August 18, 2025

The EU Data Act: Impact on Connected Products and Device Manufacturers

Any Organisation Established Outside the EU but Operating in the EU Market Will Potentially Fall Within Scope

Authors: Huw Beverley-Smith, Hans-Christian Mehrens, Emily J A Evans

At a Glance

- The Data Act applies to a wide range of "products", including any tangible, movable item (even when incorporated into an immovable item) that collects or generates data about its use or environment and can communicate this data via a publicly available electronic communications service and whose primary function is not the storing and processing of data.
- The Data Act aims to make real-time data available to owners and users of devices and third-party service providers, increasing the choice of providers and potentially reducing costs. This will have an impact on device users in a range of industries, from health care providers accessing patient data generated by medical devices through to farmers seeking data from agricultural machinery.
- Manufacturers exporting connected products to the EU must adapt both their product design and internal data governance procedures.
- Companies that previously relied on exclusive control of device data for aftermarket services, monetization or competitive advantage will face new competition from independent EU service providers. The possibility of continuous, real-time access for third parties can also open doors for data-driven innovation.

The European Union's Data Act (Data Act) marks a transformative shift in the governance of data generated by connected products, especially within the Internet of Things (IoT) ecosystem. In Part 1, we discussed the impact on U.S. businesses of the new data switching rights for EU customers. Other key changes are the new technical requirements and burdens on the manufacturers of connected products and device manufacturers.

Background: Perceived Market Problems in Respect of Connected Devices

The Data Act aims to address issues which have been on the European Commission's agenda over the last 10 years or so in respect of data generated by connected "Internet of Things" (IoT) devices. Prior to the introduction of the Data Act, manufacturers of IoT devices had exclusive control over all data generated by use of the device, by virtue of its technical design. This could give them a dominant or possibly monopolistic position in the market. Businesses or consumers who used the devices had limited access to the data generated by the devices.

The inability to access IoT data, so the argument went, stifled innovation and limited opportunities for new business models and services. This led to potential competition problems on secondary markets (for example, in relation to aftermarket and complementary products). Independent service providers were frequently locked out of secondary markets due to a lack of access to device-generated data. For example, in-vehicle data generated by connected cars (such as technical data about the car or the users' driving behaviour) is typically exclusively controlled by the manufacturers of the car. This gives the manufacturers a monopolistic position with respect to the secondary markets (such as repair and maintenance services). If the data cannot be accessed, then the car cannot be repaired. This restricts access to third-party service providers, limiting market competition and consumer choice.

Another key area of concern for the European Commission relates to data produced by smart agricultural machines, which are controlled by a small number of agricultural machine producers. Farmers and third-party agricultural service providers would have limited access to the data, potentially restricting the ability of farmers to analyse the data and for third parties to provide. For example, yield data collected by a connected harvesting machine would typically only be available through the manufacturer's proprietary application or an approved dealer. The farmer would not easily be able to export this data for analysis by the farmer or by agricultural consultants who might be able to provide tailored crop management advice. Further, only the manufacturer or an authorized dealer can typically access the machine's data and provide predictive maintenance services. The Data Act aims to make real-time data available to farmers and third-party service providers (where this is technically feasible), increasing the choice of providers and potentially reducing costs.

Connected medical devices are yet another area where the data generated by, for example, a patient monitoring device, is frequently kept within the device manufacturer's proprietary platforms. Health care providers cannot easily access the raw patient data to integrate it with their other information systems. Similarly, third-party service providers (e.g., analytics or telemedicine platforms) are unable to access the data unless the manufacturer agrees to provide interfaces to the data — which they can refuse at their discretion or charge prohibitively high licensing fees which go beyond what's required to recoup the manufacturer's investment costs in developing the device.

The Data Act: IoT Data Objectives & Scope

The Data Act aims to redress these perceived imbalances. Its objectives include:

- Facilitating data access and use for consumers and businesses
- Empowering individuals regarding their IoT data
- Promoting fairness in the allocation of data-derived value
- Ensuring competition and innovation across sectors
- Maintaining incentives for continued investment in data-generating technologies

As highlighted in our previous alert, the Data Act has extraterritorial scope. Any organisation established outside the EU but operating in the EU market will potentially fall within scope of the Data Act. Companies outside of the EU that come within the scope of the Data Act must appoint a legal representative in one of the EU member states (similar to the requirements for representatives under the GDPR).

The Data Act applies to a wide range of "products", including any tangible, movable item (even when incorporated into an immovable item) that collects or generates data about its use or environment and can communicate this data via a publicly available electronic communications service and whose primary function is not the storing and processing of data, will be included. This includes most IoT devices, from smartwatches to connected industrial and home appliances. However, it excludes products whose primary function is to display or record content for online services (e.g., PCs and smartphones).

