AN A.S. PRATT PUBLICATION
JULY - AUGUST 2022
VOL. 8 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 6** **July - August 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [189] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The EU Data Act: Stimulant or Roadblock for the Data Economy?

By Andreas Grünwald, Hanno Timner, Christoph Nüßing and Philip Radlanski*

The authors discuss the significant impact of the European Commission's proposed EU Data Act on the European Union's data economy.

The European Commission has published its proposal for the EU Data Act,[1] a sweeping regulation which aims to provide a harmonized framework for data sharing, cloud switching, and international transfers of non-personal data, The Data Act is intended to "form the cornerstone of a strong, innovative and sovereign European digital economy" according to the Commission's press release.[2] One main idea behind the proposal is the notion that every actor that contributes to the generation of data should be able to freely access that data. As such, the proposal touches upon both data protection and competition aspects.

Once adopted, the Data Act will have significant impact on the data economy in the European Union ("EU"). It will primarily affect providers of connected products and related services as well as cloud providers, but it will potentially also concern any company that holds any data – personal and non-personal – as a result of offering its services in the EU. The Commission proposal will now be debated in EU Parliament and Council and can be expected to enter into force by mid-2024.

SCOPE

The Data Act aims to regulate all "data," which it defines as "any digital representation of acts, facts, or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording." This broad definition includes both personal and non-personal data.

* Andreas Grünwald is managing partner of Morrison & Foerster's office in Berlin and a member of the firm's worldwide board of directors. He heads the firm's German antitrust and regulatory practice from the firm's Berlin and Brussels offices. Hanno Timner, a partner in the firm's office in Berlin, advises clients on data protection matters and employment law issues and disputes. Christoph Nüßing, counsel in the firm's office in Berlin, advises clients on a broad range of regulatory questions. Philip Radlanski, a senior associate in the firm's office in Berlin, is a member of the firm's Global Privacy and Data Security Group. The authors may be contacted at agruenwald@mofo.com, htimner@mofo.com, cnuessing@mofo.com and pradlanski@mofo.com, respectively.

[1] https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data.

[2] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

The scope is similarly broad in terms of who the Data Act will affect because it is likely to impose obligations and/or confer rights upon a host of stakeholders, in particular:

- Manufacturers of connected products (e.g., Internet of things ("IoT") products) placed on the market in the EU, and providers of related services offered in the EU, as well as users of such products and services (business users and consumers). "Related services" include any service incorporated or interconnected with an IoT product, the absence of which would prevent that product from performing one of its functions.

- "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.

MAIN OBLIGATIONS

The proposed Data Act establishes a broad catalog of obligations for the different categories of stakeholders. On that basis, the Data Act can be expected to have a significant impact on the data economy across the EU. It may foster the inception of new IoT business models through easier access to IoT data. It contains provisions intended to facilitate switching between cloud services, which may increase competition among cloud providers and reduce any potential lock-in effects.

However, the Data Act's obligations will also entail a significant compliance burden for IoT manufacturers and service providers, cloud services, and other data holders – and particularly for those relying on international data access and transfers.

In particular:

- *Product design requirements*: Companies will need to design their IoT products and services so that users can easily access any data generated through their use. Certain information on the generation and use of data associated with any IoT product must be made available before the product is sold to EU customers. Data holders must not use personal data generated via IoT products and services without having a valid legal basis under general data protection laws (see below), and they must not use non-personal data without a contractual agreement with the user. The latter requirement in particular will require more effort from data-reliant businesses to ensure that they have a valid legal basis for their activities.

- *Data sharing obligations*: Upon request, data generated via IoT products and services must be made available to the user of the respective product or service without undue delay, free of charge, and (where applicable) in real-

time. Under the same conditions, the user may also request that "their" data are made available to any third party – but not to "gatekeepers" designated under the EU Digital Markets Acts (see below). This will require efforts from IoT manufacturers and service providers to establish new (or revisit existing) data sharing interfaces.

To protect the data holder's rights, data recipients must not make the data available to other third parties or use it to develop IoT products or services that compete with those of the original data holder. At the same time, data that is subject to trade secrets are only required to be disclosed under specific confidentiality arrangements (but the data must still be disclosed). It is unclear how compliance with these restrictions will need to be monitored. In practice, data holders will have limited means to prevent further uncontrolled sharing or use of data from their services.

- *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 non-discriminatory, and the data holder bears the burden of proof for their non-discriminatory nature. The same applies to any compensation paid to the data holder in exchange for the data sharing. The compensation to be paid by small and medium enterprises ("SMEs") must not exceed the costs of sharing the specific data. In addition, the proposal establishes a catalog of terms considered to be unfair in data sharing agreements – comparable to the rules already in place under general consumer contract laws. In the first instance, 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.

- *Cloud switching requirements*: The proposal establishes a suite of requirements designed to facilitate switching between different cloud services as well as the porting of all cloud services to an on-premise solution. These requirements will apply to a broad spectrum of cloud services, ranging from simple data storage services to highly customized software-as-a-service solutions. They include contractual safeguards, a limitation to the duration of switching processes to 30 days, the gradual elimination of any switching charges, and obligations to ensure functional equivalence between originating and retrieving cloud services. These requirements apparently borrow from the provider-switching regime under EU electronic communications laws and could require significant investments in interfaces and processes from cloud service providers even

considering that the Commission is tasked with developing open standards for cloud interoperability.

