nlighten

close · coupled · connected

Where Is Your Data Really?

Understanding Data Sovereignty, Residency, and Compliance in the New European Cloud Era.

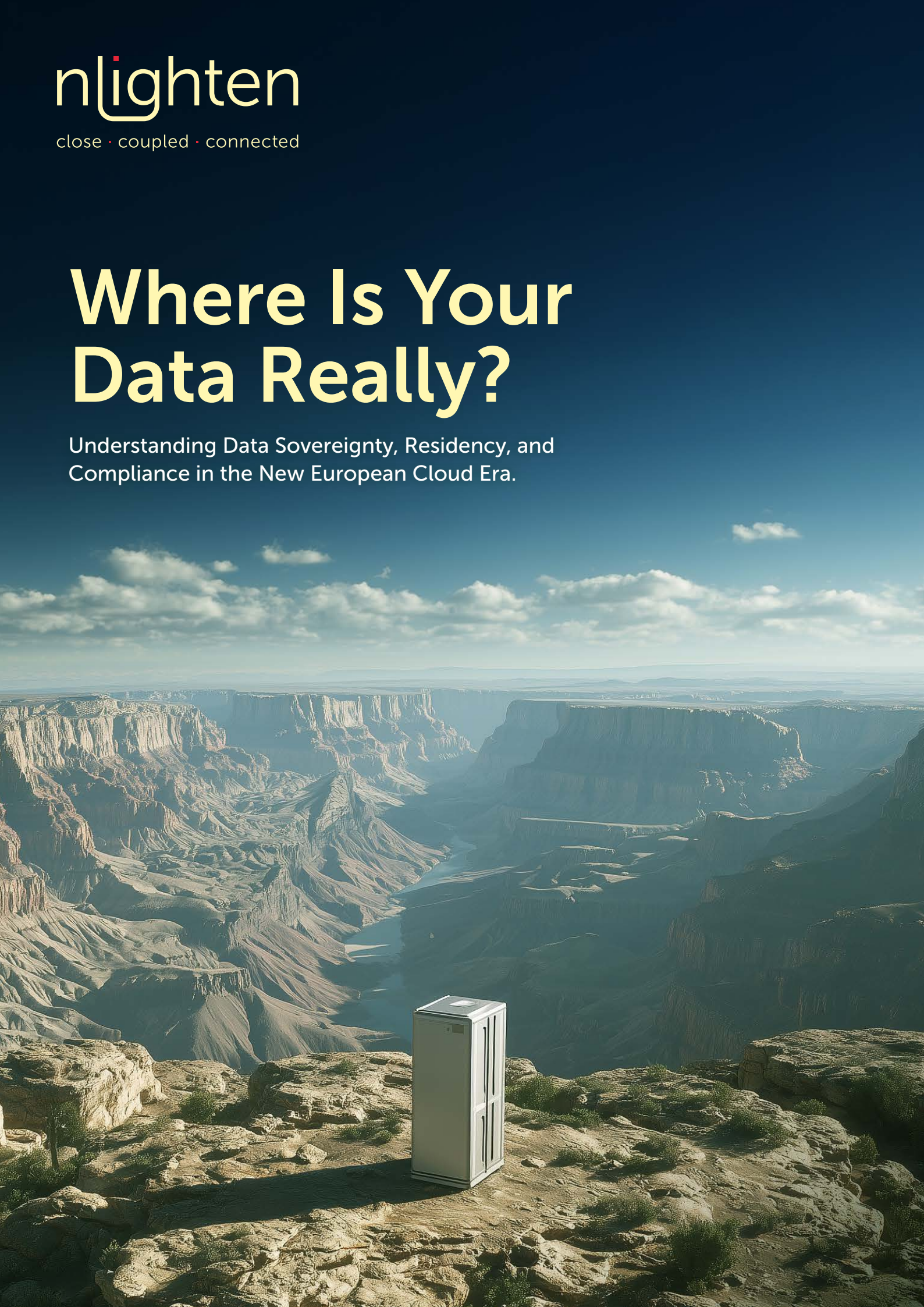


Table of Contents.

Where Is Your Data Really?

Europe is redefining the digital economy around a single idea: trust through control. For too long, data has flowed across borders faster than the laws designed to protect it. The result is a growing gap between where data lives and who governs it. At nLighten, we believe this moment marks a turning point.

As Europe builds its digital future, infrastructure sovereignty begins at the edge — close to users, under European law, powered by sustainable energy. Data sovereignty is no longer a niche compliance concern. It's the foundation for digital competitiveness, innovation, and resilience in the decade ahead.

When people talk about "data sovereignty," they often focus on restriction — what companies can't do. But the real story is empowerment. Sovereignty gives European enterprises the freedom to innovate within trusted legal frameworks.

