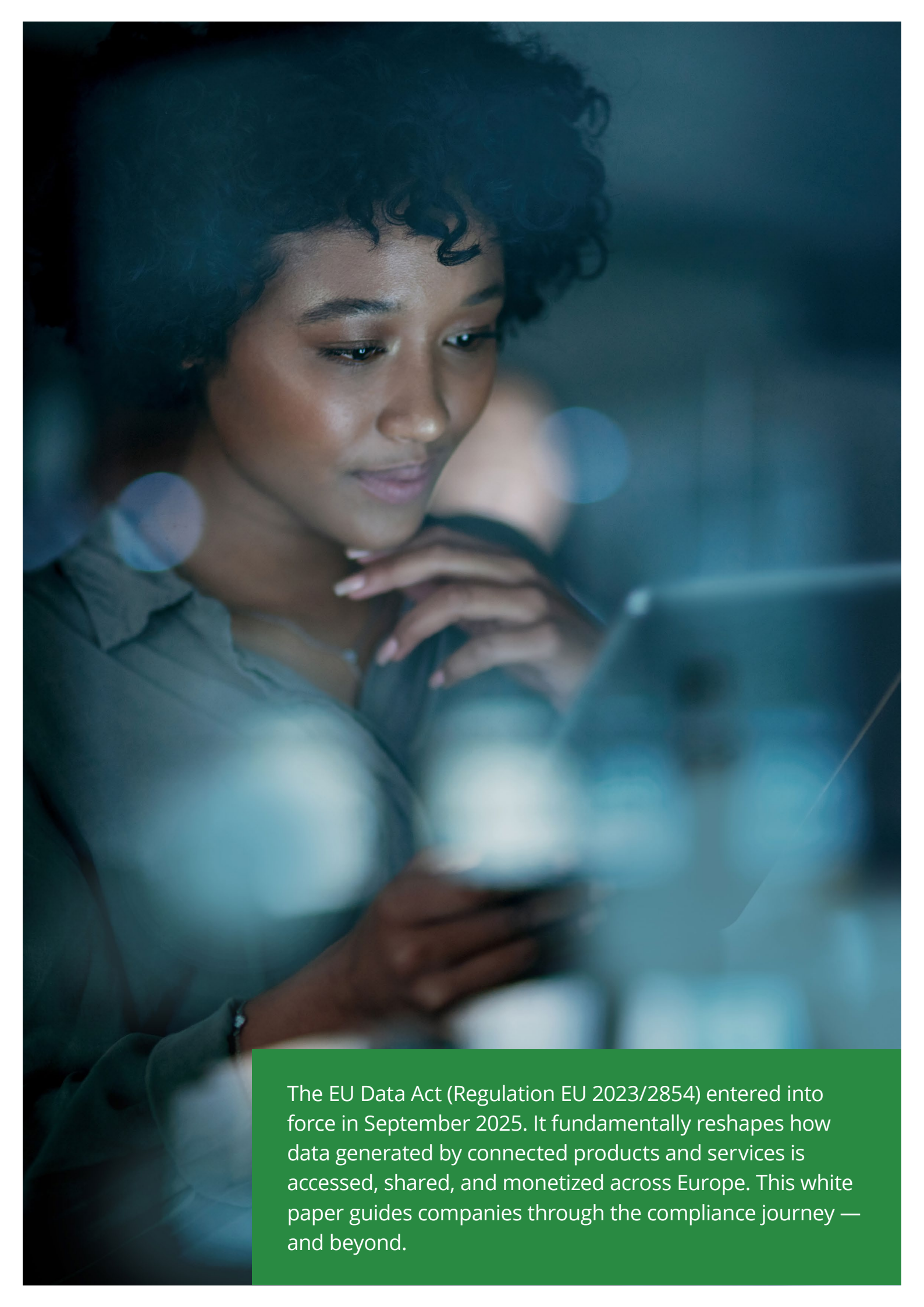


Navigating the EU Data Act
Turning compliant data
access into business value

The EU Data Act — A Brief Overview	05
Market Overview — How Does the EU Data Act Affect Different Industries?	06
From Compliance to Monetization — The “Five-Phases” Model	08
Industry Scenarios — The EU Data Act in Practice	10
The Steelbridge Data Act Platform (DAP)	12
Outlook — What Comes Next	16
Frequently Asked Questions — Addressing Common Concerns	18
Contacts	22

A woman with dark, curly hair is looking down at a tablet computer. She is wearing a light-colored, button-down shirt. The background is dark and out of focus, with several bright, circular bokeh lights. The overall mood is professional and focused.

The EU Data Act (Regulation EU 2023/2854) entered into force in September 2025. It fundamentally reshapes how data generated by connected products and services is accessed, shared, and monetized across Europe. This white paper guides companies through the compliance journey — and beyond.