Personal and Nonpersonal Data

The Data Act's requirements apply to all data, both personal and nonpersonal. This includes data generated by the use of a product that is recorded intentionally or captured by the device. However, it does not cover derived or inferred data, r including data which is the result of additional investments in developing systems for analysing the

data (for example, analysis of users' health, such as fitness age through an algorithm).

Key Legal Obligations for Manufacturers

User Access Rights

The Data Act gives rights to users of connected products to access the data or request access to the data to be provided to a third party of their choice. If users cannot directly access their data, the manufacturer (or the "data holder") must provide it "without delay, free of charge, and, where applicable, continuously and in real time."

Notably, the definition of a data holder may shift, depending on the context. If a manufacturer transfers control of the data, the recipient business takes on the obligations of a data holder. For example, if a connected machine tool is installed in a factory and the manufacturer contracts with a third-party maintenance provider to monitor the machine tool's performance and health, the maintenance provider will be the data holder in addition to or instead of the manufacturer, since the maintenance provider collects, stores and analyses the data. Similarly, if a hospital's IT department aggregates, stores and controls access to patient data from patient monitoring devices, it may be the data holder, rather than the manufacturer. Businesses and users will therefore need to analyse the role of each party in the data supply chain.

There are, however, certain limitations on the rights of access. Data holders can impose restrictions on access, use or further sharing of data where this would undermine the security requirements of a connected product under EU or member-state law (for example if such access compromised the confidentiality of patient data under the GDPR or member-state confidentiality laws). In addition, the data holder can impose limits on the disclosure and use of their trade secrets by agreeing with the user on appropriate technical and organisational measures to protect the shared data. Where restrictions cannot be agreed, or if the user fails to implement appropriate measures, the data holder can withhold or suspend the sharing of data it has identified as trade secrets (but must notify the competent member-state authorities).

Further, users may not use the data obtained from the data holder to develop a competing product, nor share the data with a third party for the purposes of using the data to derive insights about the economic situation, assets and production methods of the manufacturer or the data holder. However, this restriction does not prevent users from developing related services (which is one of the key policy objectives of the Data Act).

Contractual & Commercial Terms

The Data Act prohibits certain unfair contractual terms in business-to-business (B2B) data sharing contracts. Data

holders must provide access to third parties on “fair, reasonable, and non-discriminatory” (FRAND) terms. While the Data Act leaves flexibility around what constitutes FRAND, costs charged to micro, small or medium enterprises (SMEs) must not exceed the direct cost of making data available. This may affect pricing strategies and licensing models for U.S. manufacturers operating in the EU.

Data Access by Design

Manufacturers must ensure that in-scope products are designed so that data generated through their use is easily, securely and directly accessible to the user by default. This does not mean that the data holder must transfer a copy of the data, but that the data should be made available to the user from a remote server. This technical accessibility must be built into the product itself, representing a significant new data-portability right for users and a corresponding design and compliance burden for manufacturers.

This is not an absolute obligation requiring access to data to be granted in all situations — it only applies “where relevant and technically feasible”. The European Commission has clarified in its guidance that this is meant to reinforce the manufacturers’ discretion to decide whether to design a connected product in a way that provides users with “uncontrolled” access (i.e., without any intervention by any other party) or in a way that provides access with additional controls (typically via a remote server). Manufacturers may assess, for example, whether direct access is technically possible; the costs of potential technical modifications; and the difficulty of protecting trade secrets or IP, or of ensuring the connected product’s security. Based on this assessment, manufacturers may choose to design the connected product in such a way that all or part of the product data is directly accessible or may enable only indirect access.

However, the device-generated data need only be available to the user, and the IoT product does not need to be designed in such a way that the user can make the data accessible to third parties as well. As such, this data access by design provision is of limited benefit to providers of aftermarket and connected services. Given that the redesign of products will take time, the obligations relating to product design will apply from 12 September 2026.

Relationship With the GDPR & Penalties for Noncompliance

The Data Act sits alongside the General Data Protection Regulation (GDPR), but in the event of conflict the GDPR will take precedence. If noncompliance with the Data Act also involves personal data (as will frequently be the case), then GDPR-level fines will apply in respect of such personal data.

The Data Act requires member-states to set out rules on penalties, which must be “effective, proportionate and

dissuasive". The types and amounts of penalties are not set at EU level. This will be determined by each member state through national implementing legislation. It is likely that these will be similar to (although not directly reflect) the penalties imposed by the GDPR relating to personal data (which provides for fines of up to €20 million or 4% of global revenue, whichever is higher). For example, the Netherlands provides for fines up to €1,030,000 or 10% of global revenue (whichever is higher). In addition to fines, nonmonetary penalties can include reprimands, warnings, orders to comply or cease infringing conduct, and compensation awards to affected parties.

