accenture

Digital & National Sovereignty

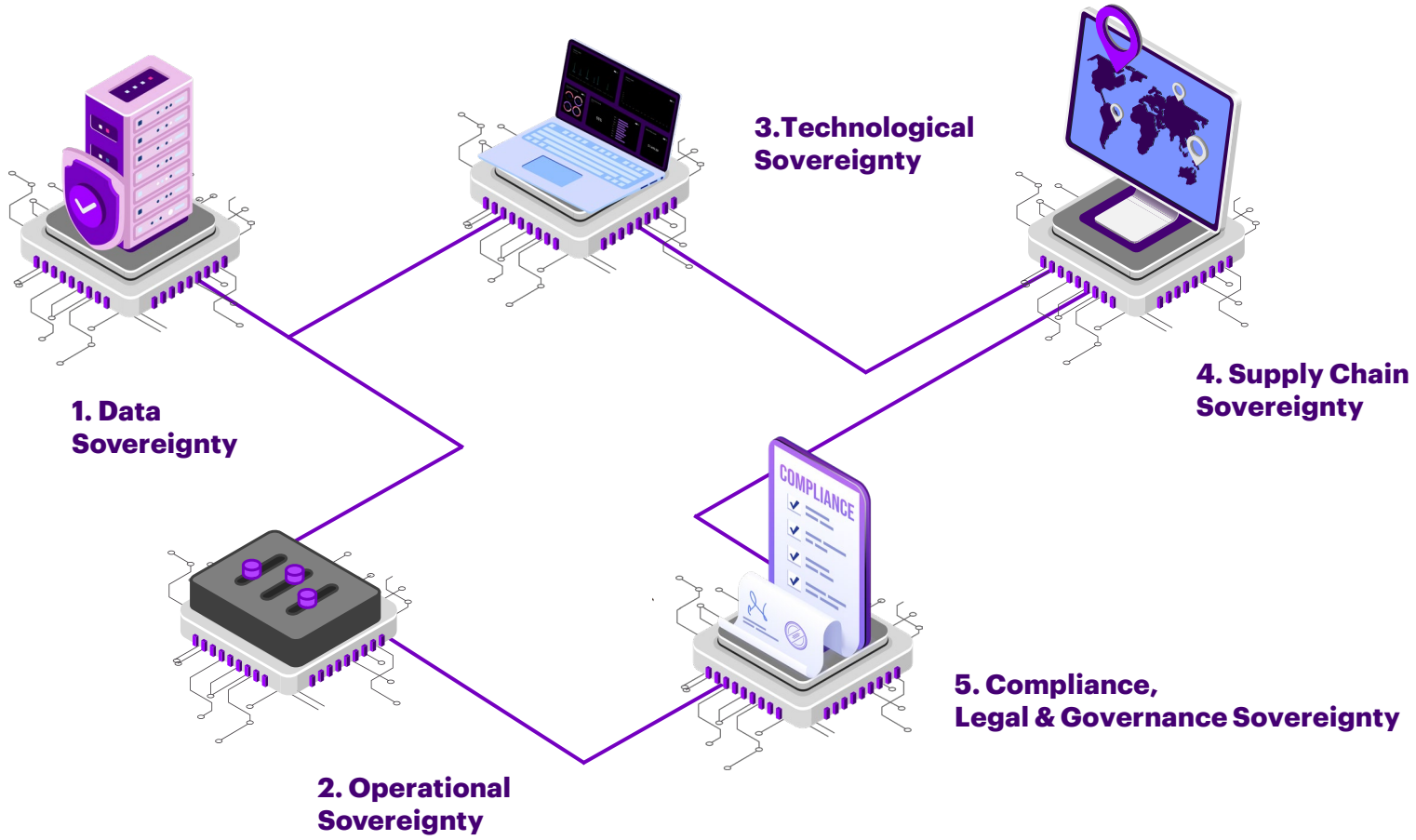
Panagiotis Psarrakos
Technology Director
panagiotis.psarrakos@accenture.com

