Nemko Digital

How the EU Data Act Reshapes Value Creation in the IoT Economy

The EU Data Act (2023/2854) is often treated as a regional regulatory update, relevant mainly for legal and compliance teams operating within Europe. However, that interpretation misses its broader impact: the structural shift in how value is created and distributed in the Internet of Things (IoT) economy.

For business leaders, the implication is not simply that "data access rules are changing." It is that the underlying economics of connected products are being rewritten from systems where manufacturers control and monetize data end-to-end, to ecosystems where access is shared, and value must be actively created across multiple actors.

As companies adapt their data flows ahead of the September 2026 compliance deadlines, business leaders must look beyond compliance and consider the strategic implications of the Data Act.

A shift in control, not just compliance

For the past decade, IoT business models have been built on a simple logic: companies that design and sell connected products also control the data those products generate. That control has underpinned product improvement, after-sales services, and integrated digital ecosystems.

The EU Data Act challenges this foundation. It grants users the right to access data generated by connected devices and requires data holders to make that information available under fair conditions, including sharing with third parties.

The strategic implication is straightforward: exclusive control over machine-generated data can no longer be assumed.

Why this matters beyond Europe

Although the regulation originates in the EU, its impact is global in practice. Any company selling connected devices into the EU must comply, regardless of headquarters location.

More importantly, EU digital regulation has repeatedly shaped global standards. GDPR is the clearest precedent: regional rules often become de facto global design baselines.

The Data Act is likely to follow a similar trajectory in industrial and IoT systems, meaning firms will increasingly design products and data architectures around portability and shared access as default conditions rather than exceptions.

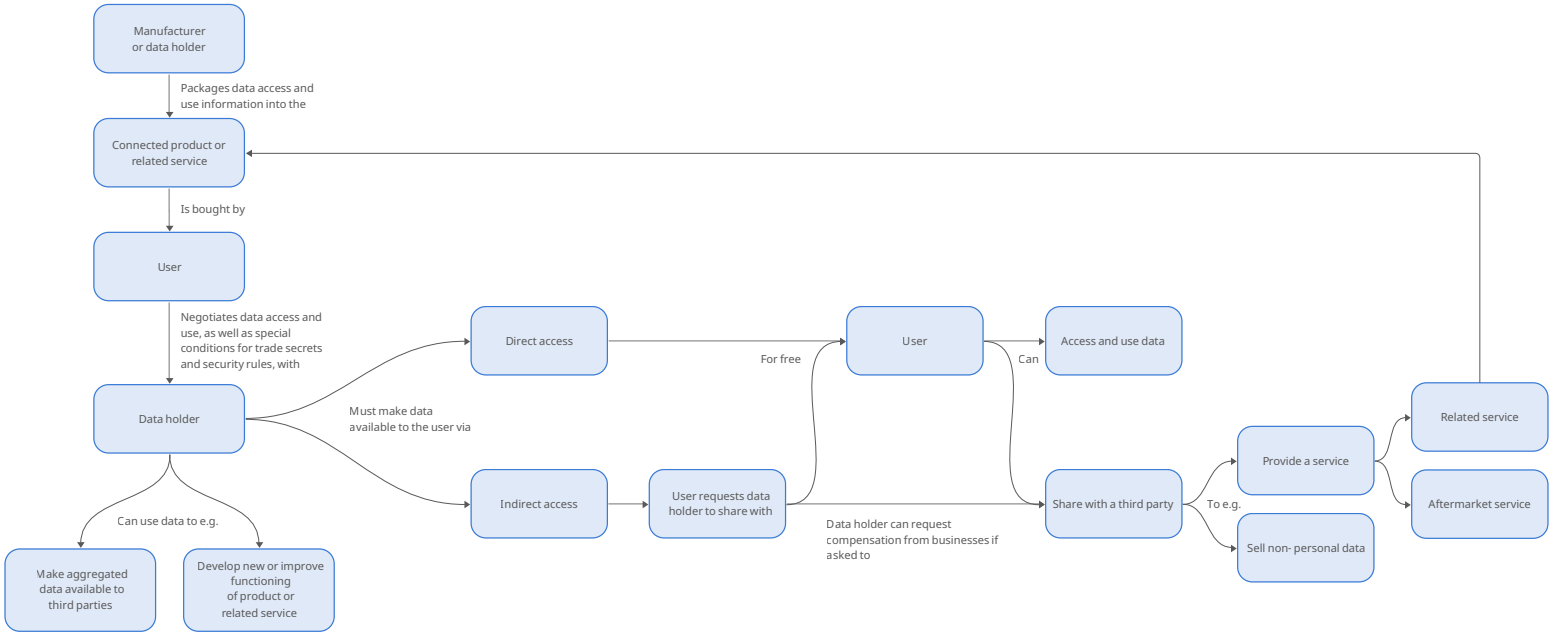
From proprietary data to shared ecosystems

In traditional IoT models, value creation was structured as a closed loop. Manufacturers collected and analyzed data internally, using it to improve products and deliver after-sales services. The value chain was largely contained within a single organization.

