



Nemko
Digital



CASE STUDY

Building a Practical EU Data Act Compliance Framework for Connected Products



Executive summary

A multinational provider of connected products and digital services had already completed a broader assessment of EU digital regulation and identified the EU Data Act as a priority. The next challenge was practical implementation: determining which exact products and data was in scope, assigning ownership, designing request-handling processes, and establishing the governance, contractual, policy and technical controls needed for sustainable compliance.

The resulting framework translated regulatory obligations into an operating model that could be applied across business units without unnecessary complexity or over-engineering.

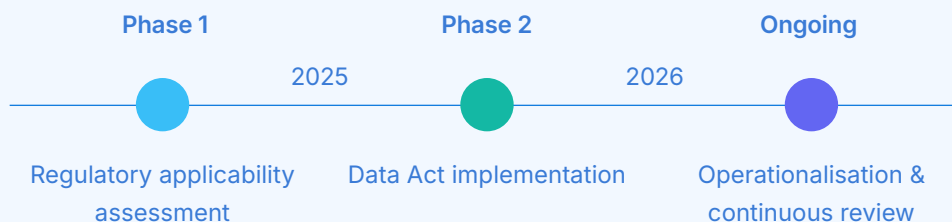


Figure 1. Programme progression from applicability assessment to implementation and ongoing operationalisation.

Section 01

Situation

01

The organisation operates connected products across multiple European markets, generating telemetry, event information and operational insights for service delivery and product improvement. Following the Data Act's September 2025 applicability, attention turned to the September 2026 milestone for data-access-by-design requirements affecting connected products and related services. The regulatory direction was clear, but translating it into clear ownership, user rights, data access mechanisms and technology requirements remained unresolved.

The programme therefore focused on six practical questions:

01. Which data must be made available under the Data Act?

04. What contractual and policy changes are required?

02. How should customer requests be received, validated and fulfilled?

05. How should technical capabilities support compliance?

03. Which central and local teams should own each activity?

06. How can the model scale across products, markets and business units?

Section 02

Why implementation was challenging

02

The scale and diversity of the portfolio created several distinct challenges:

Data scope

Connected products generate large volumes of information across systems. The organisation needed a defensible inventory of data categories falling within scope.

Ownership

Technology, legal, compliance and customer-facing functions all had roles. Without clear accountability, validation, communication and delivery could become fragmented.

Practical process design

The regulation establishes rights and obligations while leaving room for implementation choices. The operating model needed to be proportionate to anticipated request volumes.

Future-proofing

The organisation wanted more than point-in-time documentation: it needed a framework that could accommodate future products, markets and evolving expectations.

Section 03

03

The approach

1. Identify data in scope

The project mapped the connected-product ecosystem and assessed the primary data and relevant metadata. The data was classified according to key Data Act-relevant criteria, as outlined below:

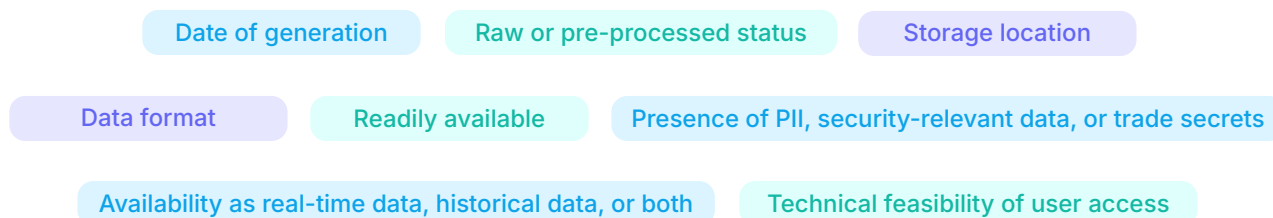


Figure 2. Data-in-scope inventory classification

The outcome was a formal inventory identifying the datasets that fall within the scope of the Data Act and are therefore subject to the applicable obligations.

2. Establish governance and ownership

A governance framework separated central technical delivery from local customer-facing responsibilities. Corporate oversight and compliance governance provided the control layer, while central technology handled storage, extraction, technical enablement and data preparation. Local business units handled customer communication, authentication, request validation and contract implementation.

3. Design a proportionate data-access process

Rather than introducing highly automated workflows by default, the organisation adopted a practical model based on anticipated request volumes. Requests move through user authentication, validation, data preparation, delivery and record-keeping, with historical and real-time access mechanisms supported as appropriate.



Figure 3. High level data request journey.

4. Assess and refine contractual arrangements

The programme assessed customer agreements to identify provisions affected by the Data Act. Existing contractual frameworks were reviewed against Data Act requirements relating to data access, data sharing, user rights, responsibilities of the parties and operational processes for handling requests.

The outcome was a set of recommended contractual updates and model clauses that could be incorporated into future contract negotiations and renewals. The review also established a governance mechanism to periodically reassess contractual arrangements as products, services and data-sharing models evolve.

5. Put controls and documentation around the process

The compliance package included data inventory documentation, data-sharing policies, request-handling procedures, logging mechanisms, customer communication materials, contractual guidance and governance recommendations. Together, these elements supported both implementation and ongoing maintenance.

Supporting deliverable: Data Act Compliance Documentation Package

The implementation was consolidated into a formal Data Act Compliance Documentation Package, providing a structured record of key decisions, documented controls, short-term actions, implementation responsibilities and handover considerations.

Data Act Compliance Documentation Package

Organization: ExampleCorp
Framework / Regulation: Data Act (Regulation (EU) 2023/2854)
Document Version: 1.0 (15/06/2026)
Date: 17/06/2026
Prepared By: Nemko Digital

1. Purpose of this Documentation Package	2
2. Key decisions and delimitations underlying Data Act for ExampleCorp	2
3. Overview of Documented Controls	3
3.1. Data In Scope Inventory	3
3.2. Data Sharing Policies and Processes	3
3.3. Customer contract clauses.....	3
4. Items requiring short-term actions	4
5. Implementation across ExampleCorp	4
6. General Considerations	5
7. Handover	5
8. Disclaimer	6

Figure 4. Data Act Compliance Documentation Package — document structure.

The package provides evidence that the programme moved from regulatory interpretation into documented operational controls, including the data-in-scope inventory, data-sharing policies and processes, customer contract clauses, short-term actions, implementation considerations and handover.

Section 04

Value Delivered

04

The Data Act compliance approach delivered value beyond regulatory readiness, establishing a practical and sustainable framework for data access, accountability and governance. By focusing on proportionate controls and clear ownership, the organisation strengthened its ability to meet current Data Act requirements while building the operational foundations to respond to evolving data-sharing obligations.

Clear accountability

Defined ownership across governance, technology and customer-facing functions.

Practical compliance

A proportionality-based approach avoided unnecessary investment in overly complex technical solutions.

Operational readiness

The organisation can receive Data Act requests, validate user rights, deliver historical data, support real-time access mechanisms, maintain audit trails and prepare for future reviews.

Long-term sustainability

The governance model can evolve with new products, technology changes and regulatory expectations.

Section 05

Next steps

The focus shifts from project implementation to operationalisation. Priorities include maintaining inventories and policies, monitoring implementation across business units, reviewing product changes for Data Act implications, embedding compliance reviews into governance processes, and supporting future connected-product initiatives.

The case demonstrates how an organisation can move from regulatory interpretation to practical capability. By combining data scoping, clear accountability, proportionate request processes, supporting controls and technical enablement, the organisation established a scalable framework for ongoing EU Data Act readiness.

