Nemko Digital

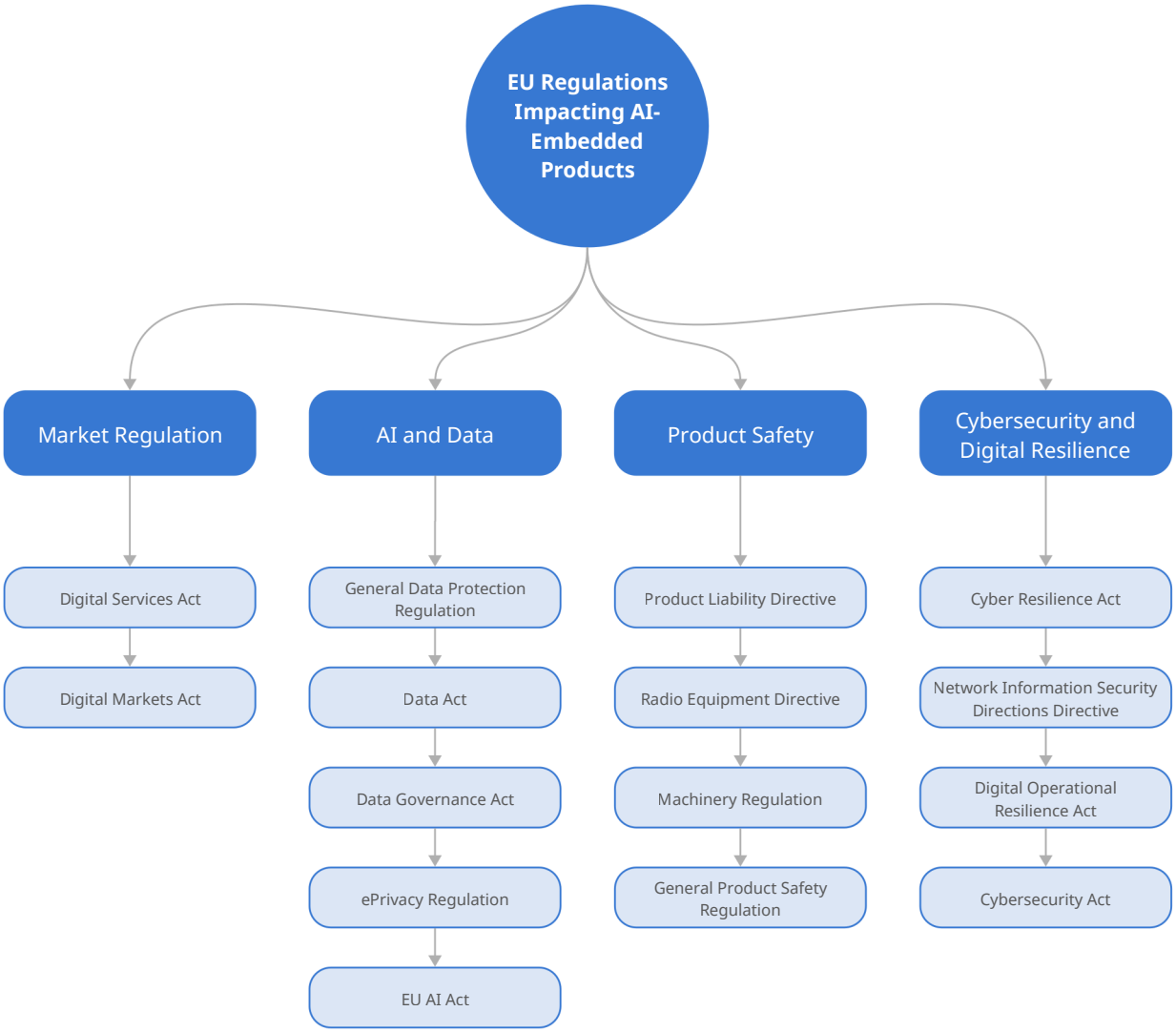
# Product Regulation in the Age of Embedded AI

# Why AI Trust Must Extend Beyond Algorithms

Artificial intelligence is often discussed through the lens of data protection, ethics, and algorithmic transparency. However, as AI systems become increasingly embedded in physical products, another regulatory dimension is gaining importance: product regulation.

AI is no longer confined to digital platforms or decision-support software. It is integrated into industrial systems, consumer electronics, HVAC systems, medical devices, smart cameras, robotics, and IoT devices.

When AI becomes part of a regulated product, compliance is no longer governed solely by AI-specific legislation. Instead, it intersects with product safety frameworks, market regulation, and other digital regualtions (on data and cyber) that contribute to the shaping of AI-embedded products. This intersection significantly reshapes how AI must be designed, assessed, and maintained.



