

AN A.S. PRATT PUBLICATION

OCTOBER 2023

VOL. 9 NO. 8

PRATT'S  
**PRIVACY &  
CYBERSECURITY  
LAW**  
REPORT



LexisNexis

**EDITOR'S NOTE: THE DATA**

Victoria Prussen Spears

**GENERATIVE ARTIFICIAL INTELLIGENCE, DATA  
MINIMIZATION AND TODAY'S GOLD RUSH**

D. Reed Freeman Jr.

**POWER GRIDS AND POINTS OF VULNERABILITY:  
KEEPING THE LIGHTS ON AMID CYBERSECURITY  
CONCERNS**

Alicia M. McKnight and Brian E. Finch

**SECURITIES AND EXCHANGE COMMISSION  
ADOPTS NEW RULES ON CYBERSECURITY  
INCIDENT REPORTING AND DISCLOSURE FOR  
PUBLIC COMPANIES**

Adam Aderton, Daniel K. Alvarez,  
Elizabeth P. Gray, Laura E. Jehl,  
A. Kristina Littman, Nicholas Chanin,  
Erik Holmvik and Marc J. Lederer

**FAQS FOR BUSINESSES AS TEXAS PASSES  
CONSUMER PRIVACY LEGISLATION**

Risa B. Boerner and Brent Sedge

**SUPERIOR COURT OF CALIFORNIA PROHIBITS  
ENFORCING CALIFORNIA PRIVACY RIGHTS ACT  
REGULATIONS UNTIL MARCH 2024**

Peter A. Blenkinsop, Reed Abrahamson and  
Anya L. Gersoff

**META: COURT OF JUSTICE CONFIRMS THAT  
COMPETITION AUTHORITIES CAN ASSESS GDPR  
COMPLIANCE IN ABUSE OF DOMINANCE CASES**

Elena Chutrova and Ambroise Simon

**THE EUROPEAN COMMISSION ADOPTS ADEQUACY  
DECISION ON EU-U.S. DATA PRIVACY FRAMEWORK**

Huw Beverley-Smith, Charlotte H. N. Perowne and  
Jeanine E. Leahy

# Pratt's Privacy & Cybersecurity Law Report

---

VOLUME 9

NUMBER 8

October 2023

---

**Editor's Note: The Data**

Victoria Prussen Spears

257

**Generative Artificial Intelligence, Data Minimization and Today's  
Gold Rush**

D. Reed Freeman Jr.

259

**Power Grids and Points of Vulnerability: Keeping the Lights on Amid  
Cybersecurity Concerns**

Alicia M. McKnight and Brian E. Finch

265

**Securities and Exchange Commission Adopts New Rules on Cybersecurity  
Incident Reporting and Disclosure for Public Companies**

Adam Aderton, Daniel K. Alvarez, Elizabeth P. Gray, Laura E. Jehl,  
A. Kristina Littman, Nicholas Chanin, Erik Holmvik and Marc J. Lederer

271

**FAQs for Businesses as Texas Passes Consumer Privacy Legislation**

Risa B. Boerner and Brent Sedge

278

**Superior Court of California Prohibits Enforcing California Privacy Rights  
Act Regulations Until March 2024**

Peter A. Blenkinsop, Reed Abrahamson and Anya L. Gersoff

283

**Meta: Court of Justice Confirms That Competition Authorities Can Assess  
GDPR Compliance in Abuse of Dominance Cases**

Elena Chutrova and Ambroise Simon

285

**The European Commission Adopts Adequacy Decision on EU-U.S. Data  
Privacy Framework**

Huw Beverley-Smith, Charlotte H. N. Perowne and Jeanine E. Leahy

288

## 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

LexisNexis® Support Center ..... <https://supportcenter.lexisnexis.com/app/home/>

For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940

Outside the United States and Canada, please call ..... (518) 487-3385

---

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 [82] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2023 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

*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](http://www.lexisnexis.com)

MATTHEW  BENDER

(2023-Pub. 4939)

# *Editor-in-Chief, Editor & Board of Editors*

---

## **EDITOR-IN-CHIEF**

**STEVEN A. MEYEROWITZ**

*President, Meyerowitz Communications Inc.*

## **EDITOR**

**VICTORIA PRUSSEN SPEARS**

*Senior Vice President, Meyerowitz Communications Inc.*

## **BOARD OF EDITORS**

**EMILIO W. CIVIDANES**

*Partner, Venable LLP*

**CHRISTOPHER G. CWALINA**

*Partner, Holland & Knight LLP*

**RICHARD D. HARRIS**

*Partner, Day Pitney LLP*

**JAY D. KENISBERG**

*Senior Counsel, Rivkin Radler LLP*

**DAVID C. LASHWAY**

*Partner, Sidley Austin LLP*

**CRAIG A. NEWMAN**

*Partner, Patterson Belknap Webb & Tyler LLP*

**ALAN CHARLES RAUL**

*Partner, Sidley Austin LLP*

**RANDI SINGER**

*Partner, Weil, Gotshal & Manges LLP*

**JOHN P. TOMASZEWSKI**

*Senior Counsel, Seyfarth Shaw LLP*

**TODD G. VARE**

*Partner, Barnes & Thornburg LLP*

**THOMAS F. ZYCH**

*Partner, Thompson Hine*

---

*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. Copyright 2023 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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 European Commission Adopts Adequacy Decision on EU-U.S. Data Privacy Framework

*By Huw Beverley-Smith, Charlotte H.N. Perowne and Jeanine E. Leahy\**

*In this article, the authors discuss the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework.*

The European Commission has adopted its long-awaited adequacy decision for the EU-U.S. Data Privacy Framework (the DPF). With immediate effect, the adequacy decision provides a new lawful basis for transfers from the EU to the U.S. This means that companies that participate in the DPF are able to transfer data from the EU to the U.S. without relying on another data transfer mechanism, such as Standard Contractual Clauses (SCCs) or binding corporate rules (BCRs).