- *Restrictions on international data transfers*: Finally, the proposal includes severe restrictions on international data sharing by cloud services. Cloud providers must take all measures necessary to prevent any international access or transfer of non-personal data held in the EU that would be contrary to EU or Member State laws, e.g., in light of rules protecting the fundamental rights of an individual, the national security interests of a Member State, or intellectual property rights. Third-country data access requests are only permitted if based on international agreements or if the third country's legal system affords protections that are similar to the Data Act. These restrictions could affect existing cloud data flows between the EU and third countries as well as affect EU opportunities for new cloud-based businesses from third countries such as the United States or the UK. In particular, these rules appear to be stricter than the requirements for the transfer of personal data as outlined by the European Data Protection Board ("EDPB") following the *Schrems II* decision[3] by the European Court of Justice. While the EDPB has issued guidance[4] for an impact assessment regarding the transfer of personal data, the Data Act appears to leave no room for either such an assessment or for respective supplementary measures safeguarding data security, which are put in place by the data exporter.

Other areas that the proposal addresses are data access requests by public sector bodies across the EU, "smart contracts" in the context of data sharing, and the adoption of harmonized interoperability standards for data sharing. SMEs are exempted from certain of the above obligations.

ENFORCEMENT

The Commission draft is designed as an EU Regulation, i.e., 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 the EU General Data Protection Regulation ("GDPR"), for example, but different from the Digital Markets Act, where the Commission is intended as the sole enforcement authority.

---

[3] https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=186537.

[4] https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

Infringements will be sanctioned by "effective, proportionate, and dissuasive fines" – but without proposing any GDPR-style revenue-based penalties. The Data Act also foresees new dispute settlement bodies to solve disagreements about data sharing and access. In addition, many of the rights and obligations introduced by the Data Act will be subject to private enforcement before civil courts, and litigation can be expected, e.g., by customers trying to pursue the Data Act's new data access or cloud switching rights.

INTERPLAY WITH OTHER AREAS OF LAW

Based on its current catalog of obligations and requirements, the draft Data Act will particularly touch on data protection and competition laws:

- *Data protection*: Even though it extensively deals with access to and use of data, the Data Act is not privacy legislation. It leaves intact the rights and obligations under the GDPR which apply to personal data, and the Data Act should thus be read parallel to the GDPR. This means that all rights and obligations under the Data Act are to be understood without prejudice to the existing access and portability rights for individuals under the GDPR and any personal data shall only be made available under the Data Act where there is a valid legal basis under Article 6(1) GDPR, e.g., the individual's consent, a legitimate interest, or a contractual necessity.

  However, the Commission's proposal evidently borrowed extensively from the GDPR regarding many of the Data Act's key concepts: for example, the need to have a contractual agreement that justifies the use of non-personal data resembles the GDPR's notion of requiring a valid legal basis for any processing of personal data. The provisions on switching cloud providers closely resemble the GDPR rules on data portability. Similarly, the proposal's restrictions on international transfers of non-personal data are apparently modeled after the ones that apply to transfers of personal data under the GDPR. It is highly questionable whether such more or less direct transpositions of existing data protection rules to the realm of non-personal data are actually justified.

- *Competition*: The Data Act will apply in addition to any data-related obligations under existing and/or upcoming competition laws, such as the EU Digital Markets Act, that is expected to enter into force in the course of 2022 and which will impose certain data access and portability obligations on large companies that provide core platform services (e.g., social networks, online marketplaces, or search engines) and have been designated as "gatekeepers" by the EU Commission. For the Data Act, the Commission proposes that such gatekeepers can never be eligible data recipients and therefore must not receive any data shared under the Data Act.

> Data access and portability obligations can also be imposed upon companies designated as "undertakings with paramount significance for competition across markets" ("UPSCAM"), and they apply to dominant companies or to those with relative market power under the revised German competition law. Unlike these competition-specific obligations, the obligations under the Data Act will apply regardless of the competitive relationship between the data holder and recipient.

Beyond that, the proposed Data Act does not seem to interfere with other legal positions regarding in-scope data in terms of intellectual property rights or trade secrets.

NEXT STEPS

Many aspects of the Commission's draft are still unclear, e.g., its specific scope and details regarding its substantive obligations. These issues will now be addressed in the upcoming legislative discussion in the other EU bodies, i.e., the European Parliament and the EU Council, which will kick off as of today. Both can be expected to come up with their proposed amendments to the Commission's draft by late 2022 or early 2023. The three EU bodies will then enter into "trilogue" discussions to find a political compromise and to eventually adopt the Data Act by mid-2023. Per the implementation period as currently suggested by the Commission, it will then become binding for all in-scope companies within 12 months.

At the same time, the Commission's draft will likely put Member State initiatives for national "Data Acts" on hold or at least significantly limit their scope. For example, the new German government had planned to introduce its own statute to strengthen the access of anyone involved in the generation of data to their data. It remains to be seen what will happen with these plans.