LAW360

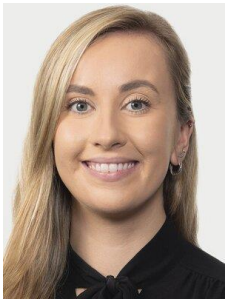
Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cos. Should Plan Now For Extensive EU Data Act Obligations

By **Nick Banasevic, Robert Spano and Ciara O'Gara** (February 1, 2024, 12:23 PM GMT)


Nick Banasevic


Robert Spano


Ciara O'Gara

The European Union Data Act entered into force on Jan. 11. With the goal of unlocking the EU's data economy, it imposes a set of wide-ranging data sharing, product design and contractual obligations on providers of so-called C devices and related services, and on cloud computing providers.

Internet of Things devices, or connected products, include all devices and equipment that collect data concerning their use or environment and that can then communicate such data through an electronic communications service, a physical connection, or on-device.

The obligations under the act apply to all sectors of the economy and to businesses of all sizes. Because of the act's extensive requirements, all companies should assess if any of their products or services are caught by the act.

The obligations under the act will start applying from the second half of 2025, so there is little time to prepare effective compliance strategies.

Overview

The act rests on the general assumption that the vast majority of data generated by connected devices, services and cloud software is unused, or collected by a handful of large companies.

Through this new legislation, the EU seeks to unlock this data, facilitate moving data between one service and another, and make it accessible to users — and also to third-party businesses if approved by the respective users.

The act will apply to the following:

- Manufacturers of connected products and providers of related services placed on the EU market;
- The users of such connected products or services in the EU;
- Data holders that make data available to recipients in the EU;

- Data recipients in the EU;
- Providers of data processing services offering services to customers in the EU; and
- EU institutions and public sector bodies.

The act will therefore also apply to foreign companies that operate in EU markets, irrespective of their place of establishment or subsidiary presence in the EU.

The act will affect companies of all sizes in almost every sector of the European economy, including manufacturers of smart consumer devices, cars, smart home appliances, connected industrial machinery, and any related services that interact with connected products such as streaming services or data analytics software.

Specifically, it will require availability and portability of data generated through the use of connected products or related services that connect to these devices.

The act will equally affect cloud computing providers, by introducing far-reaching obligations aimed at allowing users to easily switch between cloud service providers. It will also regulate smart contracts.

The act's provisions will begin to apply 20 months from Jan. 11, meaning affected businesses will need to be ready to comply by Sept. 12, 2025. Design requirements related to connected products will apply to products that are placed on the market in the EU after Sept. 12, 2026.

The act also introduces rules governing agreements relating to data access and use between companies and prohibiting unfair or abusive contractual terms. Where contracts are concluded after Sept. 12, 2025, these provisions will automatically apply. For contracts concluded on or before Sept. 12, 2025, these provisions will begin to apply from Sept. 12, 2027.[1]

Because of the act's extensive scope and range of obligations, it is imperative that businesses start preparing for compliance now. The act's implementation will require significant product changes and revision of contract terms.

For example, companies should start auditing their data storage policies and considering the changes required to implement the act's extensive data sharing requirements. Contracts governing data sharing and processing practices will also need to be reviewed and likely revised.

For some companies, the act will also open up novel business opportunities, and — as the rights under the act are not limited to small and midsized companies — large businesses will be empowered to benefit from this legislation and develop new business models based on third-party data becoming more accessible.

Internet of Things Devices and Services

The act creates a legal obligation to make data generated from connected products available to their users, to third parties if requested by the user, and to public sector bodies in circumstances where there is an exceptional need to do so.

The scope of affected products and services is very broad. For instance, B2B-connected products might include car braking systems, elevators, factory machines capable of collecting data, and smart solar

panels. In the B2C sphere, examples include smart fridges, smart speakers, cleaning robots, fitness trackers, medical devices, or modern cars.

However, products that are primarily designed to display or play content, or to record and transmit content, e.g., personal computers, servers or smartphones, are outside the scope of the act.

Obligations related to connected products also cover related digital services integrated with the product either at the time of purchase or subsequently.

Such services need to be essential for the product to perform its primary function and examples include voice assistants, music streaming services that connect to a smart speaker, command and control software for industrial machines, or software used for energy optimization in buildings.

Manufacturers of connected products are recognized as data holders in the act. Then, the regulation distinguishes between product data and related-service data.

Product data refers to data generated by the use of a connected product that is designed by the manufacturer to be retrievable by a user, data holder or a third party via an electronic communications service, a physical connection or on-device access. Related-service data needs to relate to the use of the device in question to be in scope.

Under the act, data holders will be obliged to design connected products in a manner that provides users with simple and secure access to the data generated by their use.

Access should be provided by default, or at the user's request, if direct access is not possible. Further, on the user's request, data holders must share data with third parties under fair, reasonable and non-discriminatory terms.

To incentivize the generation of valuable data, in B2B relations, data holders may request reasonable compensation when legally obliged to make data available to a data recipient.

