AN A.S. PRATT PUBLICATION
OCTOBER 2019
VOL. 5 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

EDITOR'S NOTE: MORE ON THE CCPA
Victoria Prussen Spears

COUNTDOWN TO THE CCPA: UPDATING YOUR PRIVACY POLICY
Catherine D. Meyer, James R. Franco, and Fusae Nara

CLEANING UP THE CCPA: UPDATES ON APPLICABILITY AND AMENDMENTS TO CALIFORNIA'S CONSUMER PRIVACY ACT
Cynthia J. Cole

STATE PRIVACY LAWS MAY GRANT AUTO EXCEPTIONS
Sarah L. Bruno, Eva J. Pulliam, and Casey Perrino

THE DASHBOARD ACT—PROPOSED NEW LAW WOULD FORCE LARGE TECHNOLOGY COMPANIES TO DISCLOSE THE VALUE OF USERS' DATA
Alexis Collins, Jane C. Rosen, and Natalie Farmer

EUROPEAN COMMISSION Q&A ON THE INTERPLAY BETWEEN THE CLINICAL TRIALS REGULATION AND GDPR
Ronan Tigner and Alex van der Wolk

THE GDPR: A CONTRACTING FLOWCHART
Lindsay R. Dailey

COOKIES, CONSENT, AND COMPLIANCE: ICO PUBLISHES NEW GUIDANCE
Paul Kavanagh and Madeleine White

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 8 | OCTOBER 2019

Editor's Note: More on the CCPA
Victoria Prussen Spears 245

Countdown to the CCPA: Updating Your Privacy Policy
Catherine D. Meyer, James R. Franco, and Fusae Nara 247

Cleaning Up the CCPA: Updates on Applicability and Amendments to California's Consumer Privacy Act
Cynthia J. Cole 252

State Privacy Laws May Grant Auto Exceptions
Sarah L. Bruno, Eva J. Pulliam, and Casey Perrino 257

The DASHBOARD Act—Proposed New Law Would Force Large Technology Companies to Disclose the Value of Users' Data
Alexis Collins, Jane C. Rosen, and Natalie Farmer 260

European Commission Q&A on the Interplay Between the Clinical Trials Regulation and GDPR
Ronan Tigner and Alex van der Wolk 264

The GDPR: A Contracting Flowchart
Lindsay R. Dailey 268

Cookies, Consent, and Compliance: ICO Publishes New Guidance
Paul Kavanagh and Madeleine White 270

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 [245] (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 inquiries 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.

The GDPR: A Contracting Flowchart

Lindsay R. Dailey*

The author offers a flowchart to identify several key issues under the General Data Protection Regulation.

The purpose of this flowchart is to identify when a Data Processing Agreement ("DPA") is required by the General Data Protection Regulation ("GDPR"), and then to determine the role that each party plays when providing the underlying services. Capitalized terms used in this Flowchart have the same meanings as those terms defined by the GDPR.

STEP #1: IS A DPA REQUIRED?

A DPA is required when all four components are present as outlined below.

Personal Data	• Name, email, health data, Social Security number, location or identification device • Political opinion, race, ethnicity, genetic or financial information
Data Subjects	• Patients, employees, applicants, health care providers • Located in the European Union/European Economic Area
Processing	• Collecting, recording, storing, retrieving, using, disclosure • Transmitting, erasing, destroying, aligning, combining
Controller & Processor	• Controllers determine the purposes for Processing Personal Data • Processors act on the instructions of the controller

A DPA is *not* required when Personal Data is not processed to perform the underlying services, or if both parties are Controllers.

* Lindsay R. Dailey is an associate and member of the Health Care Operations Practice at Polsinelli. She serves clients at the intersection of healthcare and data privacy compliance. Ms. Dailey counsels clients on HIPAA, GDPR, and other related international and domestic privacy laws. She may be contacted at ldailey@polsinelli.com.

STEP #2: WHO IS THE CONTROLLER VERSUS THE PROCESSOR?

Examine the underlying services and processing activities to determine each party's role.

Controller	Processor

• Alone or jointly with others, determines the purposes and means of the **Processing of Personal Data**.
• Carries out **Processing** activities such as interpretation, the exercise of professional judgment or significant decision-making in relation to **Personal Data**.
• If an entity is required by law to process **Personal Data**, it must retain its status as a **Data Controller** and assume responsibility for the **Processing**. For example, if Entity A hires a third party to fulfill its own legal obligations to its employees (such as hiring an external accountant to assist with calculating salary or hiring a vendor to do specific trainings for employees), Entity A is the **Data Controller**.
• If an entity makes decisions regarding **Personal Data** which demonstrate its overall control of the Processing, then that entity is likely the **Data Controller**. Some of these decisions may include:
  • To collect the **Personal Data** in the first place and the legal basis for doing so;
  • Which types of **Personal Data** to collect;
  • The purpose(s) the **Personal Data** is to be used for;
  • Who to collect **Personal Data** from;
  • Whether to disclose **Personal Data**, and if so, to whom;
  • Whether **Data Subject** access and other rights apply; and
  • How long to retain the data or whether to make non-routine amendments to **Personal Data**.
	• **Processes Personal Data** on behalf of a **Data Controller**.
	• Carries out **Processing** activities which are more limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure.
	• Typically only makes some decisions regarding **Personal Data** similar to the below items:
	  • What IT systems or other methods to use to collect **Personal Data**;
	  • How to store **Personal Data**;
	  • The detail of the security surrounding the **Personal Data**;
	  • The means used to transfer the **Personal Data** from one entity to another;
	  • The means used to retrieve **Personal Data**;
	  • The method for ensuring a retention schedule is adhered to; and
	  • The means used to delete or dispose of **Personal Data**.