AN A.S. PRATT PUBLICATION
OCTOBER 2017
VOL. 3 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 8 | OCTOBER 2017

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [272] (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

(2017–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, 718.224.2258. 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.

Germany Enacts GDPR Implementation Bill

By Hanno Timner and Jens Wollesen*

Germany has approved a law implementing the General Data Protection Regulation ("GDPR"). The new Federal Data Protection Act will repeal the current Federal Data Protection Act on May 25, 2018, when the GDPR enters into force. The authors of this article explain the new Act.

Germany is the first Member State in the EU to approve a law implementing the General Data Protection Regulation ("GDPR") into national law. Germany's Federal Assembly ("Bundesrat") cleared the new Federal Data Protection Act ("New Act") on May 12, 2017.

The New Act will repeal the current Federal Data Protection Act ("FDPA") on May 25, 2018, when the GDPR enters into force. Companies that fall within the New Act's scope (see below) will therefore not only have to comply with the GDPR but also with the New Act.

THE GDPR'S HARMONIZATION IS NOT ALL-ENCOMPASSING

The GDPR will enter into force across the European Union on May 25, 2018, and it will replace and harmonize the national data protection laws of the 28 EU Member States. There are, however, a number of areas in the GDPR where Member States may add their own rules (e.g., processing in the employment context and processing of sensitive personal information), so local requirements may vary.

THERE WILL BE A TIERED APPROACH WHERE THE NEW ACT COMPLEMENTS THE GDPR

The German New Act is meant to repeal and replace the FDPA in its entirety. A large portion of the GDPR's material provisions takes effect directly and do not require any implementation. Such provisions are therefore not included in the New Act. Rather, the focus is on the areas that require, or offer the possibility of, further regulation by the national legislation.

* Hanno Timner is the co-managing partner of Morrison & Foerster LLP's Berlin office, head of the Employment and Labor practice group in Germany and a member of the Privacy & Data Security Practice Group, advising and representing national and international employers in all labor law issues and disputes. Jens Wollesen is an associate in the firm's Berlin office and a member of the Employment & Labor and Privacy & Data Security Practice Groups. The authors may be reached at htimner@mofo.com and jwollesen@mofo.com, respectively.

THE SCOPE OF THE NEW ACT MIRRORS THAT OF THE GDPR BUT ALSO DOES MORE

The New Act will apply to the processing of personal information:

- In the context of activities of an establishment of a controller or processor in Germany.
- If the controller or processor is not established in the EU or European Economic Area but offers goods or services to individuals in the EU or monitors their behavior. This is a broader application than would have been expected from a national implementation, as the New Act seems to apply also if goods or services are offered or behavior is monitored in an EU Member State other than Germany. This aspect is not further addressed or explained in the legislative materials, and it may give rise to controversies in the future.
- If the controller or processor processes personal information in Germany. Here too, there is a departure from the principles of the GDPR (and from e.g., the draft Dutch GDPR implementation act), where the German New Act provides that if mere processing takes place in Germany—even if the controller or processor itself is established in another EU Member State—the German New Act needs to be complied with. The FDPA is explicitly not applicable if a controller located in another EU Member State processes personal information (unless carried out by a branch in Germany). A similar provision is missing from the German New Act. The German New Act may also act as a disincentive for non-EU companies to select service providers in Germany. As the New Act expressly applies to controllers processing personal information in Germany, the scope of the New Act is broader than the scope of the GDPR.

The above expansions as to the scope of application are noteworthy, as the GDPR has been intended to ensure harmonization of the European privacy regime and a prevention of an accumulation of different national regimes that apply. The expansion of application principles under the German New Act could very well end up having a contrary effect.

The New Act does not, however, deviate from the GDPR's rules on the (national) DPAs' authority to enforce privacy law. Thus, an Irish or Polish DPA could have authority to enforce the German New Act.

HIGHLIGHTS OF THE NEW ACT

- *Sensitive Personal Information*: Article 22 para. 1 of the New Act covers the cases in which the processing of sensitive personal information is permitted without having to obtain specific consent (provided the processing takes place within defined parameters). According to Article 22, this would be the case, for

example, for the assessment of the working capacity of an employee and for compliance with obligations under social security law.

