AN A.S. PRATT PUBLICATION
FEBRUARY/MARCH 2019
VOL. 5 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 NUMBER 2 FEBRUARY/MARCH 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@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*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [37] (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

(2019–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, 646.539.8300. 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.

New EU Regulation to Strengthen the Free Movement of Data

Kristina Ehle and Stephan Kress*

This article examines the European Union's plans and considers the potentially confusing interplay between regulations, which cover non-personal data, and the regime on personal data introduced by the General Data Protection Regulation.

The European Union is close to finalizing a new regulation on the free flow of non-personal data within the EU. This is part of an EU goal to remove technical and legislative barriers to open data flows, including data location restrictions which force service providers to build expensive local infrastructures in each region or country. The EU wants to make it easier to move, share, and re-use non-personal data across global markets and borders.

This article examines the EU's plans and considers the potentially confusing interplay between these regulations, which cover *non-personal data*, and the EU's regime on *personal data* introduced by the General Data Protection Regulation ("GDPR") in May 2018.

The European Commission launched its Digital Single Market ("DSM") strategy in May 2015.[1] The DSM strategy consists of three "pillars" and 16 "Key Actions."

---

* Kristina Ehle, a partner of Morrison & Foerster (International) LLP and co-managing partner of the firm's Berlin office, focuses her practice on advising German and international clients in the media, information technology, e/m-commerce, consumer electronics and products as well as clean technology industries on commercial transactions, intellectual property issues as well as IT, internet, consumer rights and commercial law matters. Stephan Kress is a senior associate at the firm's office in Berlin advising German and international clients with regard to drafting and negotiating technology-related agreements and matters concerning cloud computing, software, e/m-commerce, digital media, intellectual property rights, consumer rights, electronic communication, big data and cyber security requirements. The authors may be reached at kehle@mofo.com and skress@mofo.com, respectively.

[1] For information about the DSM's progress, *see*,

- Inception: https://media2.mofo.com/documents/150514eudigitalsinglemarket.pdf;
- One year in: https://media2.mofo.com/documents/160808digitalsinglemarketstrategy.pdf; and
- In 2017 following a mid-term review: https://www.mofo.com/resources/publications/170608-eu-digital-market-strategy.html.

See also,

- 2018 EU Work Programme: https://www.mofo.com/resources/publications/180109-regulatory-changes-europe.html;
- Key Action 1 – Regulating Cross-Border E-Commerce: https://www.mofo.com/resources/publications/180118-european-e-commerce-reforms.html;
- Key Action 2 – Enforcing Consumer Protection Rules: https://www.mofo.com/resources/publications/180202-eu-new-consumer-protection.html;
- Key Action 3 – Cross-Border Parcel Delivery: https://www.mofo.com/resources/publications/180208-eu-cross-border-parcel-delivery.html;

BACKGROUND

Data-reliant technologies play an increasingly large role in Europe's economy and, as a result, facilitation of the free movement of data across the EU has become a vital policy area. In terms of personal data, the implementation of the General Data Protection Regulation in 2018 resulted in far-reaching obligations for companies in the EU that collect, use or otherwise process *personal* data.

The Commission has now turned its attention to *non-personal* data, and committed itself to removing national restrictions on data flow in the hope that this will stimulate growth and establish European companies at the forefront of developing and exploiting digital technology – especially in the fields of automation, robotics, the Internet of Things ("IoT"), sustainable manufacturing and artificial intelligence.

Key Action 14 in the DSM involves creating a free-flow-of-data initiative. The European Commission believes that the fragmented nature of EU rules, as well as national obligations imposed by some Member States, is a barrier to the full adoption of new technology trends across the EU. To benefit fully from the potential of digital and data-reliant technologies, the EU plans to remove a series of technical and legislative barriers. The European free-flow-of-data initiative is intended to tackle restrictions on the free movement of data for reasons other than the protection of personal data within the EU, and eliminate unjustified restrictions on the location of data for storage or processing purposes.