The General Data Protection Regulation (GDPR) and the new EU Data Act are not barriers — they're guardrails that let innovation scale safely. They ensure that the next generation of AI, healthcare, finance, and industrial IoT can grow on European terms, without foreign exposure or dependency.

"Europe must strengthen its own capacities for hosting, processing and using data, based on European values and rules."

— European Commission, A European Strategy for Data (COM(2020) 66 final)

This is what sovereignty means in practice: local control, legal certainty, and digital independence.

1. The New Era of Digital Responsibility

Data is the new capital of the digital economy — yet few organizations truly know where their data resides, who can access it, or under which laws it falls.

The European Union has made its position clear: data belonging to Europeans must be governed by European law. This principle stems from Article 8 of the Charter of Fundamental Rights of the European Union, which guarantees citizens the right to the protection of personal data concerning them.

The General Data Protection Regulation (GDPR) translates that right into enforceable law. Article 3(2) extends EU jurisdiction globally — applying to any organization processing EU citizens' data — even if that organization is located outside the EU.

However, compliance with GDPR alone no longer guarantees safety. The global cloud economy has created new risks, where data location and data control often diverge.

In 2020, the Court of Justice of the European Union (CJEU) reaffirmed this in its landmark Schrems II (C-311/18) judgment, striking down the EU–US Privacy Shield because U.S. surveillance powers were not limited to what is strictly necessary and therefore incompatible with EU fundamental rights.

Since then, EU regulators have begun enforcing not only data protection, but data sovereignty — the right of EU citizens, companies, and governments to maintain control over their own data under EU law.

2. Data Sovereignty vs. Data Residency — The Crucial Distinction

Many businesses confuse data residency with data sovereignty — but under EU law, the two concepts are very different:

Concept	Definition	Limitation
Data Residency	The Physical location where data is stored or processed	Determines where data sits, but not who controls it or which laws apply
Data Sovereignty	The Legal Jurisdiction that governs access to and ownership of the data	Determines who can legally access or demand that data, even if it's stored elsewhere

3. Enforcement: From Paper Law to Operational Reality

Over the past three years, EU data protection authorities (DPAs) have shifted from guidance to decisive enforcement, focusing on the cross-border flow of personal data and the accountability of controllers.

Examples include Meta's €1.2 billion fine, Vodafone Spain's €8.15 million penalty, Österreichische Post AG's cease order also, disruption to business continuity.

Hamburg DPA (2021)
Issued a formal notice to the Senate Chancellery to stop using Zoom because data could be accessed by U.S. authorities — a direct result of Schrems II (Datenschutz-Hamburg.de).

BayLDA (Bavaria, 2021)
Instructed a German publisher to suspend use of Mailchimp for newsletters until additional safeguards were verified (BayLDA Case).

CNIL (France, 2022)
Issued multiple sanctions against companies using Google Analytics without valid EU transfer mechanisms, stating that "data transfers to the United States are illegal in the absence of adequate guarantees."

Why Fines Are Only Part of the Story
Cease-and-desist orders often inflict more damage than fines.

They can:
- Force critical services offline (e.g., suspension of analytics or email systems).
- Interrupt revenue generation and customer engagement.
- Require emergency migration of workloads to sovereign providers.
- Damage brand trust with regulators and clients.

In short, sovereignty failures disrupt business continuity — the hidden cost few executives anticipate.

4. The European Legal Backbone of Sovereignty

The European Commission's legislative framework reinforces a unified message: European data must remain under European control.

Legal Instrument	Key Provisions for Sovereignty
GDPR (2016/679)	Articles 44-49 restrict international transfers; Article 83(5) sets penalties up to €20 million or 4% of global turnover.
EU Data Act (2023/2854)	Article 5 & Recital 62 require prevention of unlawful foreign access and enforce EU-only jurisdiction for data holders
EDPB Recommendations 01/2020	Oblige data exporters to assess third-country laws and apply supplementary technical/legal measures.
Cybersecurity Act (2019/881)	Establishes certification for secure cloud and ICT service
Digital Decade Policy Programme (2022/2481)	Sets 2030 targets for "Secure, Sovereign and sustainable" digital infrastructure.

5. The Myth of “EU Hosting”

The assumption that using an EU data center equals compliance is increasingly dangerous. If a provider is subject to non-EU jurisdiction, data stored in the EU can still be exposed to foreign access requests. True sovereignty is about control, not coordinates.

6. Turning Compliance into Competitive Advantage

Organizations that treat data sovereignty as a strategic asset — not a cost — gain trust, agility, and long-term resilience. Benefits include legal defensibility, public-sector eligibility, and simplified procurement.

