

AN A.S. PRATT PUBLICATION

OCTOBER 2026

VOL. 12 NO. 8

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



LexisNexis

EDITOR'S NOTE: PRIVACY IN THE STATES

Victoria Prussen Spears

**DELAWARE'S PRIVACY LAW IS ABOUT
TO EXPAND: 6 STEPS EMPLOYERS AND
BUSINESSES SHOULD TAKE TO PREPARE**

Vivian Isaboke

**OKLAHOMA ENACTS NATION'S TWENTIETH
STATE COMPREHENSIVE PRIVACY LAW**

Kirk J. Nahra, Ali A. Jessani and
Blythe Riggan

**ALABAMA ENACTS NATION'S TWENTY-FIRST
STATE COMPREHENSIVE PRIVACY LAW**

Kirk J. Nahra, Samuel Kane and Blythe Riggan

**NEW YORK STATE DEPARTMENT OF FINANCIAL
SERVICES RAMPS UP HEALTH CARE CYBERSECURITY
ENFORCEMENT WITH \$2.25 MILLION SETTLEMENT**

Jason Johnson and Linda Malek

**THE GOOD, THE BAD, AND THE UGLY: WHAT 7
RECENT COURT DECISIONS TELL YOU ABOUT
TODAY'S WEBSITE PRIVACY LIABILITY**

Usama Kahf

**CHARTING NEW WATERS: ENGLISH HIGH COURT
CONFINES EFFECT OF *THREE RIVERS (NO 5)*,
CONFIRMING PRIVILEGE CAN APPLY TO
INTRA-CLIENT COMMUNICATIONS**

James Norris-Jones and Tim Vogel

**COURT OF JUSTICE OF THE EUROPEAN UNION
RULES THAT A FIRST DATA SUBJECT ACCESS
REQUEST CAN BE REFUSED AS EXCESSIVE**

Huw Beverley-Smith, Charlotte H N Perowne
and James Ford

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12

NUMBER 8

October 2026

Editor's Note: Privacy in the States Victoria Prussen Spears	255
Delaware's Privacy Law Is About to Expand: 6 Steps Employers and Businesses Should Take to Prepare Vivian Isaboke	257
Oklahoma Enacts Nation's Twentieth State Comprehensive Privacy Law Kirk J. Nahra, Ali A. Jessani and Blythe Riggan	264
Alabama Enacts Nation's Twenty-First State Comprehensive Privacy Law Kirk J. Nahra, Samuel Kane and Blythe Riggan	268
New York State Department of Financial Services Ramps Up Health Care Cybersecurity Enforcement With \$2.25 Million Settlement Jason Johnson and Linda Malek	273
The Good, the Bad, and the Ugly: What 7 Recent Court Decisions Tell You About Today's Website Privacy Liability Usama Kahf	277
Charting New Waters: English High Court Confines Effect of <i>Three Rivers (No 5)</i>, Confirming Privilege Can Apply to Intra-Client Communications James Norris-Jones and Tim Vogel	283
Court of Justice of the European Union Rules That a First Data Subject Access Request Can Be Refused as Excessive Huw Beverley-Smith, Charlotte H N Perowne and James Ford	288

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@lexisnexus.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.lexisnexus.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*, [7] PRATT’S PRIVACY &
CYBERSECURITY LAW REPORT [179] (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 © 2026 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.lexisnexus.com

MATTHEW  BENDER

(2026–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 2026 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 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, 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 opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Court of Justice of the European Union Rules That a First Data Subject Access Request Can Be Refused as Excessive

*By Huw Beverley-Smith, Charlotte H N Perowne and James Ford**

In this article, the authors explain that, following a decision by the Court of Justice of the European Union, companies with operations in both the European Union and the United Kingdom should assess their data subject access request policies separately for each.

The Court of Justice of the European Union (CJEU or Court) has confirmed that a controller may refuse a data subject's very first access request under Article 15 GDPR as "excessive" where it can demonstrate, to a high evidential standard, that the request was made with abusive intent — for example in order to bring a compensation claim rather than to exercise a genuine right.¹ The ruling also clarifies that compensation under Article 82 GDPR is available for breaches of the right of access even absent any unlawful processing, but that the causal link to damages can be broken by the data subject's own conduct.

This judgment is binding across the EU, but is only treated as persuasive in the English courts. Companies with operations in both jurisdictions should assess their data subject access request (DSAR) policies separately for each.

BACKGROUND

In March 2023, TC, an individual resident in Austria, subscribed to the newsletter of Brillen Rottler, a family-run opticians practice based in Germany. He entered his personal data into the newsletter registration form on the company's website and consented to its processing. Thirteen days later, he submitted a DSAR under Article 15 GDPR, which grants data subjects the right to obtain confirmation of whether their personal data is being processed and, if so, access to that data.

Brillen Rottler refused the request, arguing it was abusive. In support, the company pointed to publicly available reports, blog articles, and legal newsletters indicating that TC followed a systematic pattern: subscribe to a company's newsletter, submit a DSAR, then claim compensation when the controller refused to comply. TC disputed this and claimed at least €1,000 in non-material damages under Article 82 GDPR for the

* Huw Beverley-Smith and Charlotte H N Perowne, attorneys with Faegre Drinker Biddle & Reath LLP, may be contacted at huw.beverley-smith@faegredrinker.com and charlotte.perowne@faegredrinker.com, respectively. James Ford, a trainee solicitor at the firm, may be contacted at james.ford@faegredrinker.com.

¹ Case C-526/24 Brillen Rottler GmbH & Co. KG v TC [2026].

refusal. Once proceedings were brought, the German court referred a series of questions to the CJEU.

ISSUE 1: CAN A FIRST DSAR BE REFUSED AS “EXCESSIVE”?

