Nemko Digital

CASE STUDY

From Regulatory Uncertainty to Strategic Clarity

Transforming 17+ frameworks into a focused, risk-based compliance roadmap

Executive summary

A global smart device manufacturer faced growing uncertainty around how 17+ EU regulations—including the Cyber Resilience Act, AI Act, and NIS2—applied to its connected product portfolio.

Within **6 weeks**, Nemko Digital delivered a **product-level regulatory applicability map, prioritized compliance scope, and actionable roadmap**, enabling the client to:

- **Reduce regulatory scope by ~30–50%** (by ruling out non-applicable frameworks such as NIS2)
- Avoid significant unnecessary compliance investments
- Accelerate compliance planning timelines by several months
- Translate legal requirements into concrete product and engineering actions

The client moved from fragmented uncertainty to a focused, risk-based compliance strategy—freeing up resources, reducing regulatory exposure, and enabling faster product innovation.

1. Situation

The client operates a global portfolio of smart, connected devices combining hardware and software. As EU regulation evolved—particularly with the introduction of the Cyber Resilience Act and the AI Act—the organization recognized that its products could fall under multiple overlapping frameworks.

Despite strong internal technical expertise, the organization lacked a unified view of how regulations applied across its new line of smart products. Different teams interpreted requirements independently, leading to inconsistent assumptions and growing uncertainty. Concerns were especially high around cybersecurity regulations such as NIS2, which were perceived as potentially imposing significant obligations.

At the same time, the company was preparing to introduce AI-enabled features, making it critical to understand not only current regulatory exposure but also future requirements.

The central question became clear: ***Which regulations actually apply, and what do we need to do to tackle those?***

2. Key Challenges

Regulatory applicability was unclear across more than a dozen frameworks, each with its own scope, terminology, and timelines. Overlaps between cybersecurity, AI, and data regulations made interpretation difficult, while legal requirements remained disconnected from product and engineering realities.

As a result, **the organization faced a dual risk**. On one hand, it risked **over-investing in compliance efforts** for regulations that might not apply. On the other, it risked **under-preparing for high-impact frameworks** that would require significant changes. Without a clear prioritization, compliance efforts were fragmented, inefficient, and difficult to align with product development cycles.

3. Approach

Nemko Digital structured the engagement as a focused two-step process, moving from regulatory clarity to execution readiness, in close collaboration with the client's innovation, legal, and engineering teams.

Step 1

Applicability and requirements

The engagement began with a **comprehensive review of relevant EU and national regulations**, including the AI Act, Data Act, GDPR, Cyber Resilience Act, and NIS2. Rather than assessing these in isolation, we anchored the analysis in the client's actual business context—mapping products, system architectures, and data flows to regulatory scope.

This was complemented by a series of stakeholder interviews across legal, technical, and operational teams to ensure that both formal structures and real-world practices were captured. Based on this, we documented clear applicability decisions for each regulation, including the rationale behind inclusion or exclusion.

The result was not just a theoretical interpretation, but a **practical applicability matrix** that showed exactly which regulations applied to which products and why. Alongside this, we developed a **plain-language requirements summary**, translating legal obligations into actionable insights for engineering and product teams, and identified a set of **open points** requiring further clarification or future monitoring.

Initial regulation longest

Artificial Intelligence	Data protection and governance	Cyber security and digital resilience	Product Safety and Conformity	Market and Critical Infrastructure
• AI Act	• General Data Protection Regulation (GDPR)	• Cyber Resilience Act (CRA)	• Product Liability Directive; revised	• Digital Services Act (DSA)
	• Data Act	• Network Information Security Directive (NIS2)	• Radio Equipment Directive (RED)	• Digital Market Act (DMA)
	• Data Governance Act	• Digital Operational Resilience Act (DORA)	• Machinery Regulation; revised	
	• ePrivacy regulation	• Cybersecurity Act	• General Product Safety Regulation (GPSR)	

EU Regulation focus

- **Data Act:** Second opinion and interpretation after earlier legal advice
- **GDPR:** Understand scope and nature of PII gathered
- **GPSR:** Review existing risk evaluations
- **PLD:** Understand added liability
- **AI Act:** Focus on planned product launches
- **CRA:** Understand high-level applicability
- **RED excluded:** *already addressed*
- **NIS2 reconsidered:** - *not applicable*