The EU Data Act — A Brief Overview

The EU Data Act creates a fair and competitive data economy by establishing clear rules for the access, use, and sharing of data generated by connected products and related digital services. It defines who can access data, under what conditions, and how data must be made available — applying to any company that manufactures connected devices, provides related digital services, or processes data from such devices.

Tab. 1 – Key Regulatory Impacts

Regulatory Requirement	What it means for Data Holders
Data Access Rights	End users gain the legal right to access and share data generated by the products or services they use.
Data Holder Obligations	Companies must provide access to users and authorized third parties through secure, interoperable, and non-discriminatory interfaces.
Contractual & Pricing Rules	Data access terms must be transparent and fair, with specific pricing conditions for SMEs.
Public Sector Requests	In exceptional circumstances (e.g., public emergencies), authorities may request access to private sector data under defined safeguards.
Cloud Portability	Providers must enable customers to switch cloud or edge services freely, preventing vendor lock-in.

Tab. 2 – Two Paths to Compliance: Access by Design and Access by Request

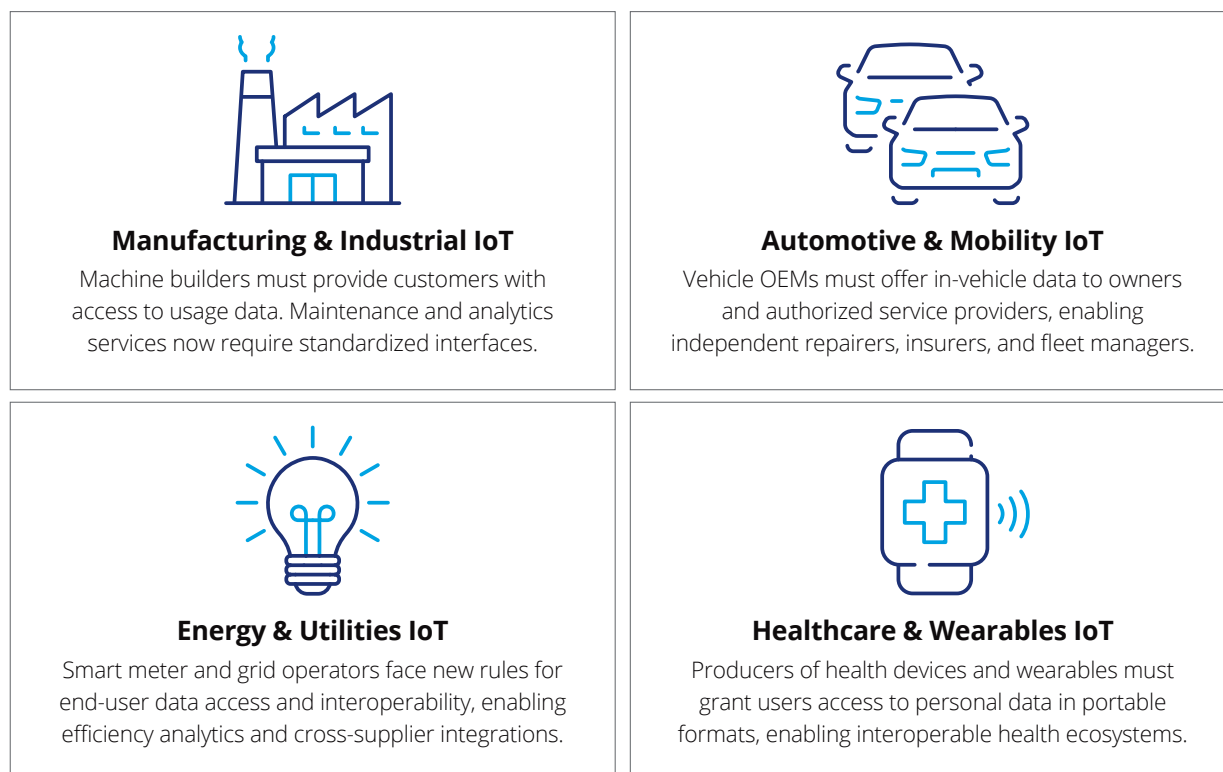
The regulation distinguishes between two primary compliance mechanisms under Article 3 and Article 4:

Access by Design (Art. 3)	Access by Request (Art. 4)
Systems built with embedded, automatic access pathways for users. • Embedded Mechanisms: Systems designed with built-in access pathways • Predefined Conditions: Rules governing automatic access under specific circumstances • Security Measures: Governance & safeguards to prevent unauthorized access • Interoperability: Standards ensuring seamless integration with other systems Example: An API provides near real-time access to equipment performance data without any additional request required.	Clear, verified processes for submitting and handling user data access requests. • Request Mechanism: Clear and secure processes for submitting and managing access requests • Authorization Protocols: Verified identities and roles for granting access • Compliance Checks: Processes to ensure requests align with legal and organizational policies • Auditability: Logging and tracking of access requests and decisions. Example: Fleet operators request machine location, operating hours, and service intervals for maintenance planning.

