The EU Data Act Is Coming — Is Your Company Ready?

Compliance and Ethics

Government

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by Vector Image Plus / *Shutterstock.com*

When I first learned about the European Union Data Act (the "Data Act") in late 2023, it was described as "GDPR for the Internet of Things." However, as the Data Act's effective date of Sept. 12, 2025, draws nearer, greater focus and scrutiny of the Data Act has revealed that it might actually apply to a far broader set of companies and the data they collect.

What is certain is that the Data Act is one of a series of regulations put in place by the EU in recent years to make the EU a leader in the information economy, while balancing European values of individual protections and rights with a free-market economy. This article will help you, as an in-house attorney, determine whether the EU Data Act applies to your organization, what its implications are, and how to improve your compliance.

Why did the EU create the Data Act?

The EU created a monumental shift in how we think about personal information when it rolled out the General Data Protection Regulation (GDPR) in 2018. GDPR established the notion that data is the personal property of an individual (specifically, an EU citizen) and that the individual must be afforded certain rights and protections of their personal information, which is often used by companies providing tech-based services.

The adoption of the Data Act takes a similar tone by recognizing that data, beyond personal information, is a valuable commodity and that use of such data carries with it certain rights of the owner, and responsibilities by organizations using the data. Additionally, the Data Act reflects the EU's ambitions to boost the EU's data-based economy and to create a common market for that data.

The act was initially positioned to recognize the rise in volume of data being collected in devices connected to the internet, specifically referred to as "connected products." Companies providing services related to these connected products were harnessing the value of this data, both to provide better services for their customers, but also to enhance their own products and, ultimately, to find new uses of that data to increase their own innovation and competitive position.

Does it apply to my company?

The Data Act applies to "data holders" who are holding customer data in the EU market or who are making data available to data recipients in the EU. The intended target is manufacturers of connected products (i.e., IoT devices) and providers of "related services."

The potential broad application of "related services" may mean that companies not initially considered as needing to comply with the Data Act might find themselves under its purview after all. For example, a builder of industrial machine equipment or a connected car manufacturer clearly falls under the Data Act. Because of the broad interpretation of related services, however, a company that is hired to analyze performance of a manufacturing floor, or an internet service provider who allows a connected car to connect to services may fall under the regulations as well.

While there is no simple binary checklist, it is important to make a logical assessment of what products or services your company provides. One primary objective of the Data Act is to create fairness in the data economy and empower users to reap value from the data they generate using their connected products. If your company collects data or provides any value to customers through the use of their data, you might be subject to the Data Act.

Assuming the Data Act applies to my company, what are our responsibilities?

While your company's total obligations extend beyond the high-level nature of this article, there are a few areas you should immediately focus on.

Identify the universe of applicable data

If you believe that the types of products or services your company provides may be subject to the Data Act, the next step is to parse out *what* data applies. The Data Act states that it applies to "all raw and pre-processed data generated from the use of a connected product or a related service that is readily available to the data holder (e.g., manufacturer of a connected product/ provider of a related service)." Said differently, data that can be easily accessed without disproportionate effort is included. It is also worth noting that the raw data does not include a company's analytics. Any processing or manipulation of the data can remain with the company.

Additionally, although GDPR has its own set of regulations governing Personal Data, the EU Data Act regulations apply to personal as well as non-personal data. The Data Act defers to GDPR in the

event the two acts conflict, but personal data is specifically not excluded from the Data Act.

> If you believe your company may be subject to the Data Act, the next step is to parse out *what* data applies.

The Data Act does not affect rights and obligations under the GDPR and does not create any new legal basis for processing personal data. This means that the access rights described above require data holders to check whether personal data is involved and whether there is a legal basis for making available such personal data (e.g., if the requestor requests personal data of several users). Data holders must therefore identify which parts of the data qualify as personal data. Erring on the side of caution by treating data with uncertain status as personal data will cease to be an option.

Overall, aligning compliance with the GDPR and with the Data Act will be challenging given data protection authorities' restrictive interpretation of the GDPR and the principle of data minimization, which requires that no more personal data than necessary is processed. Businesses will therefore need to define a well-thought-out policy and consider appropriate options, especially data anonymization, which may be a complex, time-consuming and resource-intensive process.

Making data available

Ideally, connected products are designed so that data is accessible by default so that customers can directly access the data that is collected. However, this is not likely a built-in feature for most products and not a requirement of the Data Act. If direct access is not possible, the organization must make the data readily available to users.

Practically speaking, companies cannot make the process to obtain data unduly difficult to enforce and can't charge for providing a customer's data. For the sake of security and privacy, it is reasonable to require the customer to provide sufficient information to demonstrate that they have the right to access such data, but the company can't make this process overly burdensome.

> If direct access is not possible, the organization must make the data readily available to users.

Note that there are exceptions to what data must be given to the customer. For example, a company may withhold information if release of which undermined the security of the product. Likewise, if the collection of certain elements of information is somehow tied to a trade secret, the company may have a limited exclusion from providing some data back to the customer. Such limited scenarios are the exception rather than the rule, however.

Notification of data collected

Data collectors must provide written notice to their customers of what data is collected. Additionally, they are required to not discriminate in the types of data collected based on the customer.

Because such written notices are considered contractual terms between the data collector and its customer, the EU requires that the company use written notice terms that are not considered unfair. At a high level, the company should only collect data in alignment with commercial needs and good commercial practice. If terms are deemed to be unilateral and onerous, the burden will be on the

company collecting the data to demonstrate otherwise.

Data collectors must provide written notice to their customers of what data is collected.

How do I prepare?

Here are some best practices to implement if you think your organization is subject to the Data Act:

- **Conduct an initial assessment of customer data.** First and foremost, it is critical to get your arms around what data is being collected, how it is processed and who it is shared with. This initial baseline will help you determine the extent of your compliance obligations and may expose any vulnerabilities in your existing practices.
- **Create a data governance framework.** You should create a baseline of policies on how your company will handle data. This data governance model is a place to fall back to with a set of universal standards and, as long as it is followed, can protect in the event anyone challenges your compliance with EU regulations.
- **Host regular training and awareness programs.** Because building a governance model is only as good as it is used, you need to regularly educate employees about the EU Data Act requirements and the importance of following your organization's data governance practices.
- **Keep records.** It is critical that you maintain comprehensive records of your company's practices and compliance. In the event that you are audited or accused of noncompliance, these records will demonstrate adherence to your compliance with your governance framework.
- **Stay updated on regulations.** Because the Data Act is new, it will continue to evolve. Be sure to regularly review for updates and align your company's strategies with changes in the regulations.

Rob Keller

Senior Director and Associate General Counsel

Cisco Systems, Inc.

Rob Keller is a Senior Director and Associate General Counsel at Cisco Systems, Inc. where he leads the Product Legal Team responsible for the Campus, Branch, Industrial IoT and Collaboration Product Groups. His team advises on product-specific legal issues including compliance, IP ownership, and go-to-market matters.

Prior to joining Cisco, Rob was a Corporate and Securities Lawyer in the Silicon Valley firm Carr & Ferrell. He currently lives in Washington, DC.