THE EU DATA ACT EXPLAINED: RIGHTS, OBLIGATIONS AND CHALLENGES FOR DATA HOLDERS AND MANUFACTURERS

Data & AI

Written by Zohar Efroni & Selman Özen
26 Jun, 2024

Agenda

What does the EU Data Act regulate?

The EU Data Act aims, among other things, to enable better access to IoT data and to strengthen "fairness" in B2B contractual relationships over data. It addresses the harmonization of rules on access to and use of IoT data within the European Union by providing a comprehensive set of rules and a framework for data sharing. This framework, including the implementation of various data sharing concepts, impacts both individuals and organizations. This is in line with the aim of promoting innovation and fair access to data, while protecting privacy and continuing to ensure fair competition in the European Union's internal market.

The law defines which user-generated data can or must be shared with companies and authorities or public sector bodies, thereby promoting the maintenance of user control over user-generated data and increasing data interoperability. The law regulates data access and transfer by providing guidelines to which data intermediaries, platforms and other relevant stakeholders must adhere. It also sets out clear responsibilities in relation to data processing, transparency and accountability, while establishing mechanisms to resolve disputes and enforce compliance.

Which products are affected and what are the challenges for manufacturers?

According to Article 2 (5) of the EU Data Act, a "connected product" is

primary function is not the storing, processing or transmission of data on behalf of any party other than the user

Some examples are consumer products such as connected cars, health monitoring devices or smart home devices as well as industrial products such as airplanes, robots or industrial machines. The scope of application is broad, and in case of doubt, "connected products" are all connected devices that generate data during use by the user. This may also include product categories that were initially excluded from the scope of the EU Data Act at earlier stages of its development (e.g. PCs or smartphones), although the final version no longer contains these exceptions. The concept of IoT devices is therefore broad.

Connected products (also known as "Internet of Things" (IoT) devices) generate a large amount of data. According to the EU Data Act, users of such products should be given more control over the data generated through their use. In addition, the transfer of data to data recipients is to be simplified.

What challenges do data holders face?

What data should be shared?

The definition of data covered by the EU Data Act leaves some questions unanswered, e.g. whether master data, product data or other static data, for example on technical features of the IoT product, are covered by the EU Data Act. Does the data holder only have to provide dynamic raw data, even if it is not useful or fit for purpose without supplementary, static data? Even if several users use the different aspects of a product, each user is only entitled to their "own" data but not to data generated by the use of others. How the data could be dynamically segmented and shared remains a major challenge.

Which data should/cannot be shared?

The protection of intellectual property and trade secrets remains important and is taken into account in the EU Data Act. The same applies to data protection. A compromise had to be found with the purpose and implementation of data

particularly challenging to establish technical and organizational mechanisms that consolidate compliance with the EU Data Act on the one hand, and data protection, IP and trade secrets on the other.

How should the user's access to the data be guaranteed?

According to Art. 3 (1) EU Data Act, connected products must be "designed and manufactured ... in such a manner that product data ... are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, directly accessible to the user." It remains unclear what direct provision of the data can or must look like technically in individual cases (see III below for more details).

How should the data recipient's access to the data be guaranteed?

If the data recipient wishes to receive the data at the request (with the consent) of the user, he may receive the data under FRAND conditions. The data holder may charge a fee for this but may not discriminate against data recipients or impose unfair contractual terms. How these obligations are interpreted and how the consent flows are checked remains to be seen.