Applicability matrix - Summary

Data Protection and Governance

General Data Protection Regulation (GDPR)

Elements in scope	Grounds for applicability	Example controls
• Meta data • API • Analytics	• PII in all	• Internal policy adoption • Privacy notices • DPO appointment

Data Protection and Governance

Data Act

Elements in scope	Grounds for applicability	Example controls
• Telemetry from device	• Raw data generated from device	• Contract terms • User access • Governance

Artificial Intelligence

AI Act

Elements in scope	Grounds for applicability	Example controls
• Computer vision system • Chat bots • Future AI	• All classify as AI systems	• AI risk categorization • AI literacy • Transparency measures

Product Safety

General Product Safety Regulation (GPSR)

Elements in scope	Grounds for applicability	Example controls
• All devices	• Products with digital component	• Risk analysis • Record-keeping procedures • Communication channels and complaint registry • Policy for corrective actions

Cyber Security and Digital Resilience

Cyber Resilience Act (CRA)

Elements in scope	Grounds for applicability	Example controls
• All devices • API	• Hardware products linked to remote data processing solutions	• Security by design • Risk assessment • Vulnerability handling • Technical documentation

Cyber Security and Digital Resilience

NIS2

Elements in scope	Grounds for applicability	Example controls
• None	• Not defined as high criticality sector	• N/A

Step 2

Gap analysis and remediation roadmap

With applicability established, the focus shifted to understanding what compliance would require in practice.

We systematically compared the client's existing policies, processes, and technical controls against the identified regulatory requirements. This allowed us to identify concrete gaps, assess associated risks, and determine clear compliance priorities across the organization.

Rather than stopping at diagnosis, we translated these insights into action. For each gap, we defined targeted remediation measures, including indicative effort and cost considerations, and clarified ownership across internal teams and, where relevant, external support functions.

This work culminated in a **high-level gap analysis report**, and an **initial remediation roadmap** outlining timelines, milestones, and responsible stakeholders. Lastly, we defined **resourcing requirements**, providing clarity on how compliance efforts should be distributed across the organization.

In parallel, a global monitoring capability was established to track regulatory developments beyond the EU, ensuring that the client's strategy remains future-proof and aligned with international market requirements.