# From Software Governance to Product Governance

Traditional AI governance frameworks focus on bias and discrimination, transparency and explainability, human oversight, data governance, and fundamental rights, among many other principles that support the development and deployment of trustworthy AI.

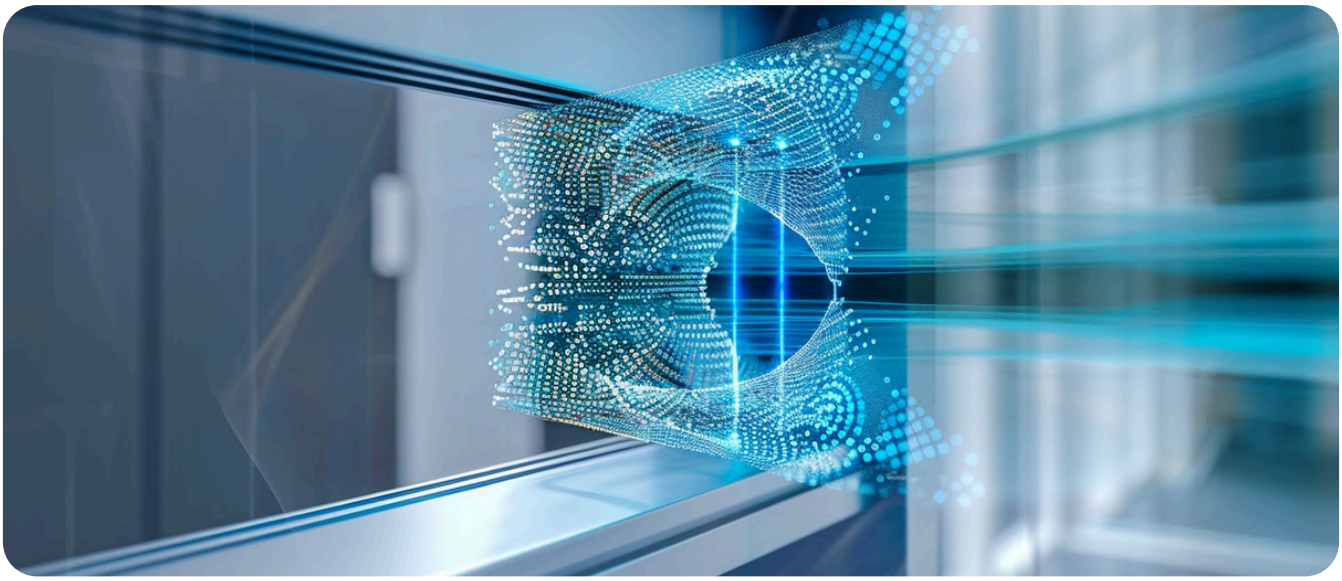
Product regulation, by contrast, focuses on mechanical and electrical safety, pressure containment, electromagnetic compatibility, cybersecurity, physical risk to persons or property, and conformity assessment before market access.

When AI is embedded in hardware, these focus points converge.

The compliance analysis shifts from "Is the model fair?" to also include:

- What happens if the model malfunctions?
- Does AI influence safety-critical parameters?
- Could adaptive behaviour invalidate prior safety certification?
- Does the integration of AI change the product's regulatory classification?

These are product safety questions, not purely AI governance questions.



# How the EU AI Act classifies AI in Products

When discussing EU AI regulation, we are primarily referring to the EU AI Act, the first comprehensive horizontal regulation governing AI systems across the European Union.

The AI Act establishes a risk-based framework that classifies AI systems into prohibited, high-risk, limited-risk, and minimal-risk categories, with escalating compliance obligations.

While the EU AI Act provides a harmonised framework, Member States are developing complementary initiatives to operationalise supervision and enforcement.

**Examples of National Implementation**

**Italy** has adopted a national AI law (132/2025) that clarifies sectoral oversight, introduces enforcement mechanisms (including sanctions for misuse), and designates competent authorities responsible for implementation.

Similarly, Spain has established the Spanish Agency for Artificial Intelligence Supervision (AESIA) and is advancing national governance measures to support enforcement of the AI Act.

These initiatives do not replace the AI Act. Rather, they shape how it is applied in practice — including how AI embedded in regulated products is supervised and assessed.

For manufacturers, this reinforces an important point: AI compliance must be monitored not only at EU level, but also through the lens of national enforcement and sectoral interpretation.

Under the AI Act, an AI system becomes high-risk under Article 6 where:

1. *It is intended to be used as a **safety component of a product** subject to third-party conformity assessment under EU harmonisation legislation; or*
2. ***It is itself a product** covered by EU harmonisation legislation listed in Annex I subject to third-party conformity assessment.*

This is where AI regulation and product law directly intersect.

# The “Safety Component” Threshold

The AI Act defines a safety component as a component that fulfils a safety function or whose failure endangers health, safety, or property.