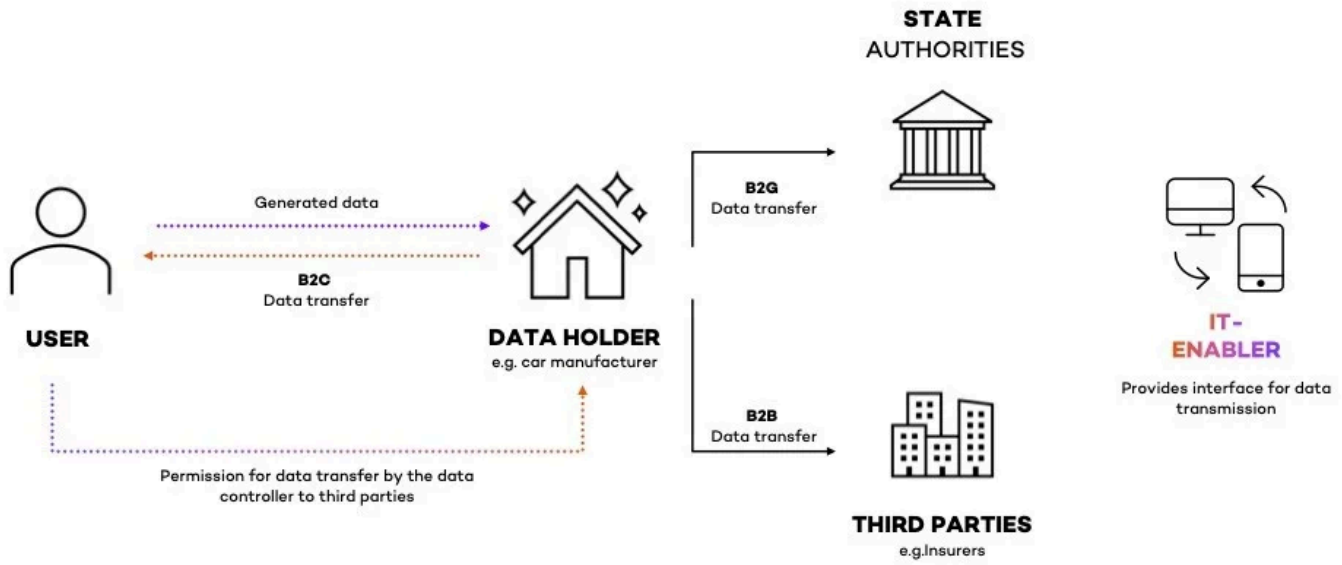
What does the data controller's duty to inform include?

Manufacturers of connected products must provide users with comprehensive and detailed information about product data capabilities. This information must also be understandable and clearly presented, which is the opposite of comprehensive and detailed. How a compromise between the two principles can be found remains to be seen.

Who are the various parties involved in the EU Data Act?

As described above, the EU Data Act focuses on data access rights to the product data of an IoT product. However, the access rights created by this not

This results in various special features and obligations for the various parties involved. The obligations arising from the EU Data Act must already be observed during the manufacturing of IoT products. The products must therefore already be manufactured in such a way that the product data can be made available easily, securely, free of charge and in a comprehensive, structured, common and machine-readable format as standard.



In the context of the EU Data Act, both manufacturers and data holder (if they are not one and the same person) should therefore examine their technical provision options, as manufacturers and data holder must provide the available data at the request of the user under the aforementioned conditions. If such a technical provision option does not yet exist, companies should introduce one in good time.

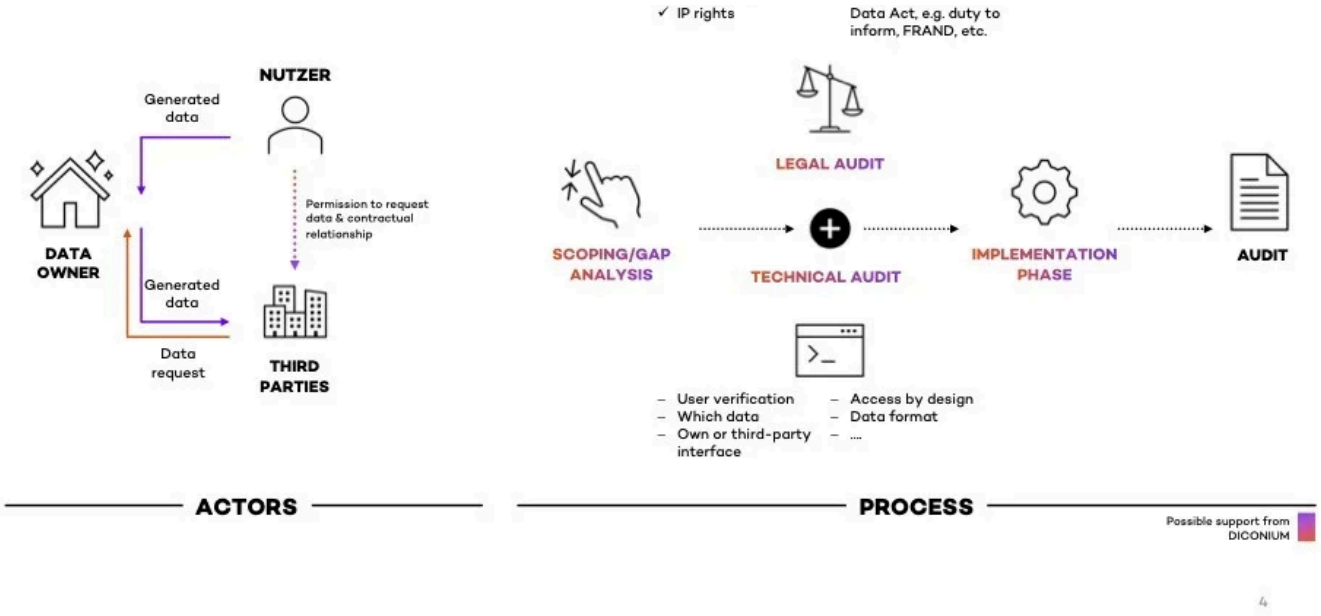
However, as already mentioned, the provision of data is not limited to the user himself. If the user requests the transfer of their data to third parties, the third party receives this data on behalf of the user. In this context, however, the third

