Hashed & Salted | A Privacy and Data Security Update
December 2022

EU Data Act

The European Commission unveiled its proposal of the much-anticipated EU Data Act in February. The Data Act, which is considered a key pillar of the EU's February 2020 Strategy for Data, is a sweeping proposal intended to "form the cornerstone of a strong, innovative and sovereign European digital economy," according to the commission's press release, sitting alongside the EU's Data Governance Act. A foundational aspect of the proposal is the notion that every actor that contributes to the generation of data should be able to freely access that data. The proposal touches upon both data protection and competition. The regulation seeks to unlock the untapped value of data across the EU and create a single market where data can flow across industry sectors in a harmonized, nondiscriminatory manner.

The proposal is a horizontal, sector-neutral regulation (but, notably, does not preclude implementation of sector-specific legislation) with rules governing who can use and access what data for what purposes across all economic sectors in the EU. It primarily targets products connected to the internet of things (IoT) and the various parties involved in the IoT chain. The regulation has broad, extraterritorial reach, applying to any IoT product and related services placed on the EU market.

Scope

The Data Act aims to regulate all "data." Data is defined very broadly as any digital representation of acts, facts or information (or their compilation) generated by the use of connected products and services that includes both personal and nonpersonal information.

The Data Act is likely to impose obligations and/or confer rights upon a broad range of stakeholders, in particular:

- Manufacturers of connected products placed on the market in the EU and providers of related services offered in the EU. "Related services" include any service incorporated or interconnected with an IoT product, the absence of which would prevent that product (e.g., software) from performing one of its functions.
- Users of such products and services (business users and consumers).
- "Data holders," i.e., enterprises having a "right or obligation" or the "ability" to make data available to data recipients in the EU, as well as these data recipients. The exact scope of the "data holder" definition is unclear, but it is intended to be very broad.
- Providers offering cloud services to customers in the EU.
- Public bodies in the EU that request data holders make available data where there are certain exceptional needs.

The proposed regulation does not apply to products with the primary function of storing and processing data (e.g., computers, phones, TVs), and it carves out large "gatekeeper entities" (as defined under the Digital Markets Act) from many rights under the legislation. There are also some exemptions for small and medium-sized enterprises (SMEs) and microenterprises.

Attorney Advertising

Key Obligations

Here are some of the Data Act's key rights and obligations:

- **Data access and sharing**
  - Akin to "privacy by design" requirements in data protection law, the proposal calls for data "access by design," requiring products to be designed and manufactured in a manner that enables access. Data must be made accessible to users of such product or service (including both individual and business users) easily and by default, securely and free of charge, and, where relevant, it must be directly accessible to the user. In some cases, data may need to be made available continuously and in real time.
  - On the same basis, data holders must make data (including continuous and real-time data) available to a third party (potentially a competitor) upon the request of the user. For example, a user may ask a manufacturer to share data with a third party to repair a connected product.
  - Further guidance is needed to clarify these requirements, such as the meaning of "direct" access, the breadth of in-scope data, and under what circumstances continuous and real-time data would need to be provided.
- **Protection of trade secrets and confidential information**
  - Companies subject to the act will need to consider how to protect commercially sensitive information, such as trade secrets, when sharing data with third parties. The law contemplates that data holders will share confidential information (and even trade secrets) with third parties where appropriate protective controls are in place. Recipient third parties are subject to various restrictions, such as purpose limitations, onward sharing limits, data deletion, noncompete/exclusivity requirements and data protection compliance.
- **Terms for data sharing**
  - The proposal establishes detailed rules for the terms and conditions for data holders to make data available if they are required to do so not only under the Data Act but also under any other subsequently adopted EU or member state legislation. Such terms must be fair, reasonable and nondiscriminatory, and the data holder bears the burden of proof for their nondiscriminatory nature. This will require IoT manufacturers and service providers to revise their standard agreements for granting third parties (e.g., developers of third-party applications interfacing with an IoT device) access to user data. The exact scope of these obligations will depend on the scope of future data-sharing legislation across the EU. The commission promises to develop model (nonbinding) contractual terms to help SMEs draft and negotiate fair data-sharing contracts.
- **Compensation for sharing data**
  - While users of IoT products and related services receive their data free of charge, data holders can require "reasonable" compensation from third-party data recipients for making the data available. Here also, compensation is subject to fair, nondiscriminatory and reasonable terms. For SMEs, it must not exceed the actual cost of making the data available.
- **Data access to public bodies**
  - The Data Act includes an obligation to provide certain data to public bodies in exceptional circumstances, such as in response to a public emergency (e.g., natural disasters, public health emergencies or terrorist attacks) or to fulfill legal obligations. Where information is necessary to respond to a public emergency, access to the data must be granted without undue delay and free of charge. In other situations, the data holder is entitled to compensation. SMEs are excluded from these data-sharing obligations.
- **Cloud services and other data processing services**
  - Switching: There are new rules on cloud and data processing services to help customers effectively

switch between services—including porting data, applications and other digital assets—without incurring any costs (although switching charges will be able to continue for three years after the act is in force). There are also rules concerning technical aspects of switching.

- International transfers or access to nonpersonal data: Subject to limited exceptions, adopting a similar stance as under the EU General Data Protection Regulation (GDPR), the Data Act requires providers of data processing services to put safeguards in place and take all reasonable technical, legal and organizational measures to prevent the international transfer of or governmental access to nonpersonal data held in the EU where such transfer or access would create a conflict with EU or relevant member state law.

Enforcement

- The commission's draft is designed as an EU regulation, meaning the Data Act would become directly applicable without a need for member states to transpose it into national law. The new provisions will be enforced by the individual EU member states, which will each be required to designate one or more responsible authorities. This approach is similar to that of the GDPR. Violations of the regulation will be sanctioned by administrative fines or financial penalties, also set at the national level. The EU Data Act also paves the way for new dispute settlement bodies to settle disputes about data sharing and access.
- The rules have extraterritorial effect and may be adopted as a global standard—similar to the GDPR. The Data Act joins a suite of regulations out of Europe that will impact the digital economy, including the Artificial Intelligent Act, the Digital Services Act and the Digital Markets Act.

Next steps

- Many aspects of the commission's draft are still unclear, e.g., its scope and details regarding its very broad, substantive obligations. The commission submitted its draft legislative proposal to the European Parliament and Council in February so the issues may be addressed in the upcoming legislative discussions, and amendments are expected. Adoption of the Data Act is anticipated by mid-2023, and the current proposal provides only a 12-month implementation period.
- It's a busy end of year for most companies pushing to address changes to U.S. privacy laws as well as their other year-end goals. When everyone is back in January, companies should consider whether they are in scope of the Data Act, understand how its requirements may affect their product road map and other business objectives, and start to create a strategy and timeline to address the technical and operational changes needed.

Related Professional

Ritu Narula . . . . . rnarula@loeb.com