In June 2018, the EU legislative institutions announced that they had reached agreement on a framework for the free flow of non-personal data in the European Union

---

- Key Action 4 – Ending Geo-Blocking: https://www.mofo.com/resources/publications/180308-eu-regulation-geo-blocking.html;
- Key Action 5 – European E-Commerce Markets: Competition Initiatives: https://www.mofo.com/resources/publications/180315-european-e-commerce-markets.html;
- Key Action 6 – European Copyright Reform Status Update: https://www.mofo.com/resources/publications/180423-eu-copyright-reform.html;
- Key Action 7 – EU Changes to TV and Radio Transmission Rules: https://www.mofo.com/resources/publications/180417-eu-tv-and-radio-transmission-rules.html;
- Key Action 8 – VAT Reform and Digital Goods and Services: https://www.mofo.com/resources/publications/180510-eu-digital-market-vat-reform.html;
- Key Action 9 – Electronic Communications Code: https://www.mofo.com/resources/publications/180508-european-electronic-communications-code.html;
- Key Action 10 – Audiovisual Media Services Directive: https://www.mofo.com/resources/publications/180709-digital-single-market-update.html;
- Key Action 11 – Illegal Content and Disinformation Online: https://www.mofo.com/resources/publications/180730-eu-illegal-content-disinformation-online.pdf?#zoom=100; and
- Key Action 15 – Technology Standardization in the EU: https://www.mofo.com/resources/publications/181022-digital-single-market-update.html?utm_source=publications&utm_medium=email.

(the "Draft Regulation"). After its formal adoption, the Draft Regulation will become directly applicable law in all EU Member States six months after its official publication.

TOP TAKEAWAYS

1) The proposal would improve data mobility across borders by eliminating any national requirements to keep data within a particular country, and make it easier for users of data storage services to port data to different service providers.
2) It is questionable whether the Draft Regulation will actually produce the vast economic and other benefits claimed by the EU lawmakers. While the most likely direct effect will be the reduction of national data localization requirements imposed by Member States, this is only one of the obstacles to the free movement of data (and the actual economic effect of this single factor remains unclear). The Draft Regulation does not address many other important legal issues regarding the sharing of non-personal data, such as questions regarding data ownership or liability in an increasingly collaborative digital economy.
3) The "vendor lock-in" effect, which was identified as another significant obstacle to the free movement of data, is addressed by the Draft Regulation. But it is dealt with in restrained fashion, through the concept of self-regulatory codes of conduct for providers of data processing services. So providers offering data processing services in the EU might want to participate in the standard-setting process of developing self-regulatory codes of conduct as envisaged by the Draft Regulation.
4) Data owners will need to pay attention to the guidance to be published by the Commission with regard to the interplay between the Draft Regulation and the GDPR, especially with regard to their application to mixed data sets.

BACKGROUND OF THE NEW REGULATION

In regulatory terms, when hearing the term "data" most people immediately think of "personal data" and, for example, how businesses can comply with the rules on the collection, processing and transfer of personal data under the GDPR, fearing the application of high penalties should they fail to do so. However, a large volume of the data upon which the worldwide data economy is built is non-personal data – such as machine data, environmental data, product and materials data, traffic data, infrastructure data and, of course, aggregated and anonymized usage data.

The digital transformation of industries in recent years, providing new technology and software with which to track and store data more efficiently, scalable storage space (in particular as result of cloud computing), and Internet access everywhere allow for the collection and processing of big data on an unprecedented scale. The number of

IoT connected devices is expected to increase from 20 billion in 2017 to almost 31 billion worldwide by 2020, further adding to the volumes of data processed.

The EU legislators intend the Draft Regulation, applicable to the processing of such non-personal data, to supplement the GDPR, so that together they form a comprehensive legal framework for the free flow of data of any kind throughout the EU. "Free flow of data" means unrestricted movement of data across borders and IT systems in the EU. The European parliament ("EP") considers free movement of data to be the "fifth freedom" in the single market, after the free movement of persons, goods, services, and capital.

