asteyo

WHITE PAPER · EU DIGITAL SOVEREIGNTY BY DESIGN

EU Digital Sovereignty by Design

Why regulated mid-market companies are rethinking who builds and operates their software.

Dr. Thomas Wolenski, CSO · Alexandru Bereczki, CEO

June 2026 · v0.4

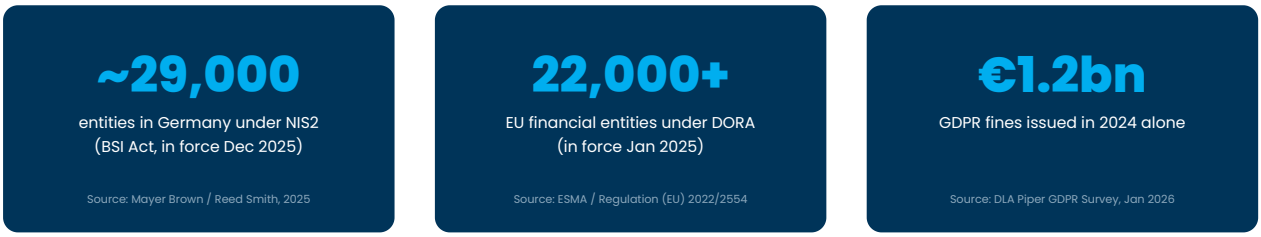
Asteyo SRL, Cluj-Napoca · office@asteyo.com · asteyo.com

EXECUTIVE SUMMARY

A governance question, not just a cost question

Germany's NIS2 Implementation Act (in force since 6 December 2025) expanded the number of regulated organisations from roughly 4,500 to ~29,000. Together with GDPR, DORA and the EU Data Act, these rules make one question a board-level matter: who builds and operates your software, under which legal order?

This paper is written for the ambitious mid-market business — typically 200 to 1,000 employees — that is now an "important" or "essential" entity under NIS2, or a smaller financial institution in scope of DORA. It sets out the regulatory landscape, quantifies the hidden compliance cost of the wrong sourcing model, and is precise about the difference between *where data is hosted* (your cloud decision) and *who builds and operates your systems* (your delivery-partner decision). Asteyo addresses the second.



Left to right: NIS2 Germany (BSI Act, Dec 2025); DORA (ESMA, Jan 2025); GDPR fines 2024 (DLA Piper, Jan 2026).

Three things this paper establishes

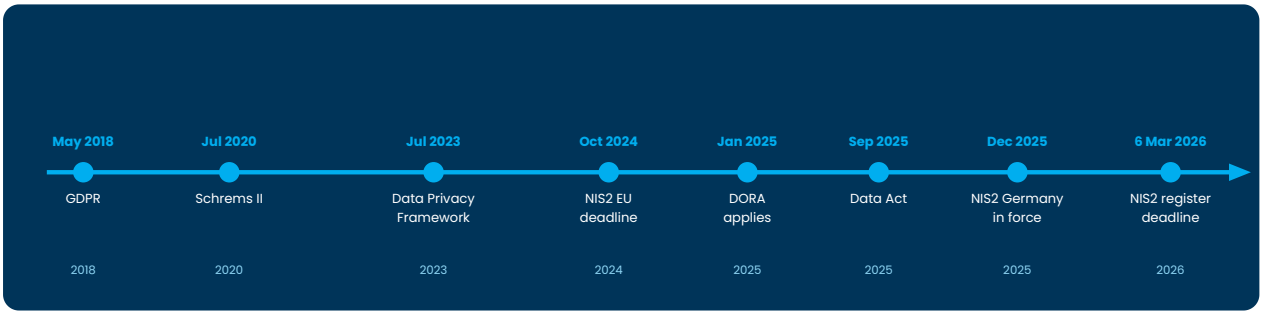
- The regulatory wave is real and the window for deferring action has closed.
- The compliance overhead of non-EU delivery models is material and largely hidden in headline day rates.
- EU-sovereign nearshore is a people-and-jurisdiction decision, not a hosting decision — and Asteyo is precise about exactly that scope.