The Data Act changes this structure by enabling broader access to device-generated data. Once multiple actors can work with the same underlying information, the ecosystem becomes more distributed.

This does not reduce value creation. It redistributes it. Competitive advantage shifts from exclusive data possession toward the ability to integrate and apply data across ecosystem boundaries.

This shift is reflected in the European Commission's Data Act guidance and implementation examples.



EU Commission guidance on Data Act implementation: Access to and use of data in the Internet-of-Things context (An example of Chapter II in practice)Industry implications: where the shift becomes visible first

Industry implications: where the shift becomes visible first

The effects of this transition will be most visible in sectors where companies currently rely heavily on exclusive access to machine-generated data.

In industrial manufacturing, equipment providers have traditionally maintained strong post-sale positions through control of machine data. This supports services such as predictive maintenance, diagnostics, and performance optimization. With broader access, customers can increasingly work with alternative providers or develop internal capabilities.

In automotive, vehicle data underpins services ranging from maintenance to insurance pricing and mobility platforms. Opening access introduces new participants into ecosystems that have historically been tightly controlled by OEMs.

In energy and infrastructure, operational data from connected assets is increasingly used by multiple stakeholders to optimize efficiency and forecasting, creating more open service environments.

Across these sectors, the key shift is consistent: control over data is becoming less decisive than the ability to create value using shared data.

The strategic challenge for established companies

For established players, this shift introduces several structural tensions. Data exclusivity becomes a weaker source of differentiation. Advantage must increasingly come from analytics capability, service design, and ecosystem positioning rather than control over data itself.

At the same time, companies must move from product-centric models toward ecosystem participation. Influence is no longer exercised primarily through ownership, but through platforms, interfaces, and partnerships.

Finally, enabling regulated data access is not a marginal compliance requirement. It requires substantial redesign of data infrastructure to ensure secure, scalable, and standardized sharing across stakeholders.

Opportunity: from control to orchestration

While much of the discussion focuses on loss of control, the same shift creates meaningful opportunities for firms that adapt early.

As data becomes more widely accessible, value moves toward services built on shared infrastructure. This includes advanced analytics, optimization tools, and applications that combine multiple data sources across ecosystems.

In this environment, competitive advantage shifts toward orchestration—coordinating data flows, enabling interoperability, and building services across ecosystems rather than within closed systems.

Data governance capabilities become central differentiators. Firms that can reliably manage security, compliance, and data sharing will be better positioned to operate as infrastructure providers in emerging IoT ecosystems.

Implications for companies outside the EU

For global firms, the relevance of the Data Act extends well beyond European operations.

EU requirements will influence global product design, particularly in complex IoT systems where maintaining separate architectures for different regions is inefficient. Over time, EU standards are likely to become global defaults.

At the same time, fragmentation of data governance across regions increases operational complexity. Companies that adopt interoperable and scalable approaches are more likely to remain competitive than those relying on localized systems.

More broadly, regulatory convergence is already underway. As additional jurisdictions introduce data access and portability rules, the principles embedded in the EU model are increasingly shaping global expectations.

A structural shift in the IoT economy

The EU Data Act is not simply a regulatory update in how data is shared. It reflects a deeper transformation in the architecture of the IoT economy.

The system is moving toward regulated data access, distributed participation across ecosystems, and competition based less on data control and more on value creation within shared environments. For business leaders, this marks a clear shift in the source of competitive advantage.

What business leaders should do next

To move from awareness to execution, organizations should focus on a small number of strategic priorities:

- Map IoT data flows across products and services to understand where value is currently created and controlled
- Assess dependency on exclusive data access and where it underpins existing revenue streams
- Redesign data architectures for shared access and interoperability, rather than closed system control
- Reevaluate service and monetization models in a context where third-party access to data is structurally enabled
- Align compliance planning with ecosystem strategy, ensuring regulatory requirements are integrated into broader business design rather than treated separately

Nemko Digital supports organizations in translating these priorities into data strategies and compliant ecosystem architectures, through regulatory compliance and digital governance services.

Contact us to receive a brief assessment of your use case.

About the author

Mónica Fernández Peñalver

Mónica Fernández Peñalver is Digital and AI Governance Lead at Nemko Digital. Drawing on expertise in digital governance and policy, she supports organizations and technical teams in applying regulations such as the EU AI Act, Data Act, GDPR, and the Cyber Resilience Act, as well as international standards like ISO/IEC 42001, to navigate regulatory requirements and implement them effectively.

Nemko Digital