AN A.S. PRATT PUBLICATION
MAY 2018
VOL. 4 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 4 | MAY 2018

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*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [107] (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

(2018–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.

The GDPR Compliance Deadline Is Looming—Are You Prepared?

By Nicholas R. Merker and Deepali Doddi*

By May 25, 2018, all entities covered under the EU General Data Protection Regulation must be able to demonstrate their compliance to EU regulators. The authors of this article explain the regulation and suggest 10 key area of compliance.

The deadline for organizations to comply with the EU General Data Protection Regulation ("GDPR") is quickly approaching.[1] By May 25, 2018, all entities covered under the GDPR must be able to demonstrate their compliance to European Union ("EU") regulators. The failure to comply with the GDPR by this date may trigger steep administrative fines of up to €20 million or four percent of the organization's global annual revenue, whichever is greater. Notably, the GDPR does not apply solely to commercial businesses—not-for-profit organizations, charities, and educational institutions may all fall within the regulation's purview.

WHAT IS THE GDPR?

Put simply, the GDPR is a regulation requiring organizations that process the personal data of individuals in the European Economic Area ("EEA")[2] to institute strong data protection mechanisms, incorporate privacy principles into the design of business processes, and allow EEA individuals to exercise certain rights over their personal data. The GDPR replaces the EU Data Protection Directive,[3] which is currently in effect, and creates more robust requirements for protecting EEA personal data.

The GDPR also significantly expands the territorial scope of European data protection law. Even organizations in the United States will need to comply with the GDPR if they either offer goods or services to EEA individuals or monitor EEA individuals' behavior. *Accordingly, your organization may be required to comply with the GDPR even if it does not have a physical presence in Europe.*

---

* Nicholas R. Merker is a partner in and co-chair of Ice Miller LLP's Data Security and Privacy Practice. Deepali Doddi is an associate in the firm's Data Security and Privacy practice. The authors may be reached at nicholas.merker@icemiller.com and deepali.doddi@icemiller.com, respectively.

[1] General Data Protection Regulation (EU) 2016/679.

[2] The European Economic Area consists of European Union (EU) Member States and Iceland, Liechtenstein and Norway.

[3] EU Data Protection Directive 95/46/EC. Unlike the GDPR, the EU Data Protection Directive was not a regulation that was immediately legally binding on EU Member States. Instead, the Directive required each EU Member State to interpret the Directive's standards and pass national legislation to implement them.

WHO NEEDS TO COMPLY?

Consider the following examples of scenarios in which your organization may need to comply with the GDPR:

- Your company operates a website or mobile app that targets EEA users.
- You track and monitor the online behavior of EEA users of your company's website or mobile app.
- Your multinational company performs human resources activities for its employees and job applicants residing in the EEA.
- Your company's customer base includes businesses located in the EEA.
- Your organization receives charitable donations from EEA individuals.
- Your educational institution processes admissions applications submitted by prospective students currently residing in the EEA.

10 KEY COMPLIANCE AREAS

Because of the wide-reaching application of the GDPR, every organization should evaluate whether it has any GDPR compliance obligations. If you determine your organization is subject to the GDPR, we suggest focusing your initial compliance efforts in the following 10 key areas:

1) *Create a Data Map for Personal Data.* A deep understanding of how your organization creates, receives, maintains, or transmits personal data about EEA individuals is foundational to a GDPR compliance program. Additionally, it is important to ascertain whether your organization processes special categories of personal data, such as information about racial or ethnic origin; political opinions; religious beliefs; trade union membership; sex life or sexual orientation; medical or genetic information; or biometric data.
2) *Inventory Processing Activities.* The GDPR requires an organization to create detailed records of all of its processing activities. This step is not only necessary for demonstrating your organization's GDPR compliance to a regulator, but it is also helpful in identifying which of your practices and operations will need to be scrutinized for consistency with the GDPR's requirements.
3) *Assess the Scope of Your GDPR Compliance Obligations*. The extent of your GDPR obligations depends on whether your organization is best characterized as a "data controller" that determines the purposes for which processing activities are carried out or a "data processor" that handles personal data on behalf of a data controller. Sometimes, an organization may be both a controller and a processor. For instance, it may be a data controller to the extent it performs human resources functions for its EEA employees and a data processor with respect to personal data received from EEA customers.

4) *Identify Legal Bases for Processing Activities.* The GDPR enumerates several bases for the lawfulness of a processing activity. For example, a processing activity may be lawful if consent has been obtained from the individual data subject; the processing is necessary for the performance of a contract entered into with the data subject; the processing is necessary to comply with applicable legal requirements; or the processing is necessary for the organization's "legitimate interests." Your organization should be prepared to articulate a legal basis under the GDPR for each category of processing activities in which it engages.
5) *Implement Valid Consent Mechanisms.* The GDPR includes stringent requirements for obtaining an individual's consent to the processing of personal data. Your organization should carefully implement valid mechanisms to obtain individuals' consent to those processing activities involving special categories of personal data and for which you have identified consent as the legal basis. Along with consent mechanisms, your organization should ensure it provides meaningful notices to individuals of the purposes of its processing activities that satisfy GDPR requirements.
6) *Evaluate Processes for Protecting Individuals' Rights.* Under the GDPR, individuals have enhanced rights with respect to their personal data, including the rights to transparency, access, rectification and erasure, restrict processing, object to certain types of processing, and data portability. Your organization should decide how it will operationalize the GDPR's requirements for protecting individuals' rights over each category of personal data you process.
7) *Examine Vendor Relationships.* Whether your organization is functioning as a data controller or a data processor, the GDPR requires you to update relevant vendor contracts to impose specific data protection obligations on them. Further, data processors are required to obtain general or specific consent from the data controller to whom it is providing services before outsourcing any processing activities to vendors.
8) *Assess Data Security Practices.* Your organization should have a documented plan for complying with the GDPR's requirements for protecting the confidentiality, availability, and integrity of EEA personal data and the resilience of systems processing such data.
9) *Appoint a Data Protection Officer and/or a Europe-Based GDPR Representative.* Under some circumstances, the GDPR requires an organization to appoint a Data Protection Officer ("DPO"). A DPO must have expertise in data protection laws and can be either an external service provider or an employee of the organization, as long as the DPO does not experience a conflict of interests when performing his or her duties. The DPO would serve as the organization's point of contact for regulators and be responsible for various GDPR compliance efforts, including training staff, conducting audits, and advising on data protection impact assessments of proposed or existing processing activities.

Moreover, the GDPR requires organizations without a European establishment to appoint a GDPR representative based in the EEA.

10) *Develop an Internal GDPR Policy Manual.* Although not explicitly required by the GDPR, we recommend creating an internal GDPR Policy Manual that your organization can not only use as a foundation for employee training, but also produce to regulators to showcase your compliance. The manual may contain policies and procedures that address topics such as consent mechanisms; individuals' rights; vendor management; meeting the GDPR's strict breach notification requirements; when to perform data protection impact assessments; receiving and investigating privacy complaints; handling special categories of data; international transfers of personal data; data retention requirements; and the concepts of "privacy by design" and "privacy by default."