01 · WHY NOW

The regulatory wave, 2018–2026

Four interlocking regulations now define what "compliant IT sourcing" means for a regulated mid-market company in the DACH region.

- **GDPR (2018).** The baseline that has not gone away. Cumulative fines now exceed €7 billion; in 2024 alone regulators issued roughly **€1.2 billion**,[2] including €310m (LinkedIn), €251m (Meta) and €290m (Uber for transferring driver data to the US).[3]
- **NIS2 — Germany (December 2025).** Expanded the national supervised-entity count from ~4,500 to ~29,000,[1] reaching manufacturing, energy, health, logistics and digital infrastructure. Supply-chain security and registration (deadline 6 March 2026[7]) are explicit obligations. Management now bears direct personal accountability for cybersecurity.
- **DORA (January 2025).** Covers 22,000+ EU financial entities.[9] Chapter V reshapes every IT procurement: a Register of Information, audit and exit rights (Article 30), sub-processor transparency and concentration risk assessment. In November 2025 the ESAs published the first list of 19 Critical ICT Third-Party Providers (CTPPs), including AWS, Microsoft, Google Cloud, Oracle, SAP and Deutsche Telekom.[11]
- **EU Data Act (September 2025).** Grants clients a legal right to switch providers: contractual, technical and commercial obstacles must be removed, and switching fees phased out by January 2027.[12]



Regulatory milestones 2018–2026. Sources: EUR-Lex, BSI, ESMA, European Commission.

> **One-time implementation cost estimate:** The German government estimated ~€2.2 billion in one-time NIS2 implementation costs across the national economy.[8] Cybersecurity is now an explicit duty of company management — not just the IT department.

02 · THE US TRANSFER QUESTION

A legal but fragile bridge

The EU-US Data Privacy Framework (DPF, July 2023) is the current operative legal basis for transfers to DPF-certified US companies. It survived its first court challenge in September 2025 — but the bridge remains under strain.

- **The appeal continues.** Latombe filed Case C-703/25 P at the CJEU on 31 October 2025; no hearing date has been set.[4]
- **Political foundations have weakened.** In January 2025 three of five PCLOB members — the body underpinning DPF safeguards — were removed.[5]
- **FISA §702 and the CLOUD Act remain in force.** US providers remain compellable by US law to disclose data held anywhere in the world.

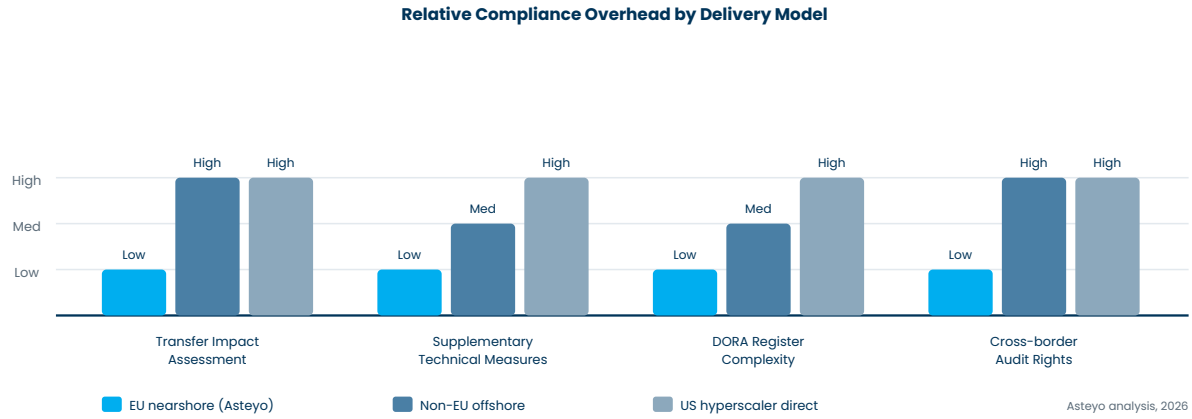
For a regulated buyer, US transfers remain legal but depend on a repeatedly litigated, politically exposed mechanism. A provider incorporated in the EU, operating under EU law, with EU-based staff and no US parent, removes that uncertainty — it does not manage it.