The CJEU confirmed that a data subject’s first access request may be refused as “excessive” within the meaning of Article 12(5) GDPR, provided the controller can demonstrate abusive intent. The Court reasoned that reference to “repetitive” requests in Article 12(5) is illustrative only, not a prerequisite. The decisive question is not how many requests have been made, but whether the request was made with an abusive purpose. The Court anchored this in the general EU law principle that EU rights cannot be invoked for abusive or fraudulent ends.

The Court was clear, however, that this exception must be interpreted restrictively and applies only exceptionally. The bar for controllers is deliberately high.

The Two-Part Test for Abusive Intent

To establish abusive intent, the controller must satisfy both limbs of a structured test:

1. *Objective element:* Despite the request formally satisfying the conditions of Article 15, the purpose of that provision (i.e., enabling the data subject to seek confirmation of the details of any processing of their personal data and verify the lawfulness of such processing) has not in fact been achieved.
2. *Subjective element:* The data subject made the request not for the purpose of finding out about any processing of their data in order to obtain protection for their rights under the GDPR, but in fact for some other abusive intention (for example, with the intention of obtaining compensation from the controller by artificially creating the conditions set out in the GDPR to give them a right to such compensation).

Critically, the Court required the controller to demonstrate abusive intent “unequivocally,” a demanding standard that goes beyond mere suspicion or circumstantial inference. The Court also emphasised that the burden of proof for demonstrating abusive intent lies with the controller.

Relevant Factors

In assessing whether abusive intent exists, the Court identified the following relevant (but non-exhaustive) circumstances:

- Whether personal data was provided on a voluntary basis, without any obligation to do so;
- The stated or objectively ascertainable purpose for which the data subject provided the data;

- The time elapsed between the provision of data and the submission of the data; and
- The overall conduct and history of the data subject, including any publicly available evidence of a pattern of systematic requests followed by compensation claims to multiple controllers.

On that last point, the Court confirmed that publicly available evidence such as reports, blogs, and legal newsletters documenting a data subject's pattern of behaviour may be taken into account, but only if corroborated by other relevant material.

ISSUE 2: COMPENSATION UNDER ARTICLE 82 GDPR

Compensation Is Available for Breaches of the Right of Access

The CJEU confirmed that Article 82(1) GDPR confers a right to compensation for damage resulting from a breach of the right of access under Article 15, even where that breach does not involve any act of unlawful data processing. Article 82(1) refers broadly to “an infringement of this Regulation” and is not restricted to processing-related violations. This is significant in that wrongful refusal to comply with a request, including one that seeks to rely on the *Brillen Rottler* defence without sufficient evidence, is independently exposed to a damages claim.

Conditions for Compensation

To obtain compensation under Article 82(1), the data subject must establish three cumulative conditions:

1. An infringement of the GDPR;
2. The existence of material or non-material damage actually suffered; and
3. A causal link between the infringement and the damage.

The data subject must therefore demonstrate actual damage distinct from the mere fact that a breach occurred. Loss of control over personal data and uncertainty as to whether data has been processed can in principle constitute non-material damage, but this must be proven on the specific facts.

Causation

The Court introduced an important causation defence for controllers. The causal link between a GDPR infringement and alleged damage may be broken by the data subject's own conduct, provided that the data subject's conduct is the determining cause of the damage. For example, where a data subject has deliberately shared personal data with a controller for the sole purpose of manufacturing a compensation claim (as alleged in the *Brillen Rottler* case), rather than for any genuine engagement, the causal chain between the controller's conduct and any alleged harm is severed, effectively foreclosing the serial litigant model.

THE DIGITAL OMNIBUS REGULATION: LEGISLATIVE CONTEXT

The *Brillen Rottler* judgment arrives during the EU legislative process for the European Commission's proposed Digital Omnibus Regulation. The draft proposal would amend the GDPR to expressly permit refusal of DSARs that abuse GDPR rights for purposes other than the protection of personal data. Recital 35 of the draft proposes that the evidential burden on controllers should be reduced to a "reasonable" standard, on the basis that abusive conduct is outside the controller's sphere of influence. This creates a tension with the CJEU's approach, which appears to impose a restrictive, evidence-heavy standard. Whether the text of the Omnibus Regulation will be amended to reflect the decision is not yet clear.

APPLICABILITY IN THE UK

The judgment is binding across EU member states but does not bind the English courts or the Information Commissioner's Office (ICO); although they may treat it as persuasive, particularly where the UK GDPR provisions in question are materially identical to their EU equivalent. The ICO's existing guidance on Article 12(5) continues to govern the UK position. Companies should assess their DSAR policies separately for EU and UK operations and should not assume that a defensible refusal in Germany will be similarly accepted by the ICO or an English court.

PRACTICAL STEPS FOR CONTROLLERS

Brillen Rottler is a meaningful development for organisations that handle high volumes of DSARs and have faced what appears to be systematic, compensation-driven activity. It confirms that the right of access, like all EU rights, cannot be exercised abusively.

The threshold for establishing abusive intent is high, however, and the exception will only apply in limited circumstances. Organisations should use this judgment as an opportunity to review and strengthen their DSAR workflows, rather than as an invitation to deny requests that are merely challenging. Some practical steps for businesses include:

- Updating DSAR intake processes;
- Documenting refusal decisions rigorously; and
- Reviewing policies separately for the UK and EU.

IN SUMMARY

- *Brillen Rottler* is a meaningful development for organisations that handle high volumes of DSARs and have faced what appears to be systematic, compensation-driven activity.
- Organisations should use this judgment as an opportunity to review and strengthen their DSAR workflows, rather than as an invitation to deny requests that are merely challenging.