SME - Surviving the "Compliance Cliff"

14 April 2026 • 7 min de lecture

SME NIS2 DORA AI Act

Originally written in French and translated into English with AI assistance.

You are an SME developing AI software. Your product sorts CVs, assesses creditworthiness, personalizes training paths, or scores credit risks. The market is responding well. POCs are turning into contracts. The runway appears sustainable.

Then comes the due diligence file from the large enterprise client (bank, hospital, energy operator). Data flow mapping, proof of non-training on client data, explainability logs, AIBOM, provenance attestations, AI Act + NIS2/DORA compliance. No complete and timestamped response? The relationship ends before the demo even starts.

This is the reality quietly taking shape for SMEs producing AI software that sells to essential or important entities. You'll need to clip in, tighten the harness, adjust the helmet, and begin the ascent of the Compliance Cliff.

This article offers a precise breakdown, built on the official texts currently in force. We will dismantle the traps, quantify the real impacts, and above all show a path that resilient AI software companies are already following: transforming compliance into automated **Evidence-as-Code**.

The Classification Trap: High Risk by Default for Most AI Software in HR Tech, Fintech, and EdTech

The AI Act is unambiguous: High Risk cases include:

- **Employment and worker management**: CV analysis and filtering, candidate evaluation, performance prediction, promotion, task allocation, or behavioral monitoring.
- **Education and training**: assessment of learning outcomes, access to institutions, fraud detection.
- **Essential services**: creditworthiness assessment, credit scoring, insurance pricing based on profiling.

If your AI software influences an individual decision with significant human impact, you are **High Risk** by default. No comfortable gray area for SMEs producing these tools.

Concrete Consequences:

- Mandatory Quality Management System (QMS).
- Risk assessment across the entire lifecycle.
- Full traceability of training data.
- Exhaustive technical documentation + registration in the EU database.
- Automatic logging of operations.
- Transparency ("You are interacting with an AI") and effective human oversight.

Real Cost for an SME: according to recent studies, the initial setup of a High Risk system ranges from €50,000 to €250,000 (low end €10K–€70K for simpler cases), plus €50,000 per year in maintenance. For an SME with €400K in revenue, this is often a runway killer.

Immediate Lever for Software Producers: Pivot your product promise today. Move from "Our AI evaluates and decides" to "Our AI **assists** the human decision-maker with explainable recommendations." This reclassifies the system as Limited Risk (transparency obligations only). This is *risk mitigation by design* and buys you 12 to 18 months. Caution: classification depends on the intended use declared in the technical documentation. A simple marketing change is not enough if the real effect remains decisional.

NIS2 / DORA: Your clients become your compliance auditors

NIS2 does not target all companies: it concerns essential and important entities (18 sectors, generally >50 employees or >€10M turnover). DORA is even more targeted: financial sector only.

But the trap lies in the **supply chain**. NIS2 requires covered entities to secure their ICT/AI suppliers: they must assess the vulnerabilities of their direct suppliers and take into account the quality of their cybersecurity practices.

DORA makes financial entities fully responsible for the resilience of their third-party ICT providers: contract registers, continuous due diligence, draconian contractual clauses, right to audit, and exit strategy.

Practical consequence: Procurement and IT departments now demand an **exhaustive due diligence dossier** (often several dozen questions) before any new contract. No ready Trust Pack? You are removed from vendor lists.

Immediate Solution for Software Producers: Prepare a **standardized Trust Pack** (10-15 pages): data mapping, clear terms of use, example AIBOM/SBOM, non-training attestation, and immutable logs. Turn the constraint into an advantage: "We are the only SME whose software will never endanger your NIS2/DORA compliance."

PLD: Presumptions of Defect and Causation That Dramatically Increase the Burden for SMEs

The Product Liability Directive (PLD), whose national transposition must occur by December 9, 2026 at the latest, explicitly includes software and AI systems.