EU-based operations: Asteyo's service delivery stays inside the EU legal perimeter.

What the wrong sourcing model actually costs

An offshore engagement running on a US hyperscaler with a sub-processor chain across three jurisdictions can require substantial compliance investment before it is appropriate for critical NIS2 or DORA work. Headline day rates hide that burden.

- **Transfer Impact Assessment** — a formal legal analysis before personal data leaves the EU; in complex chains, TIAs cascade across prime contractor, cloud provider and each sub-processor.
- **Supplementary technical measures** — where a TIA is unfavourable, encryption or pseudonymisation with EU-controlled keys adds cost and operational friction.
- **Cross-border audit rights** — exercising DORA Article 30 audit rights in a third country is logistically and legally harder, and may collide with local laws restricting inspection.
- **DORA Register complexity** — a multi-jurisdiction chain complicates the Register of Information; supervisors are actively reviewing submissions.
- **Incident and concentration exposure** — ENISA Threat Landscape 2025 ranks supply-chain compromise among top forward-looking concerns.[13] The cost of a breach originating in a third-party provider can dwarf years of day-rate savings.



Relative compliance overhead by delivery model (qualitative; Asteyo analysis, 2026). Lower bars = lower regulatory burden.

04 · WHAT "EU-SOVEREIGN NEARSHORE" ACTUALLY MEANS

A jurisdiction decision, not a hosting decision

"Digital sovereignty" conflates two distinct questions. Confusing them leads to bad procurement decisions.

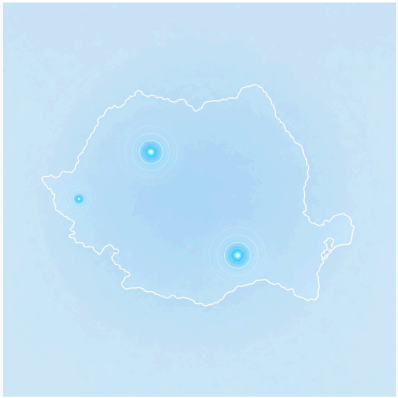
Where is data hosted?
This is your cloud decision. AWS European Sovereign Cloud, Microsoft EU Data Boundary and Google Sovereign Controls are serious answers to this question, and a mature buyer should evaluate them on their merits.

Who builds, operates, and can access the system?
This is your delivery-partner decision: which people write the code, hold the credentials, see the data and respond to incidents — and under which legal order they sit.

Asteyo addresses the second question, and is precise about it. We do not claim to solve your cloud sovereignty. What we provide is delivery under EU jurisdiction: the engineers, their access, their employer and their sub-processors all sit inside the EU legal perimeter. For most regulated mid-market buyers, the people-and-access layer is exactly where offshore models create the hardest-to-close compliance gaps.

Verifiable attributes of EU-sovereign delivery

- **EU jurisdiction over the provider** — incorporated in an EU member state, not compellable by a third-country government.
- **EU-based processing and access** — all access to client data by the provider's staff happens from within EU territory.
- **Transparent sub-contracting** — the full sub-processor chain is EU-domiciled or covered by a valid, documented transfer mechanism.
- **Audit and exit rights as standard** — offered as baseline terms, not premium concessions.
- **Independent security certification** — ISO/IEC 27001 or equivalent.



Romania — EU member state since 2007, same time zone as DACH clients (max 1h offset).

05 · HOW ASTEYO FITS

Compliant by design, honest about scope

Asteyo SRL is incorporated in Cluj-Napoca, Romania — an EU member state since 1 January 2007. This is the architecture, not a posture retrofitted onto an existing model.