Strategic benefits of data sovereignty:

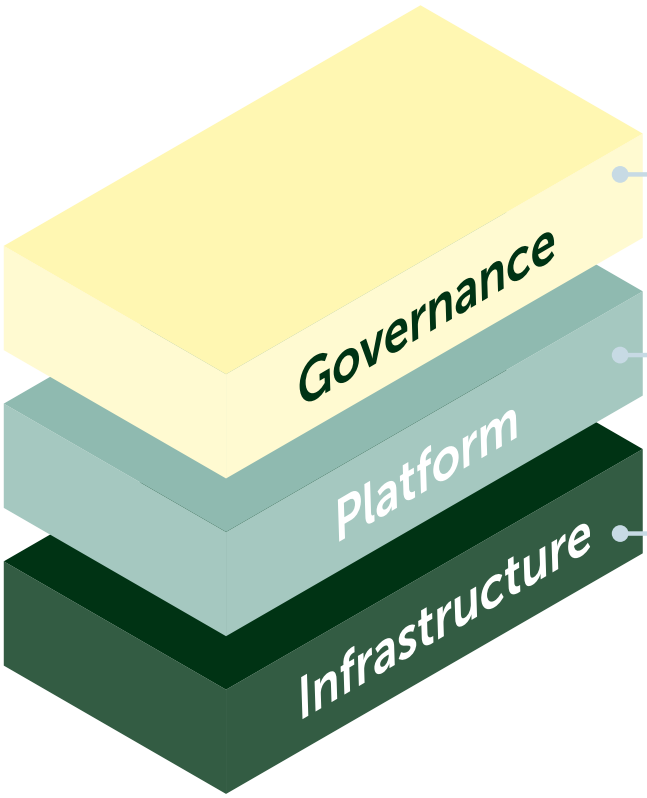
- Trusted relationships with regulators and customers.
- Eligibility for public-sector tenders requiring EU-only data handling.
- Simplified vendor due diligence and procurement.
- Future-proof architecture aligned with the EU Data Act and GDPR.
- Reduced exposure to extraterritorial surveillance laws.

The **European Commission's Digital Decade Policy Programme** (2022/2481) reinforces this opportunity:

"A secure and sovereign digital infrastructure is a precondition for a competitive and trusted European economy."

7. Achieving Full-Stack Data Sovereignty

A complete sovereignty strategy spans three integrated layers:



How compliance is proven.

- Ongoing Data Protection Impact Assessments (GDPR Art. 35).
- Transfer Impact Assessments for non-EU processors
- Contractual Clauses ensuring EU-law supremacy in all sub-processing.

Who controls it.

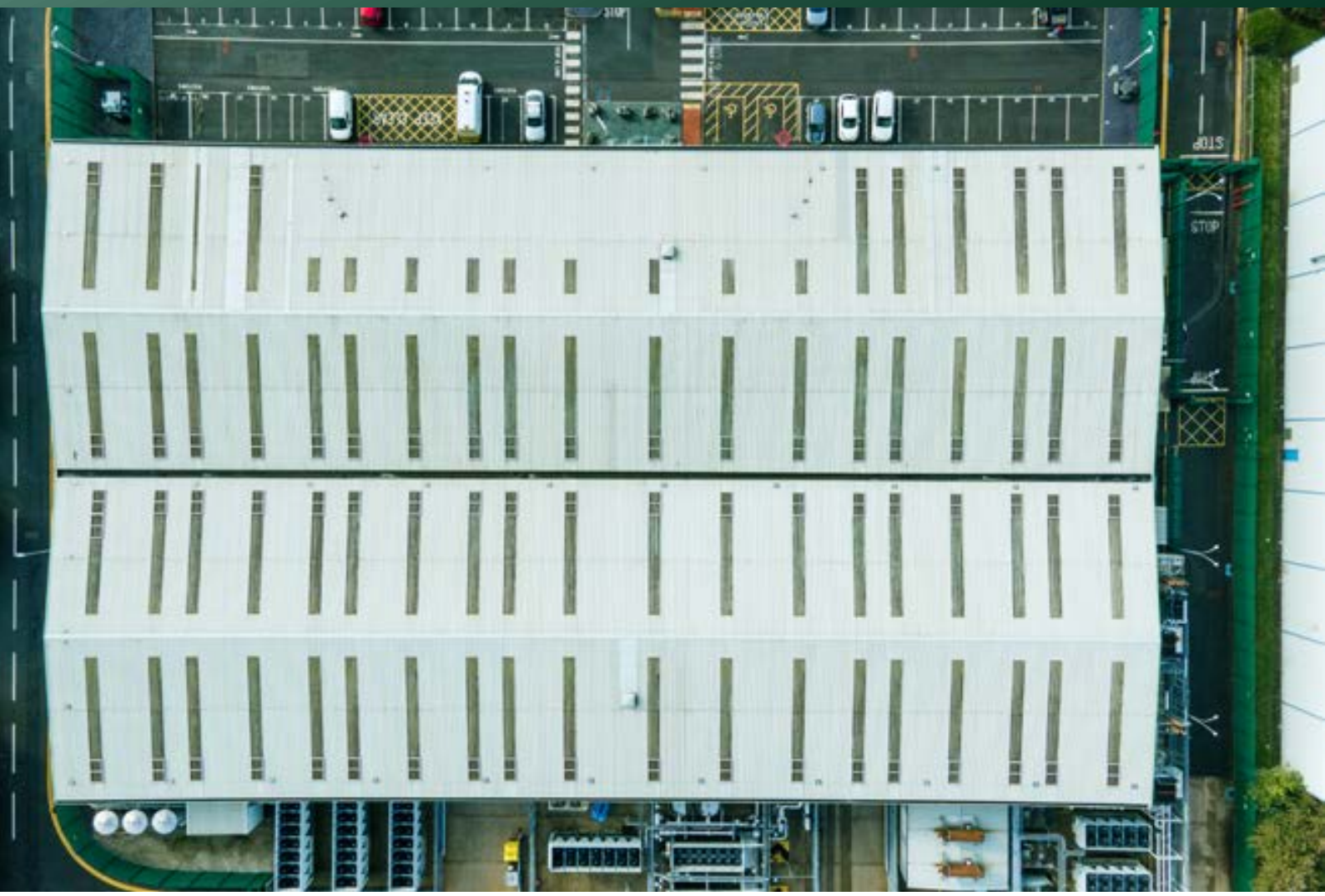
- Cloud and SaaS Services under EU legal jurisdiction only
- EU-held encryption keys and data lifecycle management
- Provider neutrality and portability per EU Data Act Chapter VII