How we define Digital Sovereignty

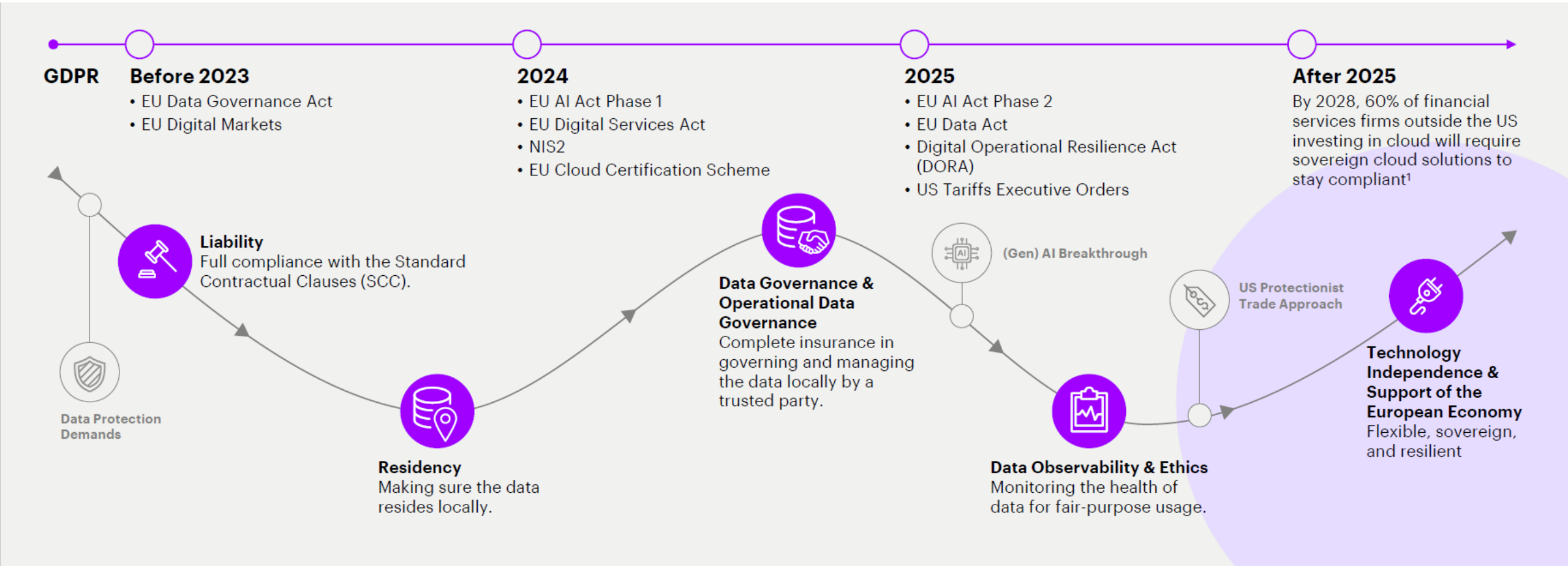
Digital sovereignty has emerged as a critical priority in today's geopolitical, economic, and technological landscape supported by a need for greater control over supply chains, logistics, operations, and data.

Digital sovereignty is the ability of a nation, organization or community to exercise independent control over its digital infrastructure, operations, identities, data, security and the rules that govern them.

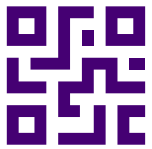
It protects, governs, and operates critical assets in line with local laws and values security requirements in strategic interest without over-reliance on foreign entities.



Digital Sovereignty has changed significantly in the last years in Europe



Digital Sovereignty & National Sovereignty



Digital Sovereignty

Digital sovereignty is the ability of a nation, organization or community to exercise independent control over its:

- Digital infrastructure
- Digital operations
- Digital identities
- Data,
- Cybersecurity security
- the rules that govern them all

National Sovereignty

Act independently in:

- Governing and legislating within its territory
- Defending borders — physical and digital
- Making autonomous strategic decisions
- Controlling critical national resources
- Resisting foreign interference or coercion

Why they converge

In the 21st century, national sovereignty cannot be sustained without digital sovereignty. Every critical function of the modern state depends on secure, autonomous digital systems.

Economic Power

GDP and trade depend on digital platforms, financial systems, and data flows that must remain sovereign.

Military Readiness

Defence command systems, logistics, and intelligence rely on trusted, non-compromised digital infrastructure.

Democratic Integrity

Elections, public institutions, and governance processes must be free from external digital manipulation.

National Sovereignty is not only for Public Sector

The National Critical Systems and Data consist of both Public and Private Sector ecosystems

Energy & Power

Telecoms & Networks

Water & Sanitation

Finance & Banking

Government & Defence

Smart Cities

Core Capabilities of Digital Sovereignty

Data Localisation & Governance

Sovereign cloud infrastructure, national data residency laws, and data classification and processing frameworks.

Secure Communications

End-to-end encrypted government networks, sovereign 5G/6G backbones...

Sovereign Cloud & Computing

Nationally operated hyperscale cloud platforms, eliminating dependency on foreign cloud providers for state data.

Digital Identity & Authentication

Biometric national identity systems, PKI frameworks, and federated identity management under state control.

Intelligence & Threat Detection

AI-powered national SIEM/SOC capabilities providing real-time visibility across all government digital assets.

Cyber Defence & Resilience

Automated incident response, threat intelligence sharing, and cyber deterrence posture.

AI-powered Sovereignty

AI Powers Sovereignty

Autonomous Threat Hunting

ML models scan billions of network events per second, identifying zero-days and lateral movement before human analysts can react.

Predictive Attack Modelling

AI simulates adversary tactics (APT, nation-state) to predict attack vectors and harden sovereign systems proactively.

Cognitive Decision Support

AI-driven situation awareness platforms provide leaders with real-time operational intelligence across all critical domains.

Automated Incident Response

Security management systems can autonomously contain, isolate, and remediate threats at machine speed, reducing dwell time to near-zero.

Protecting AI Itself

Adversarial Attack Defence

Sovereign AI models are hardened against adversarial inputs, data poisoning, and model inversion attacks by foreign actors.

Sovereign AI Training Data

National AI systems train on domestically curated, classified datasets — eliminating dependency on foreign or tainted data pipelines.

Model Integrity & Auditability

Cryptographic model signing and explainability frameworks ensure AI decisions in critical contexts can be validated and audited.

AI Supply Chain Security

Hardware security modules and secure enclaves protect AI inference workloads, preventing tampering at the chip level.

accenture

Thank you