**, helps build the ecosystem that turns Open Source into a tangible lever for technological independence, industrial capability, and digital sovereignty.

Four Dimensions for making Open Source governable

01 Technological Sovereignty

OPEN, INTEROPERABLE, AND VERIFIABLE ARCHITECTURES.

02 Skills Sovereignty

SPECIALISTS, CERTIFICATIONS, TRAINING, AND SUPPORT CAPABILITIES.

03 Industrial Sovereignty

THE ABILITY TO DEVELOP, MAINTAIN, AND CONTINUOUSLY EVOLVE SOLUTIONS OVER TIME.

04 Ecosystem Sovereignty

CONNECTING ITALIAN CENTERS OF EXCELLENCE, OPEN-SOURCE COMMUNITIES, AND EUROPEAN REPRESENTATION.

PART III

Building Digital Sovereignty

CYBERSECURITY: PERIMETER PROTECTION

09

Making control continuous and verifiable

Cybersecurity is the safeguard that makes digital sovereignty effective over time. Localized data, dedicated infrastructures, open technologies, and governed AI models create value only if the organization maintains control over identities, access rights, vulnerabilities, software components, exposed attack surfaces, and emerging threats.

This means being able to know who is accessing what, with which privileges, from which environments, through which technologies, and based on what evidence. Security therefore becomes a governance capability rather than a purely technical function.

By providing visibility, accountability, and continuous assurance, cybersecurity enables organizations to reduce exposure, validate architectural choices, and maintain the required level of sovereignty even as risks, regulations, and technologies evolve.

SCOPE

Data and Identities

CUSTOMER BENEFITS

Control access rights, privileges, encryption keys, traceability, and accountability for critical assets.

SCOPE

Technology and Supply Chain

CUSTOMER BENEFITS

Ensure visibility and verifiability of software components, platforms, dependencies, and exposed attack surfaces.

SCOPE

Compliance

CUSTOMER BENEFITS

Translate NIS2, DORA, CRA, AI Act, and GDPR requirements into actionable controls, evidence, and auditability mechanisms.

SCOPE

Resilience

CUSTOMER BENEFITS

Detect, contain, and recover from incidents while maintaining the continuity of essential business functions.

| **AI Security: protecting models, agents, and actions**

Artificial intelligence extends the scope of cybersecurity beyond data and applications to include models, agents, tools, prompts, memory, permissions, and automated actions. An AI system can access sensitive information, invoke external tools, generate outputs, and trigger operational processes. Every stage of this chain must be governed and secured.

In practical terms, AI Security means enabling AI adoption while preserving accountability, oversight, and the ability to intervene when necessary. Every agent must have a clearly defined identity, a bounded operational scope, appropriately assigned privileges, and a verifiable audit trail. As AI systems become more autonomous, organizations must address emerging risks such as prompt injection, tool misuse, agent compromise, model manipulation, and privilege escalation. These threats require a combination of technical controls, governance processes, and continuous monitoring.

| **Resilience and Business Continuity**

Digital sovereignty is also measured by an organization's ability to withstand a crisis. Organizations must be able to detect incidents rapidly, contain their impact, preserve essential functions, and restore services and data in a timely manner. This capability extends beyond traditional IT environments to include OT (Operational Technology) and IoT ecosystems, where a cyber incident may affect industrial facilities, critical infrastructure, essential services, and physical processes.



In this perspective, **Security Operations Centers (SOCs), managed security services, incident response, threat intelligence, identity security, OT security, and business continuity** are not isolated disciplines. They are interconnected elements of a single capability: preserving control, visibility, and resilience even when the digital ecosystem is under pressure.

From the **model** to transformation journeys

DGS's contribution lies in connecting assessment, design, implementation, and continuous operations into a coherent transformation journey.

The starting point is the mapping of assets, dependencies, risks, exposures, and regulatory requirements. The next step is the design and deployment of environments, platforms, controls, and processes aligned with the required level of assurance. Finally, the operational phase ensures that evidence, resilience, and compliance are maintained over time.

PHASE

ASSESS EXPOSURE AND DEPENDENCIES

WHAT IT ENABLES FOR THE CUSTOMER

Map assets, identities, exposed attack surfaces, critical suppliers, software components, and regulatory requirements to identify where control is most vulnerable.

PHASE

DESIGN CONTROLS AND RESPONSIBILITIES

WHAT IT ENABLES FOR THE CUSTOMER

Define roles, privileges, policies, approval workflows, audit requirements, and security criteria aligned with the required assurance level.

PHASE

PROTECT DATA, IDENTITIES, AND ENVIRONMENTS

WHAT IT ENABLES FOR THE CUSTOMER

Implement controls for access, encryption keys, privileges, workloads, application components, and IT, cloud, OT, and AI infrastructures.

