TaylorWessing

Data Act step plan

Overview

- **Starting 12 September 2025**, users of connected products (e.g. connected cars, medical devices, smart home devices like smart washing machines, industrial/agricultural machinery) and related services (e.g. apps that control these products) will gain the right to access the data generated by using these products and services.
- The scope includes **raw and pre-processed data** (both personal and non-personal) generated by IoT products or related services, such as temperature, pressure, flow rate, or speed data collected from connected devices.
- The Data Act aims to boost the **EU's data economy** and foster a competitive market by encouraging broader **data sharing.**

Obligations

Data access

Data holders must allow direct or indirect data access.

- **Access by Design:** From **12 September 2026,** connected products and services, where relevant and technically feasible should be designed so that users can directly access the product data generated by their use thereof.
- **Request Mechanism**: Starting **12 September 2025**, if direct access is not available, users can request from the data holder access to readily available data **without undue delay** and free of charge.

Third-party sharing

Users may instruct the data holder to make available such readily available data to a third party (e.g. a service provider) but excluding gate keepers under Art. 3 of the EU Digital Markets Act. The data holder may charge a reasonable fee from these third parties, except for SMEs or non-profit research organizations, who can only be charged for the costs incurred.

Use limitations

While data use is generally unrestricted, users and third parties are prohibited from using the data to create directly competing products. Competition in related or aftermarket services is, however, not prohibited.

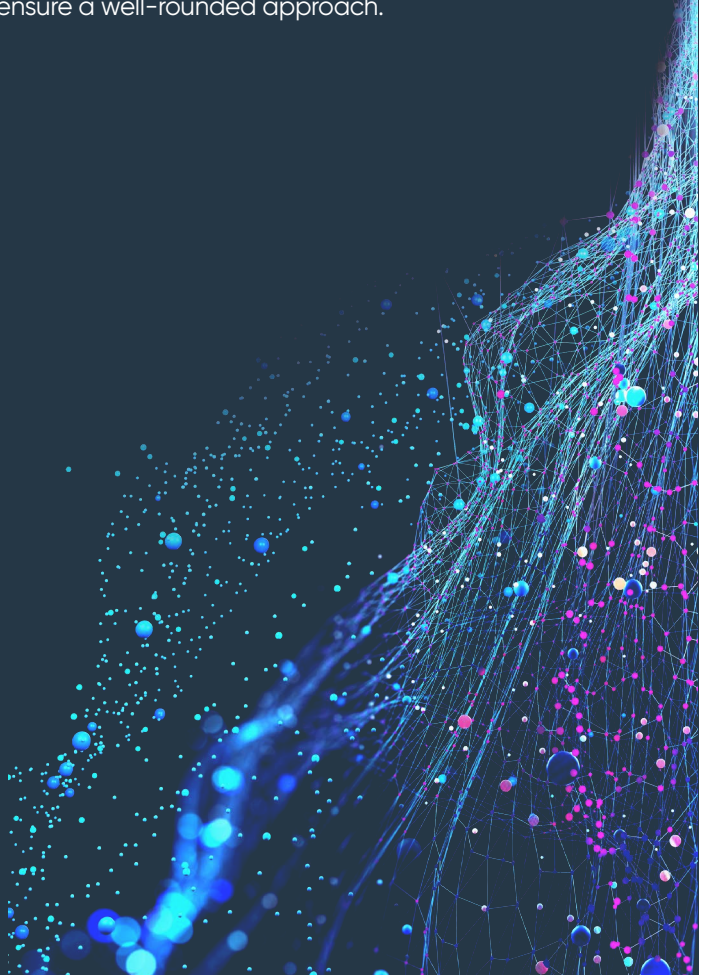
Safeguards

The Data Act includes mechanisms like the trade secrets handbrake and safety handbrake to protect sensitive data and maintain operational security.