The establishment of a framework for the free movement of data is aimed at facilitating the development of an affordable, innovative and internationally competitive European data economy as part of the DSM strategy. According to the Commission, the Draft Regulation could boost EU GDP by up to €8 billion per year by bringing down costs for data services and creating greater flexibility for companies.

Specifically, the Commission has identified four types of main obstacles to data mobility within the EU, which the Draft Regulation is specifically aiming to counter:

- *Data localization requirements* (requiring data to be stored within a certain Member State's jurisdiction) imposed by Member States' laws or administrative practices;
- The "*vendor lock-in*" effect, *i.e.*, obstacles (economic, contractual or otherwise) to movement of data between different service providers;
- The *lack of an overarching principle* in the current complex EU legal patchwork regarding the cross-border processing of non-personal data, causing legal uncertainty; and
- A *lack of trust* due to security risks (in particular, the risk of security breaches), causing a propensity of market players and the public sector to use localization as a default safe option.

MAIN AREAS OF REGULATION

The main changes proposed by the Draft Regulation are as follows:

- *Reduction of National Data Localization Requirements.* Article 4 requires that data localization requirements in the laws or administrative practices of Member States must be eliminated, unless they are proportionate and justified on grounds of public security (or based on existing EU law). Member States are obliged to repeal any prohibited data localization requirement within 24 months after the start of application of the Draft Regulation.

- *Cross-Border Access to Data by Competent Authorities*. Article 5 and Article 7 of the Draft Regulation establish a general cooperation procedure for the exchange of non-personal data between public authorities of different Member States in areas where no specific cooperation mechanism exists under EU law or international agreements. According to the Commission, this addresses the Member States' main motivation for imposing data localization requirements, namely the concern of not being able to enforce local laws because of data being stored outside the respective Member State's jurisdiction. Under the Draft Regulation, where a competent authority does not receive access to the data of a user of data processing services stored in a different Member State after requesting such access from the user, that competent authority may request assistance from such other Member States' authorities to obtain access to such data. The original requirement that a competent authority must first exhaust "all applicable means" to obtain access to the data itself before being able to submit the cooperation request has been removed from the Draft Regulation, as it would "unnecessarily prolong the process of obtaining legitimate access to the data in question."
- *Self-Regulatory Codes of Conduct to Facilitate Switching between Service Providers.* With regard to the facilitation of data portability and easier switching of service providers, the Draft Regulation applies a self-regulatory approach. Under Article 6, the Commission wants to "encourage and facilitate" the development of self-regulatory codes of conduct by providers. The Draft Regulation does not itself specify concrete minimum requirements but merely lists important key aspects that should be taken into account when developing the codes of conduct, such as (a) best practices for facilitating the switching of providers and porting data in a structured, commonly used and machine-readable format; and (b) minimum pre-contractual information requirements towards professional cloud users (not consumers) if such a user wants to switch to another provider or port data back to its own IT systems. The Draft Regulation sets out a timeframe of one year to develop these codes of conduct and to effectively implement them within 18 months after the publication of the Draft Regulation.
- *Transparency and Information Requirements.* The Draft Regulation provides publication and information obligations for both the Commission and the Member States. The Member States' single points of contact must provide users with general information on the Draft Regulation, including on the self-regulatory codes of conduct developed pursuant to it. Also, Member States must make the details of any national data localization requirement publicly available online via a national single information point, which they must keep up-to-date. The Commission will publish the links to such national

information points on its website, along with a regularly updated consolidated list and summary of all data localization requirements of the Member States.

SELECTED POINTS OF CRITICISM AND DISCUSSION

There are a few immediately obvious problem areas with the Draft Regulation.

- *Mixed Data Sets.* The Draft Regulation clearly separates the scope of the Draft Regulation (applicable only to non-personal data) from the scope of the GDPR (applicable to personal data). Many data sets, however, will contain both personal data and non-personal data ("mixed data sets"). With regard to such mixed data sets, the Draft Regulation provides that its rules only apply to the non-personal part of a data set. Although Recital 10 clarifies that the Draft Regulation does not impose an obligation to store the different types of data separately, the question is whether affected entities will ultimately be forced to do exactly that in order to be able to clearly distinguish between their respective applicable obligations.