In cases in which personal data is processed in addition to non-personal data, the GDPR must also be observed, as the GDPR continues to apply without restriction in addition to the EU Data Act.

As already mentioned above, the protection of trade secrets, among other things, may constitute an exception to the extensive right of access to data. Insofar as the relevant data embodies trade secrets, these are covered by the Trade Secrets Directive and may prevent or restrict a claim to the provision of the data to the user or to third parties. However, such a refusal or rejection would have to be considered and examined separately by the data holder in each individual case, as the existence of a trade secret would have to be demonstrated and proven.

Consequences for the automotive industry

The EU Data Act will have a significant impact on the automotive industry - particularly with regard to connected vehicles. For the mobility market, the EU Data Act opens up numerous new opportunities for business models based on the exchange of data in ecosystems, among other things. However, there are a large number of different players in the mobility sector, whose different focuses of interest and, in particular, the diversity and heterogeneity of mobility data, can lead to numerous challenges, which are explained in more detail below.



In future, car owners should have the right to use their data themselves or to pass it on to someone else, such as an independent workshop or insurance company. To this end, manufacturers must design their products and services in such a way that they technically enable access to the processed data ("data access by design"), as customers currently only have limited access to this data (e.g. via the right of access under Art. 15 GDPR). In addition, customers must be informed which IoT data is collected and for what purpose before they purchase a vehicle or use the (mobility) service (pre-contractual information obligations).

However, the legal framework that specifies the technical way in which the data from the vehicle can be made usable for all market participants is still missing. The problem here is that the EU Data Act covers all networked devices: From televisions with internet access to smartphones and smart fridges - modern cars are also covered. This approach is too broad and unspecific because the requirements for the various products differ. What is sufficient for a smart refrigerator is by no means enough for a vehicle. Sector-specific regulations for car data are reportedly planned, but have not yet been published by the EU Commission (June 2024).

In legal terms, car manufacturers are subject to transparency and information obligations, among other things. At the same time, they must comply with data protection regulations for personal data and protect their trade secrets. The EU Data Act also has an impact on various contractual documents in the

There are also a number of organizational challenges. Data providers and data recipients need to be brought together, access rights distributed and controls enforced. Governance principles are needed for data exchange, for IT and cyber security, and an agreement must be reached on who owns the customer interface, who is responsible for it and who controls access to users' (personal) data.

Car manufacturers are also concerned that third parties will enrich themselves from their technical developments if they are to share the data with them without restriction. A frequent concern of the industry is that knowledge of technical developments and trade secrets could be passed on to competitors. Insurers, on the other hand, are calling for a neutral data trustee, as they fear that car manufacturers will want to claim the potentially lucrative data business for their own benefit. According to Allianz Insurance, insurers and other companies could use vehicle data to offer new or better services, e.g. more risk-appropriate insurance offers.

The EU Commission should take the EU Data Act as an opportunity to clarify existing uncertainties for the automotive industry, particularly with regard to competition and data protection issues.

At the private sector level, companies enter into data partnerships and data cooperations with each other in order to ensure secure access to data that promotes innovation. In order to promote cooperation, the legislator should create greater legal certainty for cooperation agreements for data exchange between competitors through clarifying regulations in antitrust law.