Market Overview — How Does the EU Data Act Affect Different Industries?

The EU Data Act cuts across every sector where IoT (Internet of Things) is either part of the value adding chain or smart/connected products generate data. Below table gives an overview of selected sectors affected, incl. market figures.

Fig. 1 – Overview on IoT Market in key sectors



Tab. 3 – IoT Market Size in Key Sectors (EU & Global)

 Manufacturing & Industrial IoT	 Automotive & Mobility IoT	 Energy & Utilities IoT	 Healthcare & Wearables IoT
Europe	Europe	Europe	Europe
2025: USD 67.2B CAGR 23.2% (2025–2033) ¹	2025: USD 14.8B CAGR 17.1% (2025–2031) ²	2024: USD 13.5B CAGR 8.7% (2025–2030) ³	2025: USD 11.86B CAGR 15.32% (2025–2030) ⁴
Global	Global	Global	Global
2025: USD 556.6B CAGR 12.1% (2025–2035) ⁵	2025: USD 189.87B CAGR 18.39% (2025–2030) ⁶	2025: USD 43.5B CAGR 13.3% (2025–2035) ⁷	2024: USD 18.80B CAGR 9.8% (2025–2030) ⁸



¹ <https://www.marketdataforecast.com/market-reports/europe-industrial-internet-of-things-market>

² <https://mobilityforesights.com/product/europe-automobile-iot-market>

³ <https://www.grandviewresearch.com/horizon/outlook/iot-in-utilities-market/europe>

⁴ <https://www.mordorintelligence.com/industry-reports/europe-wearable-market>

⁵ <https://www.futuremarketinsights.com/reports/industrial-iot-market>

⁶ <https://www.mordorintelligence.com/industry-reports/automotive-iot-market>

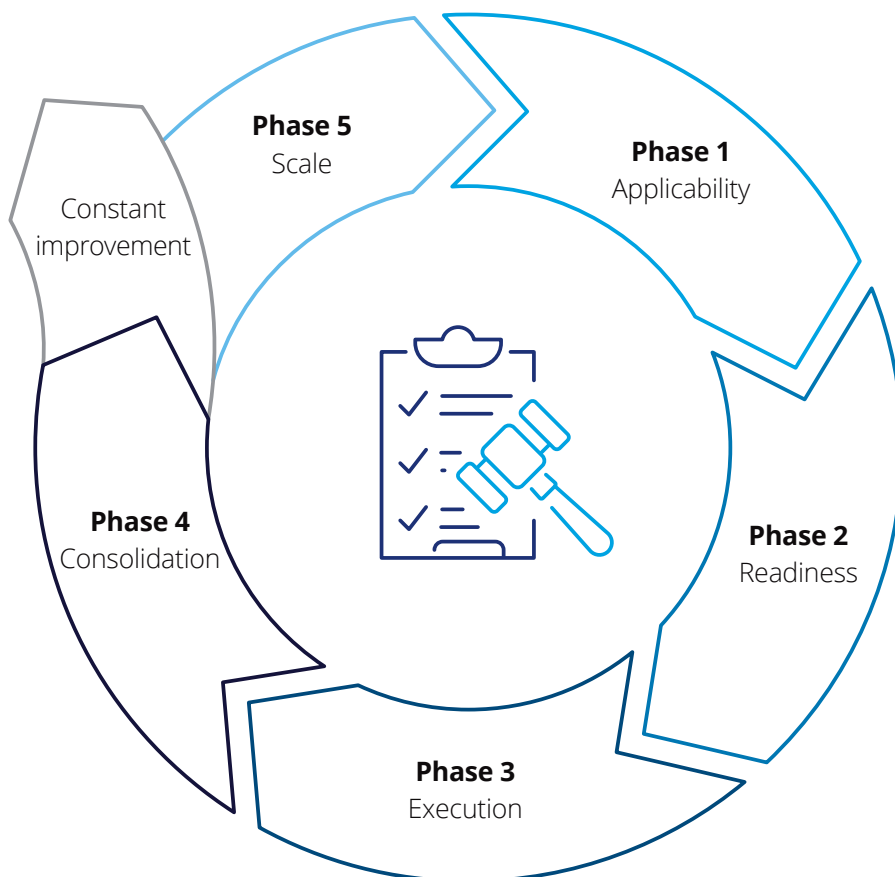
⁷ <https://www.futuremarketinsights.com/reports/iot-in-utilities-market>

⁸ <https://www.grandviewresearch.com/industry-analysis/iot-wearable-device-market-report>

From Compliance to Monetization — The “Five-Phases” Model

Achieving EU Data Act compliance is not a one-time project — it is a strategic journey. Our proven maturity model takes companies from initial readiness assessment through to scalable data usage and monetization.