Practical steps to ensure compliance

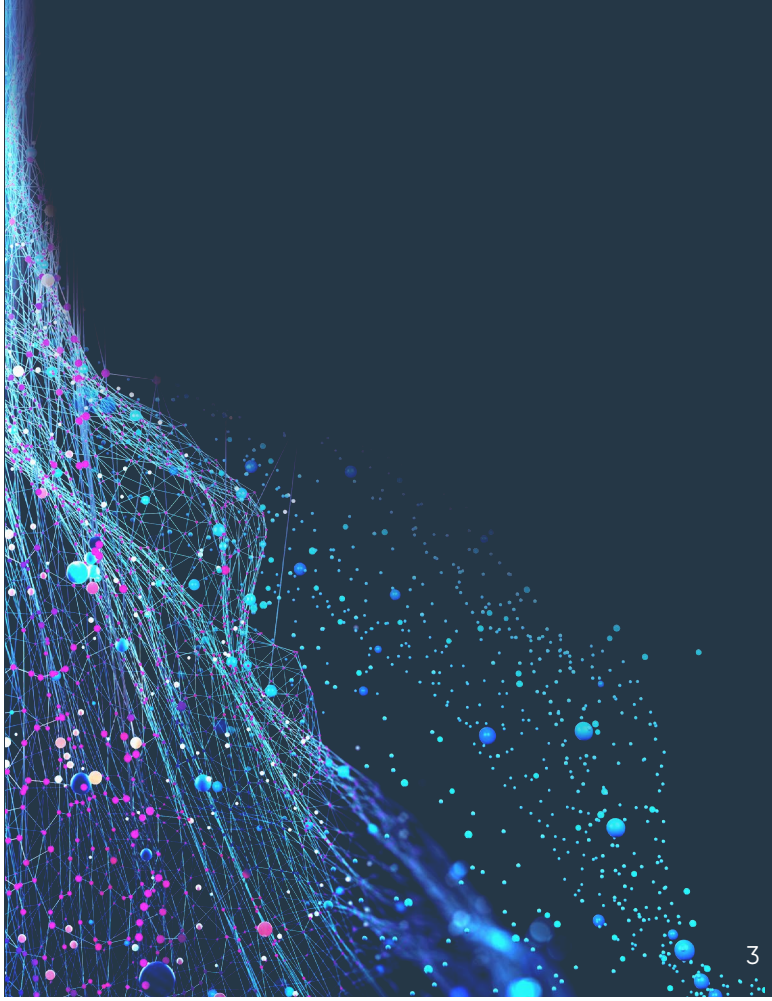
Step 1: Data identification and classification

- **Inventory of all data:** Start by identifying all data generated by IoT products or related services. This includes:
  - **Raw and pre-processed data** like sensor readings (e.g. temperature, pressure, usage patterns).
  - **Business-sensitive information** such as **trade secrets** or data critical for competitive advantage.
  - **Mixed Data:** Identify and separate **mixed data sets** (containing both personal and non-personal data). Ensure that personal data is handled in accordance with the GDPR, and consider **anonymizing or pseudonymizing** these data sets to avoid compliance risks when sharing with third parties.
- **Action**
  - **Use automated data classification tools** to
    - categorize high-risk data (e.g. trade secrets). In sectors like energy, use tools that can flag data from **smart meters** or **grid management systems** as highly sensitive due to their business implications.
    - flag mixed data sets and implement processes to either separate the personal data or apply anonymization techniques before sharing.
- **Set up a task force:** Create a **cross-departmental team** to collect and analyze this data. Include legal, IT, compliance, and business development teams to ensure a well-rounded approach.



Step 2: User and access management

- **Identify users and third parties:** Define the users of your products, including **individual consumers** and **business users** who may have access to the data. Identify potential third-party recipients (e.g. service providers or aftermarket vendors).
- Implement **automated systems** (e.g. **digital wallets** or **user accounts**) to verify user identities and manage access rights, as recommended by the Data Act. This is particularly useful in shared-device environments (e.g. **smart meters in multi-tenant buildings**).
- **Develop an access decision-making process:** Establish a clear internal process for **handling access requests:**
  - Who approves or denies access?
  - How are requests documented and tracked?
  - Make an inventory of the decisions to automate the process as far as possible.
- **Trade secrets and security handbrakes:**
  - Implement safeguards to protect **trade secrets** and ensure security. Define the measures required to invoke the **„trade secrets handbrake"** or the **„safety and security handbrake"**, where sharing data might cause **economic harm** or **operational risks**.
    - Establish **Non-Disclosure Agreements (NDAs)** and **technical controls** to restrict access to trade secrets. For instance, energy companies can limit access to **grid performance data** if sharing it would endanger operational security.
    - Consider additional technical and contractual measures to ensure the ongoing confidentiality and prevent an illegal use of your trade secrets.