Once transposed, it will introduce rebuttable presumptions of defect and causal link in several cases:

- Non-disclosure of evidence by the manufacturer.
- Non-compliance with mandatory safety requirements (including the AI Act).
- Obvious malfunction during reasonably foreseeable use.
- Excessive difficulty due to technical/scientific complexity (the famous AI “black box”).

For an SME producing software without exhaustive logs, technical explainability, and cryptographically verifiable traceability, rebutting these presumptions in court becomes extremely costly (judicial expertise: €50-120K over 12-18 months).

The Only Real Shield: Immutable, timestamped, cryptographically signed logs + explainability + complete supply chain traceability (in-toto attestations, verifiable provenance). This is no longer a technical option: it is your judicial insurance policy.

The Hidden Advantage : Regulatory Sandboxes

Article 57 of the AI Act: each Member State must establish at least one operational regulatory sandbox by August 2, 2026 at the latest. Priority and free access for SMEs/startups is provided for in Article 58 and the Commission’s guidelines.

In France, the CNIL and competent authorities run ongoing application rounds. You test your AI software under supervision, receive free legal advice, temporary immunity, and a certificate that reassures large accounts.

SMEs producing AI software that apply early will gain a significant head start and decisive credibility.

The 5 Actions That Surviving AI Software-Producing SMEs Have Already Launched

1. **Map Your Classification**: Use Annex III and the Commission's guidelines. High Risk? Identify the feature to pivot.
2. **Build Your Trust Pack**: AI terms of use, data flow mapping, proof of non-training on client data, enriched SBOM example, and technical documentation (AIBOM being a good sectoral practice).
3. **Secure your contracts**: Update T&Cs and liability clauses to limit misuse.
4. **Invest in Explainability + Immutable Logs**: This is your PLD defense.
5. **Shift to Evidence-as-Code**: This is where the survival of AI software producers is being decided. Successful SMEs no longer manage compliance manually. They deploy sovereign DevSecMLOps platforms that automate everything:
    - Automatic Policy-as-Code gates that block any promotion if the maturity score is not reached.
    - Multi-dimensional maturity framework (data, model, security, governance, operations) with a mandatory minimum global score.
    - End-to-end cryptographic traceability (SLSA level 3+ attestations, immutable logs, transparency registry).
    - Automatic Evidence Locker that generates enriched SBOMs, AIBOMs, maturity radar charts, and signed attestations to answer a client questionnaire in 5 minutes.
    - Progressive deployments (Canary/A/B) coupled with real-time compliance metrics.

These tools turn regulation into a **competitive moat**: large accounts pay more for software that never creates compliance exposure.

Conclusion: The Wall Is Already Here. AI Software Producers Have the Choice Between Suffering or Becoming the Bridge.

High Risk obligations become fully applicable in August 2026. The first fines (up to €35M or 7% of global turnover) are coming. Suppliers will also start getting dropped.

You still have 4 to 6 months to pivot, apply to sandboxes, build your Trust Pack, and adopt Evidence-as-Code.

The winners of 2027 will not be those with the most beautiful demo.
They will be the AI software-producing SMEs that have turned European compliance into a superpower: end-to-end cryptographic traceability, continuously measured maturity, and an audit-ready trust dossier generated instantly.

> *And if, tomorrow, the ability to sign a contract no longer depended on your product... but on your ability to instantly produce a complete and enforceable trust dossier — are you ready today?*

Lego VII - The regulatory cliff for SME

The opinions expressed in this article are strictly personal and do not necessarily reflect those of my employer. The content is provided for information purposes only and does not constitute legal advice. This article explores emerging architectural concepts and analyzes market trends.

Eric Blaudez - AI Innovation Strategist & Technical Lead
SME - Surviving the "Compliance Cliff"

Les opinions exprimées sur ce site sont strictement personnelles et ne reflètent pas nécessairement celles de mon employeur. Les contenus sont fournis à titre informatif et ne constituent pas un conseil juridique.