Fig. 2 – The EU Data Act “Five-Phases” Compliance and Monetization Model



Operational activities within the five phases

1 Applicability

Conduct an upfront applicability analysis for connected (IoT) products and related services. Identify which products fall under the regulation, assess strategic exposure through a SWOT or impact analysis, and define key action fields, risks, and opportunities. This phase establishes the organizational baseline and strategic framing for the compliance journey.

2 Readiness

Situational Analysis – Tech Gap Assessment – Risk Evaluation

Identify your current compliance posture and map regulatory obligations against existing business processes. Key actions include defining covered products and datasets, conducting data inventories, reviewing contracts, evaluating technical architectures, and assessing organizational risks. Outcome: a detailed roadmap covering all required legal, technical, and organizational measures.

3 Execution

Planning and Implementation of Technical Solutions

Implement the measures identified in Phase 1: update internal policies, deploy secure data access interfaces, build consent mechanisms, prepare compliance documentation, and train relevant teams. Outcome: operational readiness for data access obligations and a standardized framework for controlled, auditable data sharing.

4 Consolidation

Building Scalable Compliance Infrastructure

Shift from fragmented project delivery to a production-grade compliance platform. Companies consolidate their technical and operational solutions into a unified, auditable infrastructure purpose-built for EU Data Act obligations. Steelbridge's Data Act Platform (DAP) is directly ready to deliver full compliance if the data holder's data endpoints are technically available. The platform connects data holders, end users, and third parties through standardized interfaces, consent management workflows, authorization controls, and immutable audit trails.

Where brand alignment is required, Steelbridge can deploy a fully white-labeled version of the platform using the data holder's own visual identity and assets. A white-label implementation can be completed in approximately four weeks, provided the underlying data infrastructure is in place.

5 Scale

Monetization of Data Assets

Once compliant infrastructure is established, companies can move beyond regulatory obligation and activate structured data monetization through the Steelbridge financial layer. The Steelbridge platform includes a built-in billing and licensing engine that allows data holders to define pricing models for consented user data feeds. Pricing can be configured per transaction, per API call, per dataset, or through recurring monthly invoicing.

Data holders can also apply differentiated margin logic depending on the profile of the requesting third party. For example, base feed pricing can be set as a standard rate, while larger enterprise requesters can be subject to additional margin layers reflecting commercial value, volume, or strategic positioning. This enables controlled, tiered monetization without requiring separate bilateral technical implementations for each partner.

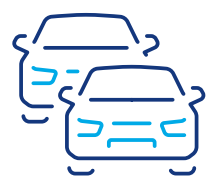
All transactions are logged, contract-bound, and traceable through Steelbridge's authorization and audit modules, ensuring that monetization remains compliant with Articles 4–6 of the EU Data Act while preserving full control over scope and access rights.

In addition, when user-specific identifiers are removed and data is properly anonymized or aggregated, data holders can publish selected feeds to the Steelbridge marketplace in an open-access format. In this model, monetization can continue independently of individual user consent flows, as the data no longer constitutes personal or user-linked information.

Through this structure, compliance becomes a scalable commercial capability. Data holders can launch controlled data products, enable third-party analytics ecosystems, participate in EU data spaces, and generate sustainable revenue streams — all within a governed, production-grade infrastructure rather than ad hoc integrations.

Industry Scenarios — The EU Data Act in Practice

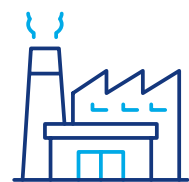
The following scenarios illustrate how the EU Data Act creates concrete compliance requirements — and strategic opportunities — across key industries.



Automotive OEM

A European automotive OEM manufactures connected vehicles equipped with telematics units, ADAS systems, and OTA software platforms. Under the EU Data Act, vehicle owners, fleet operators, and authorized workshops gain legal rights to access and share in-vehicle generated data with third-party repairers, insurers, and analytics partners. The OEM must provide standardized, secure access to vehicle-level datasets while protecting safety-critical systems, cybersecurity integrity, and proprietary algorithms.

Automotive OEM/Connected Vehicle	
Key Datasets	Sensor diagnostics, fault/error codes, battery charge cycles, ADAS event logs, firmware histories, telematics identifiers, mileage and usage counters
Platform Requirements	Dataset classification/segmentation (safety-critical/secret/operational), vehicle-level consent delegation, secure export & interoperable APIs, controlled sharing with repair networks, automated retention and redaction



Industrial Equipment OEM

A European industrial OEM manufactures connected production machines (CNC, robotics, packaging lines, compressors) and operates a remote diagnostics and predictive maintenance platform. Machine owners and operators gain legal rights to access and share machine-generated operational data with authorized service providers, insurers, and analytics vendors. The OEM must enable standardized, secure access while preserving trade secrets and safety-critical boundaries.