PHASE

MONITOR AND RESPOND

WHAT IT ENABLES FOR THE CUSTOMER

Identify and respond to anomalies, threats, and incidents through continuous oversight, rapid response capabilities, and full auditability of security evidence.

PHASE

MAINTAIN RESILIENCE AND COMPLIANCE

WHAT IT ENABLES FOR THE CUSTOMER

Continuously update controls, assessments, metrics, and continuity plans to preserve security, auditability, and recovery capabilities over time.

These capabilities are combined according to the organization's context, maturity level, and workload criticality. The continuity between strategy, implementation, and ongoing operations is what distinguishes a declaration of sovereignty from a capability that can be effectively exercised in practice.

Security makes it possible to see what is **happening**, verify what has been **decided**, and **maintain control** over what must remain governed.

CONCLUSIONS

| Sovereignty as a capability to be exercised

Digital sovereignty is the ability to **choose, intervene, replace, and evolve while maintaining control over what is strategically important**. It is not defined solely by data localization, nor by the adoption of a specific platform. Rather, it is a governance model calibrated to the criticality of each workload and capable of being verified over time.

| The DGS contribution

DGS translates this approach into practical transformation journeys: the sector defines the highest level of sovereignty that may be required, while the individual workload determines the actual level of assurance needed.

From this assessment stem decisions regarding **architectures, providers, data, models, AI agents, security, and business continuity**.

Experience in critical environments

Public administration, defense, finance, energy, and regulated industries are sectors where control, security, and compliance are not optional requirements, but operational necessities.

Translating requirements into concrete decisions

This approach enables organizations to identify the data, systems, processes, and dependencies that require the highest levels of control and protection.

Integrated capabilities

Advisory, AI & Data, Open Source, RIOS, and Cybersecurity are combined into a single, integrated journey, from the initial assessment through to ongoing operations and governance.

Italian Roots, European reach

DGS's strong connection to the Italian market is complemented by its participation in ecosystems such as RIOS and APELL, strengthening expertise, support capabilities, and long-term innovation capacity.

Proportionate Approach

Each transformation journey is designed according to the organization's risk profile, maturity level, and business objectives.

Digital sovereignty is not about owning everything. It is about always being able to choose who to depend on, and under which conditions. **DGS** exists to make that choice possible: **secure, sustainable and rooted in Italian expertise while connected to the broader European ecosystem.**

CONTRIBUTORS

Antonio Autorino

Head of AI & Data Sense

Michele Balbi

Advisor Digital Innovation Strategy

Giuseppe Blasi

Partner, Management Consulting

Pierluigi Brienza

Chief Strategy Officer

Gianluca Cimino

Chief Strategy & Delivery Officer Cybersecurity

Biagio De Marchis

Chief Business Growth Officer

Francesco Di Bianco

Physical AI Offering Leader

Irene Cosimo

Content Marketing Leader

Milena Fabbrizzi

AI & Data Business Developer

Alessandro Favretto

AI – Service Line Manager

Eraldo Federici

Chief Operating Officer Digital Solutions

Roberta Giani

Chief Marketing & Communication Officer

Fabio Storri

Head of Consulting Strategic Offering

Marco Tessarin

Head of Open Source Excellence Center

Graphic Design & Layout by Sabrina Lugato, Marco Veninati

| About DGS

DGS S.p.A. is an Italian technology partner that has supported the growth of enterprises and public sector organizations for 29 years, helping them modernize processes, systems, and infrastructures securely through deep expertise in technology and market dynamics.

With a portfolio that combines Cybersecurity, AI & Data, Digital Engineering, Management Consulting, and Smart Enterprise solutions, DGS helps organizations build strong digital foundations and foster digital trust. Its goal is to enhance operational performance, resilience, and process sustainability through AI modernization initiatives and a Secure by Design approach.

DGS delivers its services through a network of Centers of Excellence and strategic partnerships with leading global technology vendors. Today, the Group includes more than 2,700 professionals and holds over 2,500 technical certifications, providing the scale, expertise, and delivery capabilities required to support complex digital transformation programs.

Intellectual property and confidentiality of the document

Intellectual Property

All content, information, methodologies, models, software, deliverables, graphical representations, and documentation described in this material are the exclusive property of DGS S.p.A., unless otherwise expressly stated.

No part of this document may be reproduced, distributed, published, modified, or used, in whole or in part, without the prior written consent of DGS S.p.A.

Confidentiality

This document contains confidential and proprietary information of DGS S.p.A. and is intended solely for purposes related to the evaluation of the candidature.

The disclosure, distribution, or communication of the contents of this document to third parties is prohibited without the prior written consent of DGS S.p.A., except where strictly necessary for evaluation activities performed by the organizers of the initiative.

The information contained herein is provided for illustrative purposes only and does not constitute any grant, license, assignment, or transfer of intellectual property rights, industrial property rights, or know-how to any third party.

CONTACT US

 @dgs_spa

 DGS SpA

 www.dgsspa.com



visit dgsspa.com