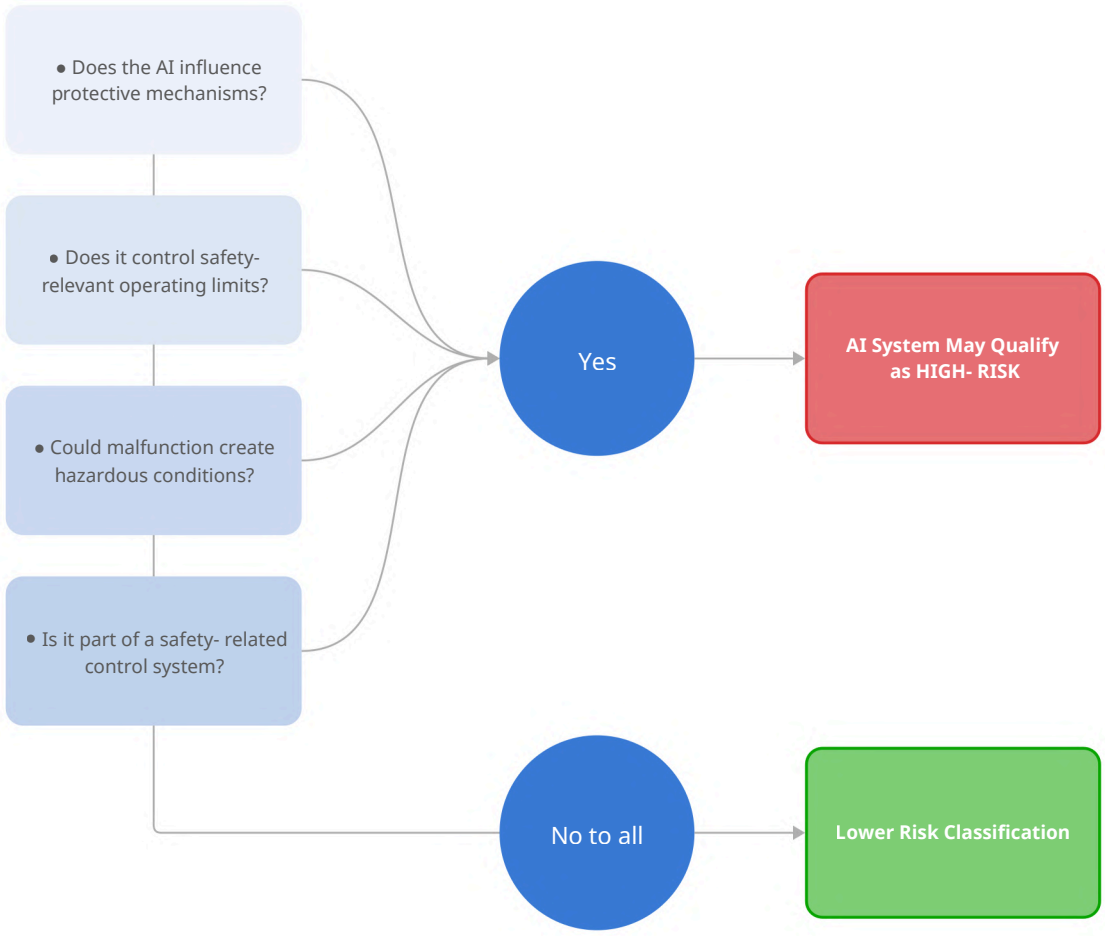
For embedded AI, the practical assessment includes:

- Does the AI influence protective mechanisms?
- Does it control safety-relevant operating limits?
- Could malfunction create hazardous conditions?
- Is it part of a safety-related control system?

If so, the AI system may qualify as high-risk.

## The Safety Component Threshold

Does Your Embedded AI Qualify as High- Risk Under the EU AI Act?



# When AI Is Itself a Regulated Product

AI may also qualify as high-risk when it is itself a regulated product under sectoral legislation. But how can that be? Take for example the Medical Device Regulation, which recognises standalone software as a medical device where it is intended for medical purposes.

**Regulation (EU) 2017/745 on Medical Devices**

*"Software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device."* (Preamble 19)

*"'Medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes (...)"* (Article 2)

This definition may be used to support the interpretation that an AI system alone or embedded in a product used for medical purposes can itself be considered a product covered by Union harmonisation legislation under the AI Act.

However, this interpretation remains subject to further guidance. While current examples indicate the intended direction, additional clarification from the European Commission is expected.

In practice, intended purpose and the functional role of the AI system remain central to evaluating its regulatory implication in other product regulation.

# Beyond the AI Act: The Broader Shift in Product Regulation

Focusing exclusively on the AI Act risks missing the larger regulatory shift.

The AI Act is only one piece of the puzzle.