Industrial Equipment OEM/Connected Machines	
Key Datasets	System operation logs, fault triggers, hardware parameters, firmware versions, device identifiers, network status, uptime and usage counters
Platform Requirements	Dataset classification (safety/secret/operational), machine-level authorization, consent delegation to service partners, immutable audit trails, retention policy automation



Smart Home & Building Platform

A smart home platform provider operates a central gateway aggregating multiple device brands into a single cloud environment. Under the EU Data Act, this provider must support controlled sharing where users can access or share relevant data per device, per dataset, per purpose — without exposing other household members' data or sensitive security details. Role-based access (owner, tenant, family) and clean revocation workflows are essential compliance requirements.



HealthTech Wearable Platform

A European HealthTech company produces connected wearable devices (smart watches, biometric sensors) with a cloud analytics platform used by individuals, clinics, insurers, and corporate wellness programs. Users legally own the right to access and share their wearable-generated data with third parties. Athletes may authorize performance analysts, patients may grant clinicians access to recovery metrics, and employees may permit corporate wellness platforms to retrieve selected datasets.

Smart Home/Building Platform Provider

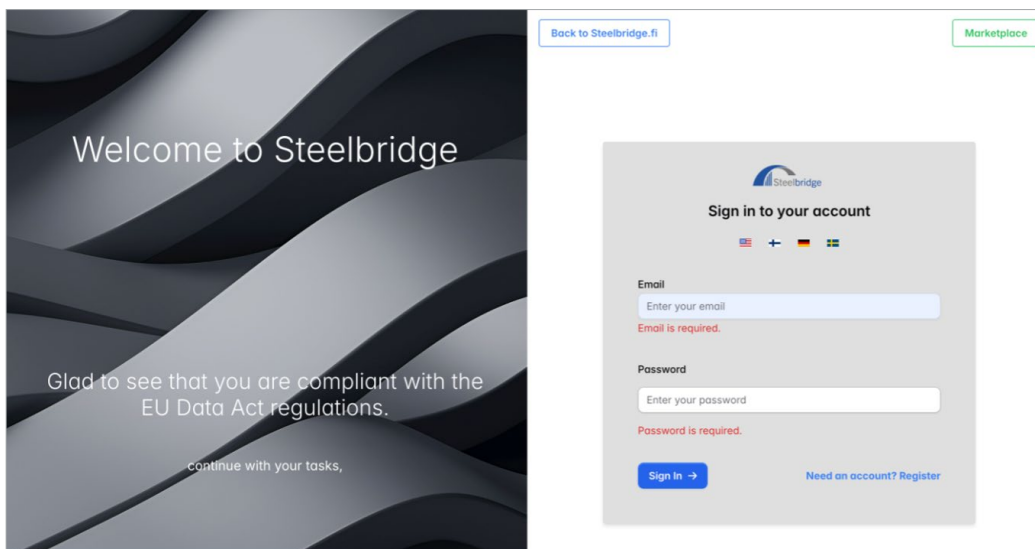
Key Datasets	Sensor streams (motion/temperature/contact), device activity logs, automation rules and execution logs, device metadata, integration logs, intercom session metadata
Platform Requirements	Identity & role management, consent flows, fine-grained dataset scoping, multi-user household permissions, third-party onboarding, traceable consent & revocation, audit & monitoring

HealthTech Wearable & Remote Monitoring Platform

Key Datasets	Time-series heart rate and motion streams, GPS and session summaries, sleep stages, training load, recovery indicators, device identifiers, consent and access logs
Platform Requirements	User identity verification, consent & revocation workflows, scoped OAuth/API access, dataset catalogues, machine-readable exports, immutable audit trails, sensitive health-data security controls

The Steelbridge Data Act Platform (DAP)

Steelbridge Oy has built the Data Act Platform (DAP) as a purpose-designed SaaS solution that operationalizes EU Data Act compliance. The platform connects data holders, end users, and third parties through standardized interfaces, automating the technical and operational requirements of the regulation. Its core principle is straightforward — Steelbridge does not store data, it makes existing data accessible and compliant.



Data Holder Interfaces

Integrate connected products and enable real-time, role-based data access for users and authorized partners.

A read-only proxy layer sits on the customer's own assets, creating compliant data access points without disrupting existing infrastructure. A built-in billing layer opens direct monetization channels, turning data access into a new revenue stream — without the complexity of building it in-house.



End User Interfaces

Allow users to view, authorize, and manage access to their data securely through compliant self-service workflows.

The platform's strong authentication and consent management capabilities ensure that individuals always remain in control of their data. Multiple cloud-side security layers protect every interaction, building the trust that regulatory compliance demands.

