Nemko Digital

Nemko Digital Webinar Report - The EU Data Act: Learn What It Means for Connected Products & IoT Across All Industries

---

Executive Summary

This report provides a comprehensive analysis of the Nemko Digital webinar on the European Union's Data Act, a regulation poised to fundamentally reshape the digital economy. The webinar, held on September 30, 2025, offered critical insights for manufacturers and providers of connected products and services operating within the EU.

The key finding is that the Data Act represents a paradigm shift, transferring data rights from manufacturers to users and mandating a new era of data accessibility and interoperability. This has profound implications for product design, data governance, and contractual agreements. Analysis of audience engagement revealed a significant gap in industry preparedness, with a majority of companies only just beginning their compliance journey. Non-compliance presents substantial financial and reputational risks.

Expert presentations detailed the Act's core obligations, including providing users with free and easy access to the data their products generate and sharing this data with third parties upon the user's request under fair, reasonable, and non-discriminatory (FRAND) terms. The timeline for compliance is aggressive, with initial obligations taking effect on September 12, 2025.

Strategic recommendations for leadership include the immediate formation of a cross-functional task force to oversee compliance, the initiation of comprehensive legal and technical audits to identify gaps, and the allocation of resources to embed a "Data Act by Design" philosophy into product development. While presenting a

compliance challenge, the Data Act also offers a strategic opportunity for businesses to build customer trust, foster innovation, and achieve a significant competitive advantage in the evolving data economy.

Overview and Objectives of the Webinar

The webinar, hosted by Nemko Digital, was designed as a strategic briefing for business leaders, product managers, legal teams, and engineers within companies that manufacture, sell, or service connected products in the European Union. The primary objective was to provide a clear and actionable understanding of the EU Data Act, moving beyond theoretical legal analysis to focus on its practical and commercial implications.

The session aimed to:

- Demystify the Data Act: Translate the complex legal text into understandable business concepts and obligations.
- Situate the Act within the Broader EU Digital Strategy: Explain how the Data Act interacts with other key regulations such as the AI Act, the Cyber Resilience Act, and GDPR.
- Define the Scope and Key Concepts: Clearly articulate what constitutes a "connected product" and "related service," and define the roles of "user," "data holder," and "data recipient."
- Outline Core Obligations and Timelines: Detail the specific requirements for data access, sharing, and contractual fairness, along with the critical deadlines for compliance.
- Provide a Strategic Roadmap: Equip attendees with a structured approach to assess their current standing, identify gaps, and plan for successful implementation.

By achieving these objectives, the webinar sought to empower organizations to not only mitigate compliance risks but also to identify and leverage the strategic opportunities presented by the new data-sharing economy.

Nemko Digital

2. In-Depth Analysis of Expert Presentations

The webinar was led by two of Nemko Digital's senior experts, who provided a multi-faceted analysis of the Data Act, covering its legal context, technical requirements, and strategic business implications.

2.1. The EU's Integrated Digital Regulatory Framework (Presented by Monica Fernandez)

Monica Fernandez, Digital and AI Trust Expert, began by contextualizing the Data Act within the EU's broader ambition to create a single market for data. She emphasized that the Act is not a standalone piece of legislation but a critical component of a cohesive regulatory ecosystem. This framework is designed to ensure that the digital transition is human-centric, fair, and secure.

Key Interconnected Regulations:

Regulation	Strategic Purpose & Interaction with the Data Act
General Data Protection Regulation (GDPR)	The GDPR remains the bedrock of personal data protection. The Data Act is built upon it, clarifying that in cases involving mixed data (personal and non-personal), GDPR's protections for personal data are paramount and must not be undermined. The Data Act extends similar principles of access and portability to non-personal data.
AI Act	This act governs the use of artificial intelligence, particularly high-risk systems. The Data Act is a key enabler for the AI Act, as it facilitates access to the vast datasets generated by IoT devices, which are essential for training and validating AI models. This promotes competition and reduces the data-monopoly power of large tech firms.
Cyber Resilience Act (CRA)	The CRA mandates baseline cybersecurity requirements for products with digital elements. This is a crucial prerequisite for the Data Act's data-sharing provisions. Secure products are essential to ensure that data shared with third parties is protected from unauthorized access or breaches.

General Product Safety Regulation (GPSR)	The GPSR extends product safety rules to the digital realm. The Data Act complements this by focusing on the data generated by these products, ensuring that users have rights and control over this data, which can itself have safety and security implications.

This integrated approach demonstrates a sophisticated and holistic strategy by the EU to govern the digital economy, balancing innovation with fundamental rights and safety.