## BACKGROUND TO THE ADEQUACY DECISION

Pursuant to Article 45(3) of the GDPR, the European Commission has the power, by means of an adequacy decision, to decide that a non-EU country has sufficient standards of data protection to be treated as equivalent to those afforded in the EU.

In the case of *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18)* (Schrems II), the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield (the Privacy Shield), the predecessor to the DPF. The CJEU found that the surveillance of personal data by U.S. public authorities goes beyond what is strictly necessary, and therefore conflicts with the EU's principle of proportionality. Since Schrems II, the European Commission and the U.S. government have engaged in lengthy discussions on a new framework.

The U.S. Executive Order (EO) 14086 on Enhancing Safeguards for United States Signals Intelligence Activities in October 2022 introduced new binding safeguards relating to data accessed by U.S. intelligence agencies in order to address issues raised in Schrems II. For instance, it limits such access to that which is necessary and proportionate, and provides for an independent and impartial redress mechanism to handle and resolve complaints from Europeans concerning data collection for U.S. national security purposes. It is clear from the recitals to the adequacy decision, that (EO)14086 was significant in laying the foundations for the European Commission's decision.

---

\* Huw Beverley-Smith ([huw.beverley-smith@faegredrinker.com](mailto:huw.beverley-smith@faegredrinker.com)) is a partner in the London office of Faegre Drinker Biddle & Reath LLP. Charlotte H. N. Perowne ([charlotte.perowne@faegredrinker.com](mailto:charlotte.perowne@faegredrinker.com)) is an associate and Jeanine E. Leahy ([jeanine.leahy@faegredrinker.com](mailto:jeanine.leahy@faegredrinker.com)) is a trainee solicitor at the firm.

## THE DATA PRIVACY FRAMEWORK

The DPF introduces significant improvements compared with the mechanisms that existed under the Privacy Shield. Under Article 1 of the adequacy decision, it concludes that the U.S. ensures an adequate level of protection for personal data transferred to organizations that have committed to the EU-U.S. Data Privacy Framework Principles (the DPF Principles), and which are therefore included in the Data Privacy Framework List, which is maintained and made publicly available by the U.S. Department of Commerce.

The DPF introduces new binding safeguards to address the concerns raised by the CJEU, outlined below.

- Limits to ensure that access to data by U.S. intelligence authorities is restricted to what is necessary and proportionate to protect national security.
- Enhanced oversight of the activities of U.S. intelligence services by judicial and non-judicial bodies.
- The establishment of an independent and impartial redress mechanism, which includes the Data Protection Review Court (DPRC), to which EU individuals may submit complaints regarding an alleged violation of the new safeguards. The DPRC will investigate and resolve complaints, including the adoption of binding remedial measures such as ordering the deletion of the data.

U.S. companies may join the DPF by committing to comply with a detailed set of privacy obligations. For instance, they will be required to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties.

Transfers from the EU to the U.S. under the DPF will not require a Data Transfer Impact Assessment (DTIA) to be performed, unlike other transfer mechanisms. However, companies that continue to rely on SCCs and BCRs will still be able to invoke the DPF's safeguards in their DTIAs to justify their data flows to the U.S. Accordingly, in its press release the European Commission stated that the DPF safeguards will "facilitate transatlantic flows more generally."

## SELF-CERTIFICATION

The DPF is a self-certification program similar to its predecessors. Therefore U.S.-based companies which self-certified under the Privacy Shield and now want to rely on the DPF as a transfer mechanism must self-certify their adherence to the DPF Principles, including by updating their privacy policies to refer to the EU-U.S. Data Privacy Framework Principles by October 10, 2023. Such companies will automatically

be transitioned and may begin relying on the DPF immediately. A separate initial self-certification submission will not be required.

Companies that had self-certified with the Privacy Shield but do not wish to participate in the DPF will need to formally withdraw. Organizations wishing to rely on the UK Extension to the DPF may do so once the UK's adequacy regulations come into force. Similar mechanisms for Switzerland came into effect on July 17, 2023, following a parallel process for adequacy being undertaken by the Swiss Federal Administration.

## TAKEAWAYS AND NEXT STEPS

The adequacy decision entered into force with its adoption on July 10, 2023, along with the DPF Principles. The European Commission has confirmed that, alongside representatives of European data protection authorities and competent U.S. authorities, it will subject the DPF to periodic reviews.

It should be noted that the adequacy decision may still be subject to an invalidation procedure before the CJEU. We anticipate that it is likely that there will be legal challenges to the DPF similar to those brought against the Privacy Shield. For example, the privacy activist group NOYB (chaired by Max Schrems) has already confirmed<sup>1</sup> it will challenge the adequacy decision.

The adequacy decision is a welcome development for companies carrying out transatlantic personal data transfers. Such companies should now have greater certainty by relying on the DPF that they will not be at risk of fines, so long as the adequacy decision is not invalidated by the CJEU. Data importing companies in the U.S. that would like to benefit from the DPF should look to self-certifying and taking steps to comply with the DPF Principles.

---

<sup>1</sup> <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.