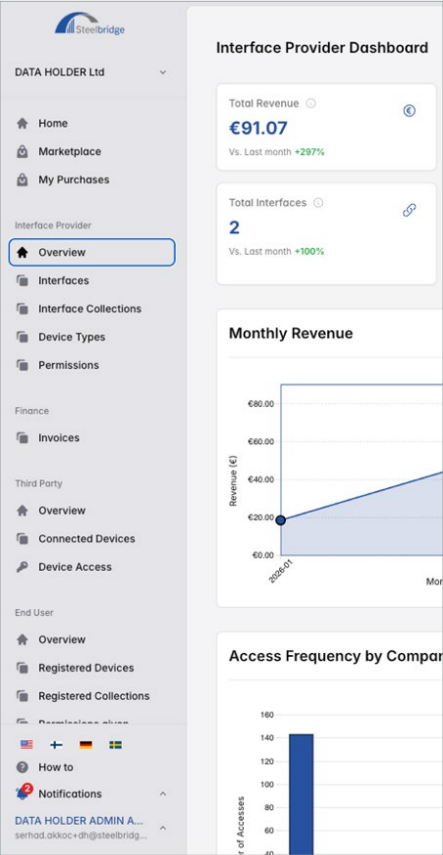


Third-Party Interfaces

Manage contractual rights, billing, and API connections for authorized analytics and service partners.

The platform handles company verification, consent tracking, and smooth onboarding through subscription-based pricing that removes high upfront barriers — alongside partnership opportunities that enable ecosystem growth.

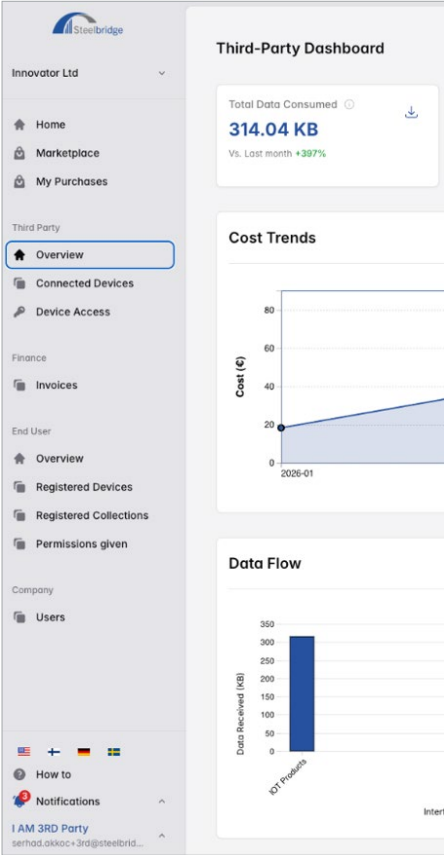
Data Holder Interfaces



End User Interfaces

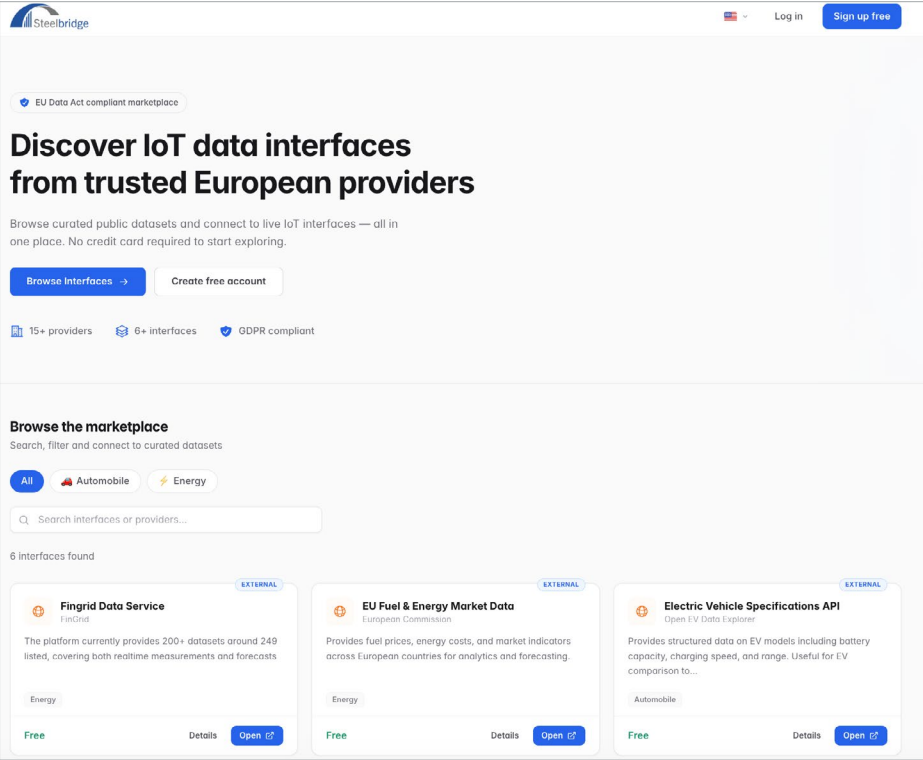


Third-Party Interfaces



Marketplace

The Marketplace enables data holders to publish public data interface feeds that contain no personal or user-identifiable information. By separating anonymized or aggregated datasets from consent-based user feeds, companies can unlock monetization pathways without being dependent on individual user permissions. This approach allows continuous data-driven revenue generation while remaining aligned with EU Data Act and GDPR principles.