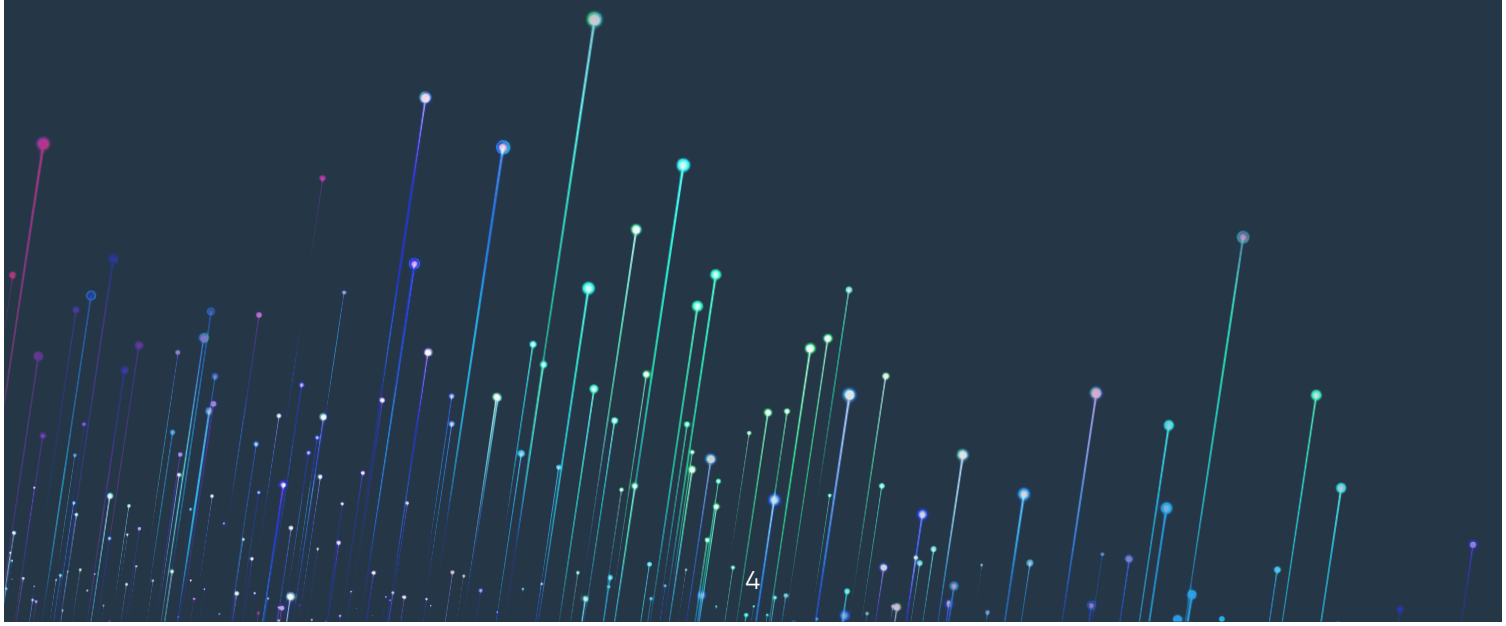


STEP 3 – Define your own data usage

- **Internal Usage of Data:** Clarify for which purposes your company will use the generated product data.
  - Is there a specific arrangement with the user for the generation and collection of product data?
  - Will the data be used to optimize product performance?
  - Can it create new revenue streams through value-added services?
  - Can it be used to train AI models or improve AI systems?

STEP 4 – Set up contractual framework and safeguards

- **Data licensing agreements:** Draft contracts that specify how data will be shared and under what conditions. Consider to include **compensation mechanisms** to encourage users limit or waive their data-sharing rights (per Recital 25).
- **Terms of use and TOMs:** Prepare terms of use that outline how users and third parties can access data. Define the **technical and organizational measures (TOMs)** needed to protect **sensitive data**, including trade secrets.
- **Transparency requirements:** Ensure that users are **fully informed** about what data will be collected, how it will be accessed, and for what purposes the data will be used.



STEP 5 – Stay Updated on Regulatory Changes

- **Monitor Regulatory Updates:** The European Commission has published an FAQ to assist with Data Act implementation. The FAQ will evolve, providing clarifications on rights and obligations under the Data Act. Monitor this FAQ and any additional guidance that follows.
- **Model Contracts:** The Commission is working on **model contractual terms** for B2B data-sharing agreements. Ensure you integrate these templates into your contractual processes to comply with the new B2B unfair contract clause section.
- The European Commission will assess **barriers to interoperability** and request the development of **harmonized standards** where needed. In case of insufficient standards, the Commission may issue **common specifications** to ensure conformity with the Data Act.
- **Track interoperability developments**
  - Interoperability between **data processing services** and **data spaces** ensures seamless data flow across systems, which is crucial for developing new products, fostering innovation, and encouraging **data-sharing** across sectors.
  - This applies especially to participants in **Common European Data Spaces** (offering data or data-based services), vendors of **smart contracts**, and **data processing services** providers.

Non-Compliance

- **Non-compliance with the Data Act can lead to severe penalties, including:**
  - Fines up to **4% of global annual turnover** or €20 million, whichever is higher.
  - **Unfair competition actions** by third parties.
  - Claims for **damages** from affected individuals.
  - Significant **reputational harm.**

Conclusion

These steps shall help companies to comply with the Data Act and capitalize on new business opportunities arising from IoT-generated data. Industries such as energy, manufacturing, and smart home services can leverage data-sharing to create **value-added services**, enhance **operational efficiency**, and **remain competitive in a data-driven economy.**

Your Contact

Alexander Schmalenberger, LL.B.
Knowledge Lawyer, Hamburg
+49 40 36803-352
a.schmalenberger@taylorwessing.com