Where data physically lives:

- EU-based, EU-owned data centres.
- ISO 27001 and EN 50600
- Local power efficiency and sustainability compliance under the EU Green Deal.

By aligning these layers, enterprises create compliance-by-design architectures that minimize legal uncertainty and audit burden.

8. nLighten: The Infrastructure Layer of Europe's Digital Sovereignty



nLighten provides the physical foundation for Europe's sovereign digital stack. Its edge data-centre platform spans key European metros, designed for local jurisdiction, low latency, and high efficiency.

9. The Vision: Europe's Sovereign Digital Future

Europe is redefining globalization on sovereign terms through initiatives like Gaia-X, EuroHPC, and the EU Data Spaces. nLighten aligns with this mission to enable enterprises to operate locally, connect globally, and comply seamlessly.

10. Practical Steps

1. Verify Your Jurisdiction: Conduct a legal and technical audit of your cloud and data providers.

Ask: Who ultimately owns the infrastructure and under which law is it governed?

2. Localise Critical Workloads
Deploy core applications and sensitive data inside EU-owned data centres to maintain GDPR and Schrems II compliance.

3. Demand Transparency from Providers
Insist on visibility into data flows, subcontractors, and storage locations. Providers should disclose all sub-processors and compliance frameworks.

4. Embed Sovereignty into Architecture
Design for portability and interoperability — use open APIs, EU-based clouds, and local edge infrastructure to avoid vendor lock-in.

5. Tie Security to Sovereignty
Retain control of encryption keys, monitoring, and incident response within the EU. Align policies with NIS2 and ISO 27001 standards.

11. Conclusion

If your data can be accessed outside the EU, your compliance can be revoked inside it. With the right partners and infrastructure, sovereignty becomes a competitive advantage.

Keep your data close. Keep your control. nLighten —Digital Sovereignty Simplified.

Legal and Policy References

1. GDPR (Regulation (EU) 2016/679) – https://eur-lex.europa.eu/eli/reg/2016/679/oj

2. EU Data Act (Regulation (EU) 2023/2854) – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854

3. CJEU Judgment C-311/18 ("Schrems II") – https://curia.europa.eu/juris/document/document.jsf?docid=228677

4. EDPB Recommendations 01/2020 – https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

5. AEPD Resolution PS/00321/2021 (Vodafone Spain) – https://www.aepd.es/en/documento/ps-00321-2021.pdf

6. Austrian DSB Decision D124.692/0009-DSB/2019 (Österreichische Post AG) – https://www.dsb.gv.at

7. Hamburg DPA Press Release on Zoom (2021) – https://datenschutz-hamburg.de/pressemitteilungen/

8. Bavarian DPA Mailchimp Case (2021) – https://www.lda.bayern.de/

9. CNIL France Decisions on Google Analytics (2022) – https://www.cnil.fr/

10. European Commission – A European Strategy for Data (COM(2020) 66 final) – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066