Romania's IT sector employs an estimated 200,000 to 250,000 software professionals. Cluj-Napoca hosts an estimated 20,000 to 23,000 IT professionals across ~450 companies, anchored by two of the larger technical universities in Central and Eastern Europe.[15] Engineers work in the same time zone as DACH clients (maximum one-hour offset), enabling real-time collaboration with no overnight handoff lag.

- **GDPR-native by design.** Asteyo has operated under GDPR since inception. There is no pre-2018 compliance debt and no legacy data-sharing agreements.
- **ISO 27001 and ISO 9001.** Asteyo holds ISO/IEC 27001:2022 and ISO 9001:2015 certification, issued by SYSTEMA (IAS/IAF-accredited), valid December 2025 to December 2028 (SoA dated 10 August 2025). Certified scope: custom, client-oriented software development.
- **DORA and NIS2 contract support.** Working with our EU legal counsel, we structure engagements to meet relevant requirements: audit and inspection rights; exit and termination rights aligned to DORA Article 30; Register of Information support; incident-reporting cooperation built into the SLA.
- **Provider resilience, addressed directly.** Every engagement is structured so the client can take work back or move it, with knowledge transfer as a contractual deliverable. The Build-Operate-Transfer path (Stage 3) is the strongest possible answer to lock-in: the capability can become yours.

200k+
IT professionals in Romania
4th-largest tech workforce in EU[14]

~22k
IT professionals in Cluj
~450 companies, 2 major tech universities[15]

Max 1h
time-zone offset to DACH
Full working-day overlap, no overnight lag

ISO 27001 SYSTEMA · ISO 9001 SYSTEMA · EU · GDPR

SYSTEMA (IAS/IAF-accredited) · Valid Dec 2025–Dec 2028 · Scope: custom client-oriented software development

06 · ENGAGEMENT MODEL

A path for risk-averse buyers

The standard CIO/CISO objection to any new vendor: how do I know this works before I depend on it for something critical? Asteyo's three-stage model answers that by design, not by assurance.

STAGE 1

Specialist Engagement

A single specialist or small pod joins an existing team for a defined scope — a natural compliance perimeter, easy to document in a DORA register or NIS2 supplier assessment. EU jurisdiction from day one. Exit at any time.