Implications for Manufacturers

Compliance & Technical Adaptation

Manufacturers exporting connected products to the EU must adapt both their product design and internal data governance procedures. This includes:

- **Technical Redesign:** Ensuring products are data-accessible by design, which may require significant R&D investment and changes to existing product lines.
- **Contractual Adjustments:** Revising agreements with EU users and third-party service providers to comply with the new data sharing, access and FRAND terms.
- **Ongoing Obligations:** Managing requests from users and third parties, maintaining secure data flows, and potentially enduring increased operational costs.

Impact on Business Models

The Data Act challenges the traditional "closed ecosystem" approach. Companies that previously relied on exclusive control of device data for aftermarket services, monetization or competitive advantage will face new competition from independent EU service providers. The possibility of continuous, real-time access for third parties can also open doors for data-driven innovation. While the changes will have a significant impact on many established manufacturers, the new regime may encourage partnerships with EU-based service providers, or drive new licensing and data-sharing business models. Some U.S. businesses will need to assess whether the additional compliance burden and competitive pressures are offset by the benefits of accessing the EU market.

Entry Into Force & Key Compliance Steps

Most of the provisions of the Data Act come into force on 15 September 2025. U.S. businesses which are in-scope (many of which are already suffering from compliance fatigue from the EU's flurry of digital legislation) have much to do. We set out below a list of key steps.

1. Assess Applicability

- Identify whether you manufacture, distribute, sell, rent, lease, or provide connected products or related digital services in the EU and assess the applicable exemptions.

2. Identify Data Holders & Users

- Determine if you are the “data holder” under the Data Act (i.e., control access to device-generated data) and assess the data supply chain.
- Identify the “users” (e.g., EU-based device owners, lessees or customers).

3. Map Data Flows

- Document what data is generated by each device or related service.
- Identify where data is stored, who has access and map the path from device to user.

4. Establish Data Access Mechanisms

- Develop or update mechanisms for users to access device-generated data (via device, app or portal).
- Set up electronic processes for user requests.

5. Enable Third-Party Data Sharing

- Provide mechanisms for users to authorize third-party providers to access their device data (e.g., agritech, digital health or analytics services).

6. Review and Update Contracts

- Revise customer contracts and terms of service to reflect user rights under the Data Act.
- Ensure that terms are fair, reasonable, nondiscriminatory and transparent.
- Review unfair contractual terms on data access or sharing, which grossly deviate from good commercial practice in data access and use, contrary to good faith and fair dealing (e.g., clauses excluding liability for intentional acts or gross negligence, clauses which give the data holder the exclusive right to determine whether the data supplied conforms with the contract, unfair limitations on use of data, or restriction of users’ remedies).

7. Review Data Security & Privacy

- Implement robust cybersecurity measures for data access and sharing.
- Ensure compliance with the GDPR and other data protection laws (data minimization, purpose limitation, user authentication).

8. Train Staff & Update Policies

- Train relevant staff (including, IT, security, product development and legal) on new data access and sharing obligations.
- Update internal IT, customer service and compliance policies.

9. Prepare for Compliance Requests & Audits

- Identify competent authorities in relevant EU markets.
- Document initial scoping assessments.
- Maintain records of data access requests, disclosures and compliance actions.

10. Monitor Legal Developments

- Stay informed about implementing legislation and enforcement practices in each EU member state, bearing in mind that there will be significant differences.
- Engage European coordinating counsel where there are obligations in multiple jurisdictions.

The Data Act comes into force on September 15, 2025.

MEET THE AUTHORS

Huw Beverley-Smith

Partner

+44 (0) 20 7450 4551
London

huw.beverley-smith@faegredrinker.com

Hans-Christian Mehrens

Associate

+44 (0) 20 7450 4531
London

hans.mehrens@faegredrinker.com

Emily J A Evans

Associate

+44 (0) 20 7450 4591
London

emily.evans@faegredrinker.com

Related Legal Services

Government & Regulatory

Health Care

Intellectual Property

International

Litigation

Product Liability & Mass Torts

Privacy, Cybersecurity, Data Ethics & Strategy

Health Care Privacy, Security & Cybersecurity

Health Information Technology & Innovation

Health Care Compliance & Regulatory

Technology Transactions & Licensing

Customs & International Trade

International Transactions

Antitrust

Trade Secrets & Noncompetes

Product Counseling & Risk Management

Recalls, Investigations & Regulatory Actions

Related Industries

Consumer Products & Retail

Financial Services

Food & Agribusiness

Health & Life Sciences

Insurance

Agribusiness

Medical Devices

Hospitals & Health Systems