When does the EU Data Act come into force and when do the obligations apply?

The EU Data Act provides for a staggered deadline for the respective regulations, which are described in particular in Chapters 3 and 4.

(see Art. 50 EU Data Act).

Conclusion and suggestions for preparation

Now is the time for the automotive industry and all commercial players that operate in the automotive ecosystem and are addressees of the Data Act standards to start a strategic compliance project. Even if the requirements will not predominantly take effect until the end of 2025/2026, initial precautions must already be taken now, taking into account various internal company development cycles. This includes the creation, review and adaptation of B2C and B2B contracts, including the General Terms and Conditions (GTC) for the provision and use of data in accordance with the requirements of the EU Data Act. It is not too early to develop an overall concept for compliance with the EU Data Act. This should include at least the following aspects:

- Technical interfaces for transferring data to users and recipients
- UX and backend adjustments
- All B2B and B2C contracts must be re-examined and adapted if necessary
- Data governance concept and workflow / approval schemes from data request to activation of access to the data.
- Possible mechanism for compliance with B2G data requests.

This is because it involves the development of a comprehensive, multi-layered and cross-functional compliance mechanism that is likely to require considerable investment and long-term planning. Its framework can only be briefly outlined here.

1. In order to meet the requirements of the EU Data Act, it is crucial for any car manufacturer or data holder to ensure cooperation between various departments in this context. At the very least, the project requires action and collaboration between IT and product, legal, business development, operations, sales and consumer-facing services.

with users, third parties and government agencies under certain conditions.

3. Once the use cases have been identified and the role of the company has been determined for each use case, the next step is to adapt the front and back-end components of products and services in such a way that a smooth and EU Data Act-compliant data transfer is possible. When the user triggers a request, the technical process should take into account the obligations and standards resulting from the role.

4. Compliance with the EU Data Act should be integrated into product development protocols at an early stage ("accessibility by design"). Technical adaptations such as system interfaces (API) with third-party providers or the creation of a function that enables users to request data in a specific format go hand in hand with the creation of a compliance and governance structure. This means that before data is passed on to external parties, it undergoes a standardized review process for data requests, which in certain aspects is similar to a data protection review and documentation.

5. In this process, a decision is made before execution as to whether a particular data request is approved and, if so, to what extent. It also determines which technical modalities apply to the execution of the request. As part of the data governance mechanisms, data holders define the function and responsibilities within the organization, including the role of the data manager, in addition to processes. Legal issues that may be associated with a particular request, such as data protection compliance in the case of personal data or the confidentiality of information in the case of trade secrets, must be clarified in advance.

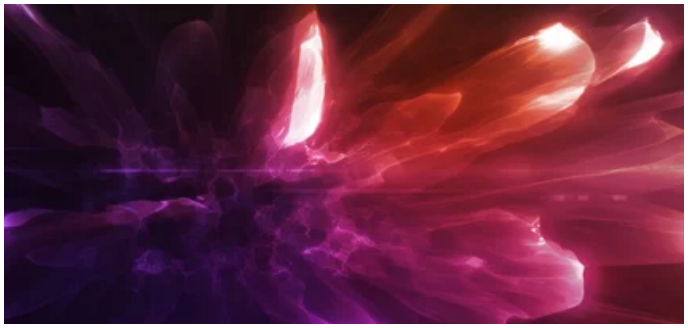
6. An important pillar of the compliance mechanism is the review and adaptation of the contracts that the OEM concludes with users and other parties. Among other things, the B2C contracts must comprehensively cover the use of the co-generated data by the OEM. Detailed B2B contracts with third parties (data recipients) on the transfer and use of data are equally essential.

7. In addition, OEMs should examine new business models in which data transfer can create new sources of income. It would also make sense to examine the extent

service portfolio and lead to a significant increase in competitiveness. The prohibition on developing competing products/services with such data must always be taken into account.

Contact us

RELATED ARTICLES



How data culture prepares you...

Explore the pillars of data-driven decision-making and the importance of effective data management.

Read insight

Data management: How...

Explore how decentralizing data management can enhance data quality and agility in companies, unlocking the full potential of data fo

Read insight

Offering

Success stories

About us

Career

Insights

DICONIUM

+49 711 2992 0

contact@diconium.com

Information requirements

Data protection

LkSG Compliance

Whistleblower System