Parallel Regulatory Radar – Compliance regulatory monitoring

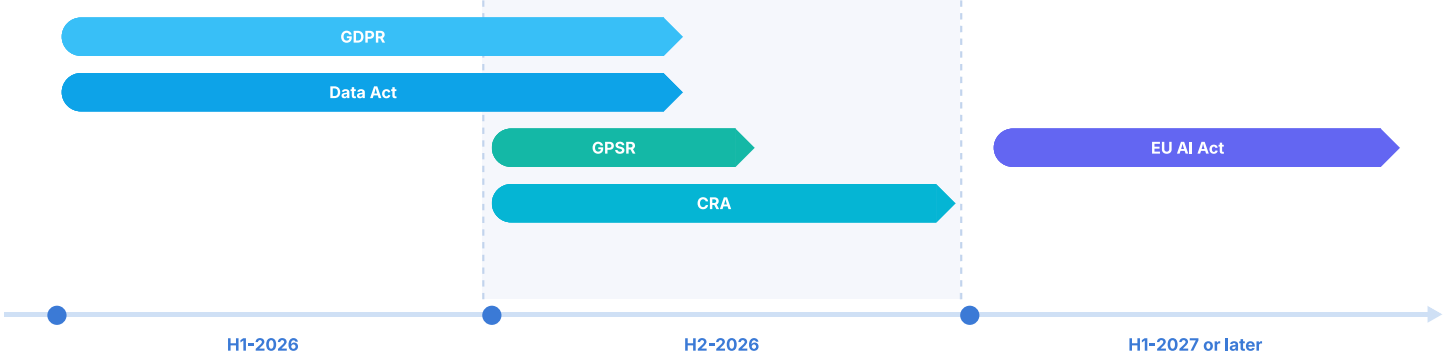
Elements of the remediation - Summary

GDPR	Data Act	CRA	GPSR	AI Act
• Enhance current compliance model	• Formalize roles and responsibilities	• Formalize roles and responsibilities	• Extend existing risk assessment	• Formalize risk categorization and document in an AI register
• Implement GDPR controls	• Adapt contract clauses	• Review risk assessments	• Define guidelines on communication channels with customer	• Train employees working with chatbots
• Integrate in the redesign of cloud architecture	• Implement interim data request and sharing processes	• Review vulnerability handling	• Extend corrective actions policy	• Ensure transparency
	• Investigate technology options compliance 'by design'	• Information provided with the product		• For procured AI solutions, add AI compliance check as part of standard procurement process
		• Declaration of Conformity		

Embedding ownership across departments and teams

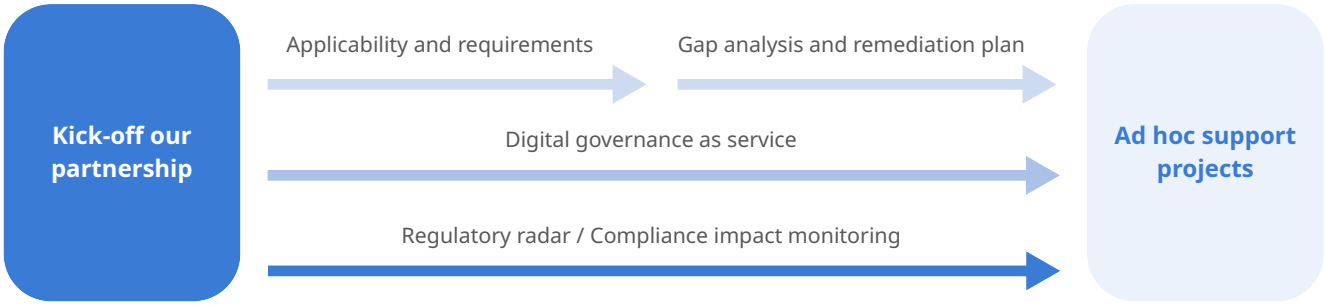
GDPR	R Department B	R Department C	I Department E	I Department F	A Department G	
	C Department H	C Department I				
Data Act	A Department A	R Department B	R Department C	R Department D	A Department E	
	C Department F	R Department H				
CRA/GPSR	A Department A	R Department B	R Department C	C Department D	C Department E	
	I Department F	C Department I				
AI Act	A Department A	R Department B	A Department E	C Department H	R Department I	

Recommended prioritization



The integrated outcome

By structuring the work in these two steps, the client gained both **clarity and direction**: first, a defensible understanding of what applies, and second, a concrete and prioritized plan for what to do next.



Value Delivered

The engagement fundamentally changed how the organization approached regulation. Where previously there had been fragmented interpretations and broad uncertainty, the client now has a clear and defensible understanding of which regulations apply and how they impact specific products. This clarity enabled a significant reduction in perceived regulatory scope, particularly by ruling out non-applicable frameworks such as NIS2.

Equally important, the client can now direct its resources toward the regulations that matter most. Legal requirements have been translated into concrete technical and organizational actions, allowing engineering, product, and compliance teams to work from a shared understanding.

The roadmap provides a practical path forward, enabling the organization to align compliance efforts with product releases and avoid last-minute disruptions. At the same time, early identification of gaps has reduced regulatory risk and created opportunities for quick wins.

Overall, the engagement delivered both efficiency and risk reduction: avoiding unnecessary compliance investments while accelerating readiness for high-impact regulations and future AI-enabled capabilities.

Next Steps

With a clear applicability baseline in place, the organization is now positioned to move into implementation.

The next phase focuses on closing identified gaps, embedding compliance into the product development lifecycle, and establishing a scalable governance model. This includes strengthening technical controls, formalizing processes, and preparing for future audits.

Rather than treating compliance as a one-off exercise, the objective is to build a system that is integrated, repeatable, and aligned with the organization's long-term product strategy.

Final Takeaway

This case demonstrates that regulatory complexity becomes manageable—and strategically valuable—once applicability is clearly defined.

By first answering *what applies*, the client avoided unnecessary work, reduced uncertainty, and created a focused, execution-ready compliance strategy that supports both innovation and market access.


Nemko
Digital