

Implications of the EU Data Act for the engineering and plant construction industry

On 11 January 2024, the **Data Act**, new EU legislation to harmonise the regulation of the data economy, entered into force. It contains rules on access to and fair use of data to make it more accessible to all involved in its generation and promote data-driven innovation. Most of the Data Act becomes applicable from 12 September 2025.

The Data Act focuses on industrial data generated by the use of networked products and related services. From the EU's point of view, this promises potential for growth and innovation for the digital transformation which has not been sufficiently exploited up until now. The Act has far-reaching consequences for the engineering and plant construction industry:

What are the main aims of the Data Act and the requirements for your company?

The Data Act is intended to "form the cornerstone for a strong, innovative and sovereign European digital economy". The aim is to create a "fair", competitive data market. The resulting requirements for the engineering and plant construction industry are diverse:

- **Data access for users of connected devices:** Users of IoT devices – such as industrial machines, cars or other connected devices – will be able to access and use data.
 - Connected products must be designed and manufactured and connected services must be provided in such a way that the data generated during their use, including relevant metadata, can be accessed easily, securely, free of charge and – as far as technically possible – directly.
 - If direct access is not possible, product users (in both the B2C and B2B sectors) have a claim against the data owner for access to this usage data. The data owner is the person who is entitled or obliged to use and make available the data (this is often the manufacturer).
 - Users are allowed to use the data for certain purposes and can also pass it on to third parties for this purpose: While it is forbidden to use it to manufacture competing products, it is expressly intended to use it for competing services, such as repairs to networked products.
- **Data security and protection of trade secrets:** The data owner can only refuse to disclose the data concerned "in exceptional circumstances" and "on a case-by-case basis"; this may be possible in limited cases to protect business secrets. The data owner must justify this in writing. The refusal can be challenged before authorities, courts and in out of court dispute resolution proceedings.
- **Data exchange between companies:** The Data Act is intended to promote the voluntary, data protection-compliant exchange of data between companies.
 - By providing contract drafting guidelines and specifications, the Act aims to ensure that SMEs have access to data that they have co-generated in order to achieve a "fair" distribution of data value creation.
- **Data exchange between company and government:** The Data Act also includes rules on making data available to public bodies and requirements for data room operators to facilitate interoperability of data and data sharing mechanisms and services.

An example in the B2B sector: machine data

Data from machines and sensors are generated in large quantities in industry, especially in the engineering and plant construction industry. Different parties have an interest in using this data. The manufacturer of an automation component, for example, would like to have access to operating data of its product that is installed in a machine operated by a third party. Up until now, the parties have been able to regulate data access contractually to a large extent freely (or in fact through technical settings). In contrast, the Data Act envisages primarily granting the user the right to dispose of its data and its use and, if necessary, to pass it on to third parties. For example, in future the user of the automation component could grant independent third-party providers access to the machine data so that they can - for example - offer maintenance work. The manufacturer may only use non-personal usage data if it has agreed this with the user.

What needs to be done?

As a first step, companies should review their products, data processing practices and business models to ensure compliance with the Data Act and at the same time be able to clearly pinpoint possible effects on their own business model. Essential points in this context are:

- Overview of generated and used machine data in the company's product portfolio;
- Examine the significance of the machine data for (i) further (own) product development and (ii) for the product-related maintenance and service business;
- Overview of the current contractual regulations on data use with end customers.

In a second step, the next strategic measures can then be derived from this assessment. This includes:

- Determination of requirements for future product design;
- Adjustment of the underlying contractual conditions for (i) new machinery and equipment and (ii) machinery and equipment under maintenance;
- Implementation of the other requirements of the Data Act.

Your team



Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Partner, Berlin
+49 30 885636-408
p.voigt@taylorwessing.com



Dr. Christian Frank, Licencié en droit
Partner, Munich
+49 89 21038-197
c.frank@taylorwessing.com



Dr. Janina Pochhammer
Partner, Hamburg
+49 40 36803-105
j.pochhammer@taylorwessing.com



Dr. Carsten Schulz
Partner, Hamburg
+49 40 36803-132
c.schulz@taylorwessing.com



Henning von der Blumensaat, LL.M.
Salary Partner, Hamburg
+49 40 36803-439
hvonderblumensaat@taylorwessing.com



David Mallmann, LL.M.
Senior Associate, Hamburg
+49 40 36803-484
d.mallmann@taylorwessing.com