Although it is one of the declared goals of the Draft Regulation to provide a coherent set of rules for the free movement of both types of data, such coherency remains elusive. Take the example of data portability: while the GDPR expressly stipulates a right for data portability under certain circumstances,[2] such right does not exist under the Draft Regulation but is left for the service providers to define as part of their self-regulatory code of conduct. Another example is the extent to which data localization is permitted. Under both the Draft Regulation and the GDPR, data localization requirements are in principle prohibited. However, where the GDPR does permit data localizations for reasons other than the protection of personal data (such as under taxation or accounting laws), the Draft Regulation only permits data localization if justified on grounds of public security (or based on existing EU law). So the possibilities for data localization of non-personal data seem more restrictive than those under the GDPR.

The problem is compounded with regard to mixed data sets where non-personal data and personal data are "inextricably linked" (*i.e.*, cannot be unbundled). While the Committee on the Internal Market and Consumer Protection ("IMCO") discussed amendments to the Commission's initial proposal for the new regulation (the "Commission's Proposal") whereby, in cases of such inextricable mixed data sets, only the GDPR should be applicable to the data set as a whole, the Draft Regulation merely states that, in these cases, the Draft Regulation "shall not prejudice the application" of the GDPR. This probably means that, with regard to mixed data sets where

[2] Article 20 GDPR.

non-personal data and personal data are inextricably linked, *both* sets of rules apply but, in cases of conflict, the rules of the GDPR will prevail over the rules of the Draft Regulation.

The problem of mixed data sets has been identified by the EU legislators as a significant point of legal uncertainty. So the Draft Regulation provides that the Commission shall, within six months of the publication of the Draft Regulation in the *Official Journal*, publish "informative guidance" on the interplay between the Draft Regulation and the GDPR, especially with regard to mixed data sets, in order to enable companies to comply with both relevant regulations.

- *Codes of Conduct.* The self-regulatory approach for the facilitation of data portability and easier switching of service providers through the development of codes of conduct has faced criticism that it is ineffective. One influential EU committee suggested the need to provide at least a series of basic contractual rules, and a "blacklist" of prohibited clauses or guidelines for drafting the codes of conduct. IMCO went even further, explicitly suggesting an express right to data portability. At first, the Commission also wanted to create an explicit right on data portability; however, after two negative opinions from the Regulatory Scrutiny Board ("RSB") criticizing the insufficient evidence to justify such an explicit right, the Commission opted for the self-regulatory solution. The Draft Regulation also does not stipulate any legal consequences for non-compliance with the obligation to develop codes of conduct – so one wonders what practical effect the self-regulatory solution will actually have.
- *Lack of Safeguards Regarding Cross-Border Data Access Requests.* With regard to cross-border data access requests between authorities of different Member States, the Draft Regulation remains fairly vague. It simply states that the administrative cooperation mechanism can be invoked as soon as a competent authority "does not receive access to data" and that no specific cooperation mechanisms under EU law or international agreements exist. For example, no rules for the treatment of business secrets are specified. The Commission has also been criticized because the Draft Regulation is silent as to how the rule of law and fundamental rights established under the EU Charter of Fundamental Rights have to be respected during the cooperation process. The only substantive requirement established in the Commission's Proposal (namely, a Member State's right to refuse to cooperate with competent authorities where it would be "contrary to their public order") was removed from the Draft Regulation. While the Draft Regulation provides that the request for access must include a written explanation by the requesting authority as to its justification and legal basis for seeking access to the data, it is unclear to what extent and in what detail the authority receiving the cooperation request has to review the written explanation.

- *Security Requirements.* Despite the declared objective of reducing the propensity of market players and Member States using data localization as a practical measure for data security by enhancing trust in the security of cross-border data processing, the Draft Regulation does not contain any specific regulations on security requirements. Recitals 25 through 27 merely clarify that the respective existing legal patchwork of EU and national law should continue to apply.