2.2. Core Principles and Obligations of the Data Act (Presented by Pepijn van der Laan)

Pepijn van der Laan, Global Technical Director, provided a deep dive into the core mechanics of the Data Act. He used practical examples, such as a smart elevator and a connected vehicle, to illustrate the Act's real-world applications.

Fundamental Concepts Defined:

- Connected Product: Any item that generates or collects data about its use or environment and can communicate this data. This is a very broad definition covering consumer, commercial, and industrial IoT devices.
- Data Holder: The entity (usually the manufacturer) with the legal and technical ability to make the data available. This role carries the primary compliance burden.
- User: The owner, renter, or lessee of the product. The Act empowers this entity with significant new rights.

The Three Thematic Pillars of the Act:

1. Data Access and Sharing: This is the central pillar. It establishes the user's right to access all data generated by their use of a product. This data must be provided easily, securely, and free of charge. Critically, it also mandates that the data holder must share this data with a third-party data recipient upon the user's request. This is intended to open up markets for aftermarket services, such as predictive maintenance or insurance.
2. Fair Contracts and Prevention of Abuse: The Act introduces measures to prevent the abuse of contractual imbalances. Article 13 specifically targets unfair terms in

data-sharing agreements that are unilaterally imposed on small or medium-sized enterprises (SMEs), making such terms non-binding.
3. Interoperability and Standardization: The Act empowers the European Commission to develop interoperability standards for data and data-sharing mechanisms. This is crucial for preventing the emergence of new data silos and ensuring a fluid, competitive data market.

Mr. van der Laan stressed that these obligations require a "Data Act by Design" approach, meaning compliance must be considered from the earliest stages of product development, not as a later add-on.

---

3. Audience Engagement and Q&A Analysis

A key segment of the webinar was dedicated to audience interaction, including a live poll and a Q&A session. This provided valuable insights into the current state of industry preparedness and key areas of concern.

3.1. Industry Preparedness: Live Poll Results

The poll results painted a stark picture of the industry's readiness for the Data Act:

- Over 50% of participants are at the very beginning of their compliance journey, with only a general awareness of the Act.
- Approximately 33% are actively working on implementation but are not yet compliant.
- Around 10% have a plan in place but have not yet started execution.
- A striking 0% of attendees reported being fully prepared for the Data Act.

Analysis: This data reveals a significant preparedness gap across the industry. The majority of companies are at high risk of being non-compliant by the September 2025 deadline. This lack of readiness suggests a potential underestimation of the Act's complexity and the resources required for implementation.

3.2. Key Concerns from the Q&A Session

The Q&A session highlighted several practical challenges and areas of uncertainty for businesses:

Nemko Digital

Question Topic	Summary of Concern & Expert Response
User Authentication & Product Ownership	Concern: How can a data holder reliably verify that a person requesting data is the legitimate user, especially in second-hand or rental markets? Expert Response: The contract is the primary source of truth. Data holders must implement robust authentication mechanisms tied to user accounts and proof of ownership/lease. This will require updates to terms of service and user registration processes.
Standardized Data Provisioning	Concern: What exactly does "provision of data in a standardized manner" mean? Are there specific formats required? Expert Response: While the EU will release more specific guidelines, the principle is interoperability. Data should be provided in a common, machine-readable format (e.g., JSON, CSV) and accessible via well-documented APIs. The goal is to make the data not just available, but practically usable by third parties.
Interface for Data Access	Concern: Does the Act require a separate, dedicated interface for data access, or can it be integrated into existing apps? Expert Response: The Act is not prescriptive on the implementation. Companies can use existing customer portals or apps. The critical requirement is that the process must be simple, secure, and transparent for the user. It should not create an undue burden.
Scope of Application	Concern: Does the Act apply to non-connected products? Expert Response: No. The Act's scope is explicitly limited to "connected products" that can generate and transmit data.

Analysis: The questions indicate that companies are moving from high-level awareness to grappling with the detailed operational and technical challenges of implementation. The key themes are security, interoperability, and user experience.

4. In-depth Outcomes and Strategic Implications

The insights from the webinar point to several profound outcomes and strategic implications that will redefine the competitive landscape for companies dealing with connected products.

1. The End of Data Silos and the Rise of a Data-Sharing Economy: The most significant outcome of the Data Act is the mandated dismantling of proprietary data silos. Historically, manufacturers have held exclusive control over the data generated by their products, creating a significant competitive moat. The Act transforms this dynamic by establishing data access and portability as a user right. This will force a shift from closed ecosystems to more open, interconnected platforms, fostering a new economy based on data sharing and collaboration.