Tab. 4 – Steelbridge EU Data Act Platform – Business Value

Platform Capabilities	Deployment
• End-user access portal with structured, machine-readable data export • Advanced consent management with granular scope control and instant revocation • Verified third-party onboarding with identity validation and contractual binding • Immutable audit trail logging across all access, transactions, and consent events • Built-in financial layer supporting usage-based pricing, subscription billing, and margin control • Tiered pricing logic allowing differentiated rates based on third-party size or profile • Dataset catalogue with feed classification, access rules, and monetization configuration • API gateway orchestration layer to standardize and govern device endpoint exposure • Marketplace module for anonymized or aggregated public data feeds • Alignment with EU Data Act Articles 4–6, with structured interoperability for EU data spaces	• Immediately deployable when device data endpoints are technically available • White-label implementation using the data holder’s brand assets delivered in approximately 4 weeks • Supports secure API integrations into existing device backends, clouds, and data lakes • Scales from single-product compliance to multi-brand enterprise marketplace environments • Designed for multi-tenant, multi-jurisdiction, and regulated industry environments

Compliance is not the destination — it is the launchpad. Steelbridge Data Act Platform turns your regulatory obligation into a governed, scalable data business from day one.



Outlook — What Comes Next

Effectively and efficiently navigating the requirements under the EU Data Act can be challenging, especially in industries with huge amounts of IoT products and services. In the following, we have summarized some of the key questions and steps from our experience from several engagements.

Is your organization ready? Key questions to ask upfront

What data does my connected product **generate**, and how is it **classified**?

Do I have **auditable, automated workflows** for consent and access?

Which products in my portfolio fall under the **EU Data Act**?

How is data compliantly **shared with users** and **third parties** today?

What **data monetization opportunities** does compliance unlock?

What **end-to-end processes** do I need to implement or update?



Recommended Next Steps

Organizations that move early will not simply comply — they will lead. We recommend the following path:

1. Initiate a Readiness Assessment —

Map obligations against current practices with Deloitte's regulatory expertise.

2. Engage Legal and Technical

Experts — Combine Deloitte's advisory depth with Steelbridge's platform capabilities.

3. Deploy Scalable Infrastructure —

The Steelbridge DAP provides a compliant, production-ready foundation that can be live immediately.

4. Design a Data Monetization

Strategy — Identify new data-driven services and revenue streams enabled by your compliant infrastructure.

As AI accelerates demand for high-quality, real-world data, the EU Data Act shifts data access from a compliance obligation to a strategic prerequisite for innovation and competitiveness.

Frequently Asked Questions — Addressing Common Concerns

Data holders often raise similar questions when evaluating their EU Data Act compliance strategy. Below we address the most common concerns and explain why proactive compliance is both a regulatory necessity and a strategic advantage.

Q1: Can't we just handle data access requests manually via email?

Email-based processes may seem sufficient at low volumes, but they create significant compliance, security, and operational risks:

- **No audit trail:** The regulation requires immutable, machine-readable logs of all data access requests, authorizations, and transfers. Email chains do not meet this standard.
- **No consent management:** Users must be able to grant, modify, and revoke access in real time. Email workflows cannot operationalize dynamic consent at scale.
- **Security vulnerabilities:** Sending sensitive operational or personal data via email violates modern security best practices and exposes companies to data breach risks.
- **Non-scalable:** Once user and third-party volumes grow, manual email handling becomes unmanageable and legally risky.

Conclusion: Email-based workarounds do not meet the technical, security, or auditability requirements of the EU Data Act. Regulators will expect standardized, automated interfaces.



Q2: Why invest now? Can't we wait until we see real demand from customers and third parties?

The EU Data Act is in force now — compliance is not optional, and demand will materialize whether you are ready or not:

- **Legal obligation, not market-driven:** The regulation grants users and third parties legal rights to access data. You cannot wait for 'enough demand' because even a single valid request triggers your compliance obligations.
- **First-mover advantage:** Companies that deploy compliant infrastructure early can shape partnerships, pricing models, and data strategies on their own terms — before competitors do.
- **Reputational and penalty risk:** Delays expose you to regulatory enforcement, customer dissatisfaction, and competitive disadvantage. Non-compliance penalties can be significant.
- **Time to deployment:** Building compliant infrastructure takes months. Waiting until demand surges leaves you scrambling to catch up while competitors are already monetizing.

Conclusion: Compliance is mandatory from day one. Proactive companies treat this as a strategic opportunity, not a reactive cost.

Q3: Why would third parties even want access to our data? Is there real market interest?