STAGE 2

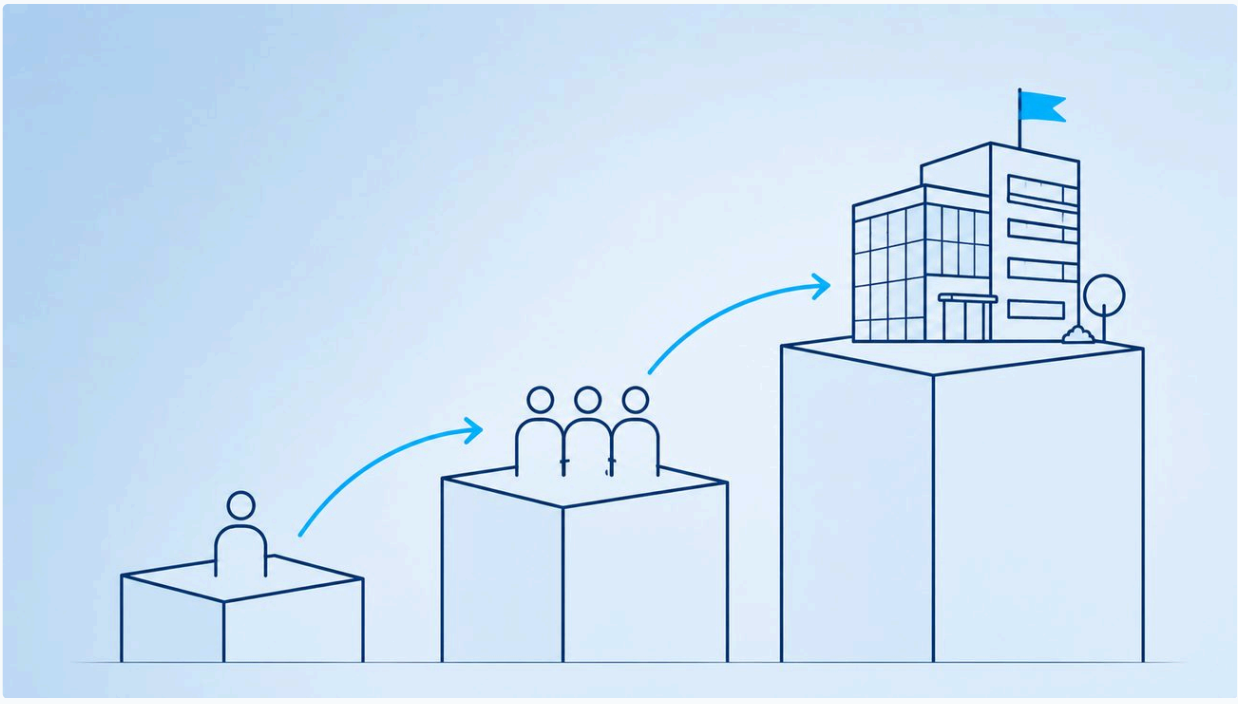
Dedicated Team

Four to twelve engineers operating as a named, stable unit under the client's security and quality frameworks. A stable, documentable provider relationship of the kind the DORA register contemplates.

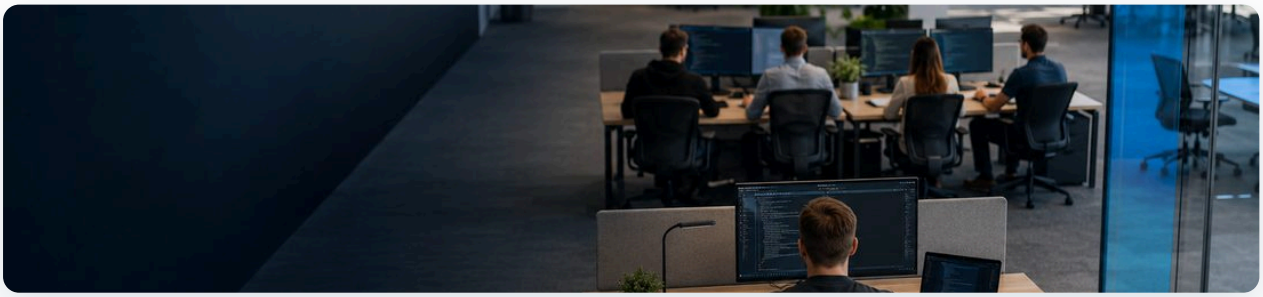
STAGE 3

Build-Operate-Transfer (BOT)

Asteyo builds and operates a dedicated nearshore capability, then progressively transfers operational control and ownership to the client. A wholly owned, EU-domiciled delivery centre.



From specialist engagement to client-owned delivery centre. Every stage is auditable and reversible.



Asteyo delivery teams grow with the client — from specialist pod to a scalable, stable unit.

asteyo

"

For a regulated mid-market company, the compliance question and the delivery question are now the same question: who has access to your systems, under which law, and how do you prove it to a regulator?

ASTEYO EU DIGITAL SOVEREIGNTY THESIS, 2026

07 · NEXT STEP

Start with a conversation

The window for deferring this question has closed. Germany's NIS2 obligations are in force with registration due by 6 March 2026. DORA's third-party requirements are live. The Data Act's switching rights apply.

A supply-chain gap audit typically surfaces one or more of:

- A provider incorporated outside the EU supporting a critical or important function.
- A US-hyperscaler dependency without an EU-sovereign fallback plan.
- A sub-contracting chain with third-country sub-processors not covered by a current TIA.
- Contract terms without audit and exit rights sufficient for DORA Article 30 or a NIS2 supplier assessment.