2. Disruption of Aftermarket and Value-Added Services: The requirement to share data with third parties at the user's request will fundamentally disrupt traditional aftermarket and service models. Independent repair shops, competing service providers, and innovative startups will now be able to access the data needed to offer competitive services, from predictive maintenance to personalized insurance. Incumbent manufacturers must now compete on the quality of their services rather than relying on a data monopoly. This necessitates a strategic pivot towards creating superior customer value to retain service revenue.

3. Elevation of Data Governance to a Core Strategic Function: The Act elevates data governance from a back-office IT or legal function to a C-suite-level strategic concern. The ability to manage, secure, and share data in a compliant manner is now a prerequisite for market access in the EU. This requires a holistic approach that integrates legal compliance, cybersecurity, product design, and business strategy. Companies that excel at data governance will build trust and be better positioned to leverage data for innovation.

4. A Catalyst for Innovation and New Business Models: While the compliance requirements are significant, the Data Act is also a powerful catalyst for innovation. The increased availability of data will fuel the development of new applications and services across industries. For manufacturers, this presents an opportunity to move beyond selling physical products to offering data-driven services and creating new

revenue streams. Companies can partner with data recipients to co-create value, enriching the customer experience and building deeper brand loyalty.

5. Redefinition of Customer Relationships around Trust and Transparency: By placing data control in the hands of the user, the Act redefines the relationship between a company and its customers. Trust and transparency become paramount. Companies that embrace this shift by making data access simple, providing clear information about data usage, and empowering their customers will build significant brand equity. Conversely, those that create barriers or are opaque in their data practices will face both legal repercussions and customer backlash.

---

5. Strategic Recommendations for Leadership

Based on the analysis of the webinar and the requirements of the Data Act, the following strategic recommendations are proposed for executive leadership:

1. Immediately Establish a Cross-Functional Data Act Task Force:

- Action: Form a dedicated task force with representation from Legal, Engineering/Product Development, IT/Data Governance, Marketing, and Sales. This is not just a legal or IT issue; it requires a unified business response.
- Objective: To centralize ownership of the compliance project, conduct a comprehensive business impact analysis, and develop a detailed implementation roadmap. This task force should report directly to the C-suite.

2. Commission a Comprehensive Legal and Technical Audit:

- Action: Initiate a two-pronged audit. The legal audit should review all existing contracts, terms of service, and privacy policies. The technical audit should map all data flows for in-scope products and assess the feasibility of implementing secure data access and sharing mechanisms.
- Objective: To create a detailed "Gap Analysis" that identifies all areas of non-compliance and quantifies the effort required to remediate them. This will form the basis of the project plan.

3. Allocate Budget and Resources for "Data Act by Design" Implementation:

- Action: Earmark dedicated funding and engineering resources to re-architect products and data platforms where necessary. This includes developing user-facing dashboards for data access and robust, secure APIs for third-party data sharing.
- Objective: To embed compliance into the product development lifecycle. This proactive approach is more cost-effective than retrofitting solutions and reduces long-term risk.

4. Rethink and Innovate the Service and Aftermarket Strategy:

- Action: Proactively develop a strategy to compete in an open data ecosystem. Instead of fighting data sharing, focus on providing superior, data-driven value-added services that customers will choose over third-party alternatives.
- Objective: To turn the threat of disruption into a competitive advantage. This may involve developing new service offerings, partnering with data recipients, or creating a developer ecosystem around your product data.

5. Launch a Proactive Communication and Training Initiative:

- Action: Develop internal training programs to educate relevant employees on the Data Act's requirements. Create external communication materials that transparently explain to customers their new data rights and how to exercise them.
- Objective: To ensure organizational readiness and to build customer trust through transparency. A well-informed customer base is more likely to engage positively with the brand.

Nemko Digital

Conclusion

The Nemko Digital webinar provided an unequivocal message: the EU Data Act is a transformative piece of legislation that requires immediate and strategic attention. The era of proprietary control over IoT data is over, replaced by a new paradigm centered on user empowerment, data fluidity, and open competition. The significant gap in industry preparedness highlights a collective vulnerability that can only be addressed through decisive leadership and proactive investment.

While the compliance journey is complex and resource-intensive, the strategic opportunities are equally significant. By embracing the principles of the Data Act, companies can move beyond a defensive, compliance-oriented mindset. They have the opportunity to redefine their customer relationships based on trust, to innovate their service offerings, and to build a sustainable competitive advantage in the data-driven economy of the future. The time for executive action is now.