- *Change of purpose*: The New Act allows a further processing of personal information (i.e., for a different purpose than for which the personal information was initially collected), if such further processing "is necessary to assert, pursue or defend civil law claims" of the controller (and the interests of the data subject do not override). The New Act supplements Art. 6 para. 4 GDPR, which provides criteria to be considered when deciding whether a secondary use of personal information is permitted. The New Act is more restrictive than the current FDPA, permitting further processing if necessary to safeguard any justified interests of the controller or processor and if such interests are not overridden by the interests of the individual.
- *Data Protection Officer*: Art. 38 of the New Act makes use of the ability under the GDPR to set specific thresholds under Member State law when the appointment of a DPO is required. There are a number of instances under the New Act when the appointment of a DPO is required:
  - when a controller or processor employs at least 10 people who are engaged in the processing of personal information on a regular basis (Art. 38 of the New Act).
  - When a controller or processor engages in high risk data processing for which a data protection impact assessment under Art. 35 GDPR is required.
  - When a controller or processor continuously engages in surveys for market research or opinion polling. A single survey or polling may require the appointment of a DPO if it is indicative of an intent to continuously engage in surveys or pollings.

The New Act provides for lower thresholds than the GDPR for the appointment of a DPO. The New Act does not require the appointment of a separate German DPO. Therefore, under Art. 37 para. 2 GDPR, a group of companies may appoint a single DPO, satisfying the requirements under the New Act.

- *Data processing in the employment context*: Art. 26 sets out specific requirements for the processing of data in the employment context and introduces (amongst other things) a test to establish whether employee consent can be considered to have been freely given (and therefore considered to be valid). The New Act provides that consent can be considered to have been freely given if it is sought for the provision of a legal or economic benefit to the employee, or where the employer and employee pursue "similar interests". The New Act's commentary sections provide examples of situations when this can be the case, such as with the introduction of a health management system or the use of company IT equipment. As an example of the "pursuit of similar interests," the commentary

refers to cases when employers circulate birthday lists and current photos of employees (supporting the communication among employees, thereby serving interests of the company and the employees). In conformity with the present FDPA, Art. 26 confirms that "collective agreements" with unions or works councils may serve as separate legal bases for the processing of employees' personal data. Art. 26 of the New Act makes use of the flexibility awarded to Member States around processing in the employment context under Art. 88 of the GDPR.

- *Information rights of individuals*: A previous version of the New Act restricted the information rights of individuals if honoring those rights is too burdensome on the company processing their information and the interest of the individual in obtaining information is relatively low. This provision had drawn criticism from DPAs and the Federal Assembly, as it would contravene the protective character of the information rights under the GDPR, and it has been deleted.
- *Sanctions*: In a previous draft, the New Act had capped penalties at EUR 300,000 for infringements (whereas the GDPR provides for maximum fines up to 20 million EUR or four percent of the worldwide annual turnover). In the final version of the New Act, the penalty cap has been deleted in response to criticism that this cap would effectively thwart the sanction regime under the GDPR. The current draft no longer provides for fines (with an exception for violations by consumer credit agencies), and therefore the sanction provisions of the GDPR apply also in Germany. In addition, however, the New Act imposes considerable criminal sanctions for violations of the New Act and increases the maximum prison sentence from two to three years (as compared to the FDPA). This sentence applies to anyone who knowingly, commercially and without authorization transfers personal information of "a large number of persons," which is not publicly available, to a third person or for making this information available in other ways. The term "commercially" denotes an intent to make a profit from repeated (illegal) data transfers. As a consequence, inadvertent data breaches would not be subject to criminal liability.

COMPREHENSIVE IMPLEMENTATION ACT MAY OBSTRUCT EFFECTIVE HARMONIZATION

It is clear that the New Act is much more comprehensive than the FDPA (by comparison, the FDPA has a total of 48 provisions versus 85 provisions in the draft New Act). German Data Protection Authorities already pointed out that the detailed provisions of the New Act may effectively get in the way of the harmonization effect of the GDPR. Lawmakers have addressed specific points of criticism, such as the previously extensive limitation of information rights, while leaving the overall structure

intact. The New Act's exemptions from the GDPR will, however, likely remain a potential source of conflict.

The original draft of the New Act is available on the webpage of the Federal Ministry of the Interior.[1] A consolidated version of the amended New Act has not yet been published.

[1] *See* http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-datenschutz-grundverordnung.pdf?__blob=publicationFile; Amendments of the legislative procedure are available at http://dipbt.bundestag.de/doc/btd/18/120/1812084.pdf (both documents in German only).