Third-party interest is not speculative — entire business models depend on accessing machine-generated data:

- **Independent service providers:** Maintenance companies, repair shops, and aftermarket service partners need operational data to diagnose issues, optimize performance, and offer competitive services.
- **Analytics and optimization vendors:** AI-driven analytics firms, energy management platforms, and fleet optimization providers monetize insights derived from aggregated operational datasets.
- **Insurers and financial services:** Usage-based insurance, leasing companies, and asset finance providers require real-time data to price risk accurately and offer dynamic products.
- **Ecosystem partners:** Smart home integrators, industrial automation platforms, and health analytics companies build value-added services on top of standardized data access.

Conclusion: Third-party demand is real, proven, and growing. The EU Data Act unlocks these partnerships — companies that provide compliant access will capture the value.



Q4: Won't providing data access expose our trade secrets or competitive advantage?

The regulation explicitly protects trade secrets and proprietary algorithms. Compliance does not mean open access to everything:

- **Dataset segmentation:** Platforms like Steelbridge DAP enable you to classify datasets as operational, safety-critical, or trade-secret protected — and expose only what the regulation requires.
- **Legal safeguards:** Article 4(2) and the Digital Omnibus proposal strengthen protections against unauthorized disclosure of commercially sensitive information.
- **Controlled sharing:** You define the scope, duration, and conditions of access. Third parties sign contracts, and all interactions are logged and auditable.
- **Competitive differentiation:** Companies that provide clean, standardized data access will attract premium partnerships and ecosystem integrations — becoming the preferred platform in their industry.

Conclusion: Proper implementation protects trade secrets while unlocking compliant data sharing. The risk lies in non-compliance, not in controlled access.

.....

Q5: Can't we just build this internally? Why use a third-party platform?

Building EU Data Act compliance infrastructure in-house is technically possible but strategically inefficient:

- **Development time:** Internal builds typically take 12–18 months. Steelbridge DAP deploys Data Holders data end points in real time, ensuring compliance before regulatory pressure escalates.
- **Ongoing maintenance:** Regulations evolve (e.g., the Digital Omnibus). A SaaS platform absorbs regulatory updates automatically, while internal solutions require continuous legal and technical overhead.
- **Specialization:** Platforms like Steelbridge are purpose-built for multi-role workflows (Data Holder, End User, Third Party), consent management, billing, and auditability — capabilities that are non-trivial to replicate.
- **Cost efficiency:** Internal development diverts engineering resources from core business innovation. Subscription-based platforms eliminate upfront CapEx and align costs with usage.

Conclusion: Unless compliance infrastructure is your core competency, buy rather than build. Focus your engineering resources on products that differentiate you in the market.

.....

Q6: What if the regulation changes or enforcement is weak? Isn't this all premature?

The EU Data Act is already in force, and the Digital Omnibus proposal strengthens — not weakens — its scope:

- **Legal certainty:** The regulation is final EU law. The Omnibus refines implementation details but expands the definition of 'data holder,' bringing more companies into scope.
- **Enforcement will escalate:** Regulators are building enforcement capacity. Early non-compliance cases will set precedents and signal seriousness to the market.
- **Customer and partner expectations:** Even without aggressive enforcement, your customers and ecosystem partners will expect compliant data access. Competitive pressure will drive adoption faster than regulatory fines.
- **Future-proofing:** Investing now in modular, scalable infrastructure prepares you for adjacent regulations (AI Act, NIS2, DORA) and evolving data governance requirements.

Conclusion: Waiting for enforcement is a high-risk strategy. Proactive compliance positions you as a market leader and avoids the costs of reactive scrambling.

The companies that succeed under the EU Data Act will be those that treat compliance as a strategic enabler, not a regulatory burden. Delay creates risk. Action creates opportunity.

By combining Deloitte Germany's regulatory and strategic expertise with Steelbridge's technology platform, companies can move confidently from compliance risk to data opportunity — building trust, transparency, and competitive advantage in the European data economy.

Deloitte GmbH Wirtschaftsprüfungsgesellschaft

EU Data Act Advisory | Germany

www.deloitte.com/de

Steelbridge Oy

EU Data Act Technology Platform

www.steelbridge.fi



Contacts

Deloitte



Dr. Ljuba Kerschhofer-Wallner

Partner & Offering Lead
Enterprise Risk
Tel: +49 151 18058037
lkerschhoferwallner@deloitte.de



Titus Aust

Senior Manager
Data Compliance & Monetization
Tel: +49 151 18295067
taust@deloitte.de

Steelbridge



Serhad Akkoc

Chief Executive Officer
Steelbridge Oy
Tel: +358 40 505 8157
serhad.akkoc@steelbridge.fi



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides leading professional services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our people deliver measurable and lasting results that help reinforce public trust in capital markets and enable clients to transform and thrive. Building on its 180+-year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's over 470,000 people worldwide work together every day to make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