Even if an embedded AI system does not qualify as high-risk under the AI Act, product legislation may still impose significant obligations. AI increasingly interacts with established frameworks governing machinery, medical devices, radio equipment, pressure equipment, general consumer safety, cybersecurity, and market surveillance of products.

Most of these frameworks were not written with adaptive, self-learning systems in mind — yet they now apply to products that contain them.

The real transformation is not simply that AI is regulated. It is that product regulation must now account for adaptive, probabilistic, software-driven behaviour inside physical systems. We already see this shift happening by taking a look at the General Product Safety Regulation (GPSR), that came into force December 13, 2024. It states that products must not pose risks to physical or mental health, explicitly addressing hazards from AI algorithms and cybersecurity threats. Under this regulation, even non-high risk AI must consider: 1) potential risks from algorithmic bias or faulty decision-making, 2) unintended behaviors in AI system deployment, and 3) comprehensive safety monitoring and rapid response capabilities.

**Over time, product frameworks, like the GPSR, will inevitably evolve to accommodate the reality of AI embedded in products. Make sure to stay alert of these changes by monitoring the regulatory landscape.**

# The Core Challenge: Dynamic Systems in Static Frameworks

Traditional product conformity frameworks assume: Stable system architecture, predictable behaviour, fixed risk profiles, clearly defined updates...

But AI challenges those assumptions.

Adaptive behaviour, data-driven optimisation, remote updates, and model retraining introduce regulatory questions such as:

- When does a software update trigger re-certification?
- Can post-market learning affect the original safety assessment?
- How should manufacturers manage version control for adaptive systems?
- What constitutes a “substantial modification” in AI-enabled products?

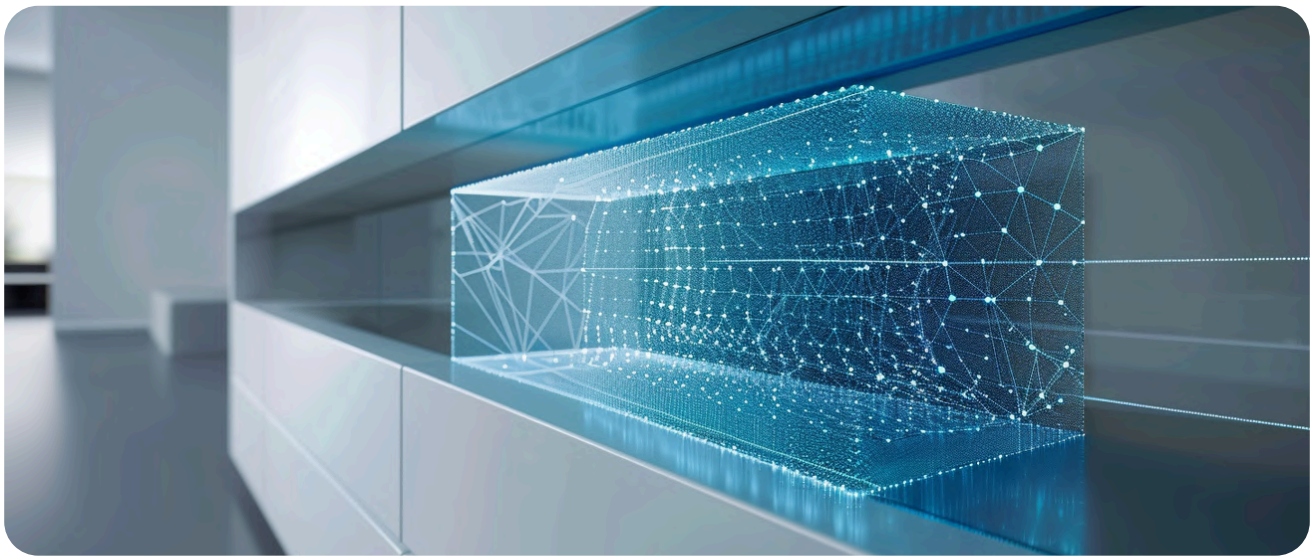
These questions extend far beyond the AI Act and will increasingly be addressed through evolving standards and industry practice.

## The Key Takeaway

As AI continues to move from digital platforms into safety-critical hardware, organisations must transition from isolated AI governance to AI-enabled product governance by design.

Those who treat AI as merely a software feature will struggle

Those who integrate AI into their product compliance journey — from design to decommissioning — will define the next generation of trusted intelligent products.



# About the author

## Mónica Fernández Peñalver

Mónica leads Nemko Digital's work on governance, assurance, and standards implementation. Drawing on expertise in responsible technology, sustainability, and policy, she translates complex frameworks such as ISO 42001 into actionable strategies, enabling organizations to meet ethical, regulatory, and operational requirements.

Nemko Digital