Get in touch

Asteyo's engagement starts with a conversation. We support gap analyses for specific workstreams, walk through how our contracts map to your DORA register or NIS2 supplier requirements, and outline what a Stage 1 specialist engagement looks like for a project you have in flight.

office@asteyo.com · asteyo.com

ISO 27001 SYSTEMA · ISO 9001 SYSTEMA · EU · GDPR

ISO/IEC 27001:2022 & ISO 9001:2015 certified · SYSTEMA (IAS/IAF-accredited) · Valid Dec 2025–Dec 2028

Asteyo — Reliability · People · Partnerships. We get things done.

REFERENCES

Sources & notes

Figures are cited to their primary or best-available public sources. Regulatory scope figures are based on government and law-firm analyses; they represent estimates that may vary by source and methodology.

1 **Mayer Brown**, "Cyber Rules for Essential and Important Entities Take Effect in Germany (NIS2 Implementing Law)," Dec 2025. mayerbrown.com – Reed Smith, "Finally: Germany enacts its NIS2 law," 2025. reedsmith.com

2 **DLA Piper**, "GDPR Fines and Data Breach Survey: January 2026" (cumulative fines >€7bn; ~€1.2bn in 2024). CMS GDPR Enforcement Tracker. enforcementtracker.com

3 **Irish DPC**, decisions on LinkedIn (€310m) and Meta (€251m), 2024. Dutch Autoriteit Persoonsgegevens, Uber fine (€290m), 2024. autoriteitpersoonsgegevens.nl

4 **IAPP**, "European General Court dismisses Latombe challenge, upholds EU-US DPF," Sep 2025. iapp.org – Appeal: Case C-703/25 P (CJEU), filed 31 Oct 2025.

5 **WilmerHale**, "European Court of Justice to Review Challenge to EU-U.S. Data Privacy Framework," Dec 2025 (incl. PCLOB membership removals, Jan 2025). wilmerhale.com

6 **European Commission**, infringement proceedings / reasoned opinion on NIS2 non-transposition, May 2025. Morrison Foerster, "Flipping the NIS2 Switch," Dec 2025. mofo.com

7 **Privacy World (Squire Patton Boggs)**, "Germany Implements NIS2: Registration portal will open on January 6, 2026," Dec 2025 (registration due by 6 March 2026). privacyworld.blog

8 **Greenberg Traurig**, "NIS2 in Germany: The New BSI Act Makes Cybersecurity a Board-Level Issue," Dec 2025. gtlaw.com

9 **ESMA**, "Digital Operational Resilience Act (DORA)." esma.europa.eu – Regulation (EU) 2022/2554 (EUR-Lex). Audit/contract clauses: DORA Article 30.

10 **National competent authorities** collected first Registers of Information from financial entities in April 2025 (deadlines per member state).

11 **European Supervisory Authorities (EBA/EIOPA/ESMA)**, "ESAs designate critical ICT third-party providers under DORA," 18 Nov 2025 (19 CTPPs: AWS, Microsoft, Google Cloud, Oracle, SAP, Deutsche Telekom etc.). eiopa.europa.eu

12 **European Commission**, "Data Act," Regulation (EU) 2023/2854, applicable from 12 Sep 2025; switching fees phased out by 12 Jan 2027. digital-strategy.ec.europa.eu

13 **ENISA**, "ENISA Threat Landscape 2025," October 2025. enisa.europa.eu

14 **Index.dev**, "Software Development in Romania: Market Analysis & Hiring Guide for 2025." Romania Insider, "Over one in five Romanian university graduates are engineers, the highest share in EU." index.dev

15 **KiTalent**, "Cluj-Napoca's Tech Sector Is Booming," 2025. kitalent.com

Contact: office@asteyo.com · asteyo.com