During the act negotiations, balancing trade secret protection with data sharing was a key debate. As a general rule, trade secrets must be protected and only disclosed if the data holder and user take all necessary measures prior to disclosure to protect confidentiality.

The act recitals provide that the obligation to disclose data should be interpreted in such a manner as to preserve the protections afforded under the EU Trade Secrets Directive.[2]

Data holders should identify trade secrets prior to disclosure and should have the possibility to agree with users or third parties of user's choice on necessary measures to preserve their confidentiality.

If no agreement is reached or measures are not implemented, data sharing can be withheld. In exceptional circumstances and on a case-by-case basis, it may be possible for a data holder to refuse the request for access to data where it can be demonstrated that it faces a threat of serious economic damage due to the disclosure of trade secrets.

It further specifies that such damage "implies serious and irreparable economic loss," which is likely to be strictly interpreted. Moreover, the open-ended nature of the exception does not allow affected businesses to rely on a clear legal standard, and it remains to be seen how the exception will be

interpreted by the EU Court of Justice.

Gatekeepers

The act aims for SMEs and "enterprises from traditional sectors with less-developed digital capabilities" to be the primary beneficiaries of its provisions. On that basis, the act prevents companies that are designated as gatekeepers under the EU Digital Markets Act from being able to receive data, with the exception of their cloud services.

Cloud Switching

The act will have a significant impact on both public and private cloud computing services by requiring providers to facilitate switching across cloud and edge offerings.

Affected providers will be required to remove "obstacles to effect switching" between their own and competing cloud services, which can be commercial, technical, contractual and organizational, and they can no longer charge users for switching.

The act, however, states that affected providers are not required to develop new technologies or services, disclose digital assets protected by intellectual property or take measures compromising the integrity and security of their service.

The cloud switching obligations in the act leave scope for interpretation and the exact nature of their application is difficult to predict.

Additionally, given the complexity of cloud switching, especially for certain types of workloads, it remains to be seen how regulators will approach the implementation of this requirement in practice, given the apparently limited attention paid to the technical complexities when formulating vague and broad obligations.

In order to build a defense, it will likely be important for a company that faces significant technical hurdles to comply with the requirements under the act to develop strategies for the documentation of those hurdles and the efforts put into compliance.

Smart Contracts

One of the act's more controversial requirements concerns the design of smart contracts. The act defines them very broadly and does not distinguish between just digital contracts and smart contracts utilizing distributed ledger technology.[3] It may also potentially affect existing smart contracts on public blockchains.

Vendors of an application using smart contracts must ensure that smart contracts offer access control mechanisms and a "very high degree of robustness." They also need to ensure that smart contracts contain a kill switch, a mechanism that can either destroy the contract or pause its operation "to terminate the continued execution of transactions."

While the full extent of businesses affected by these requirements is difficult to ascertain, any provider of a smart contract application should carefully consider how to comply with the Data Act.

Interplay With GDPR

Unlike the EU General Data Protection Regulation, which applies to personal data only, the act has a broader scope encompassing both personal and nonpersonal data.

As clearly stated in article 1(5), the act is without prejudice to EU and national data protection laws, in particular the GDPR and the e-Privacy Directive.

This means that insofar as users are data subjects, all of the rights granted under the act complement the rights granted under the GDPR, such as the right of access and the right to data portability.

However, to ensure consistency with existing data protection laws, the act clearly provides that in the event of a conflict between the act and EU law on the protection of personal data and privacy, or national law adopted in accordance with such EU law, such EU or national law should prevail.

Enforcement

While the act introduces harmonized rules across the EU, it will be enforced by national authorities appointed by the member states. It leaves the determination of applicable penalties in the hands of member states, subject to some prescribed minimum requirements.

Penalties must be "effective, proportionate and dissuasive," and member states must notify their substance by Sept. 12, 2025 to the commission.

The commission will nevertheless support member states in their enforcement by adopting guidelines and implementing legislation on, for example, reasonable compensation for shared data, interoperability specifications, model contractual terms or harmonized smart contract standards.

For those reasons, companies should put in place a coordinated and centralized EU-wide compliance strategy.

Implications of the Act

The act is an extensive and highly complex piece of legislation that will have wide-ranging implications across industries and enterprises of all sizes.

Given the numerous exceptions, somewhat open-ended provisions and seemingly unclear definitions, a lot of uncertainty remains about how the act will be enforced in practice.

One thing is clear, however: Affected businesses should begin preparing their compliance strategies, and review their product designs and relevant contractual frameworks right away.

Nick Banasevic is a managing director at Gibson Dunn & Crutcher LLP.

Robert Spano is a partner and co-chair of the artificial intelligence practice group at the firm.

Ciara O'Gara is an associate attorney at the firm.

Gibson Dunn associate attorney Jan Przerwa contributed to this article.

[1] Provided they are of indefinite duration or due to expire at least 10 years from 11 January 2024.

[2] Trade Secrets Directive ((EU) 2016/943).

[3] I.e., computer programs used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering.