AN A.S. PRATT PUBLICATION
OCTOBER 2026
VOL. 12 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT



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 255
Victoria Prussen Spears

Delaware's Privacy Law Is About to Expand: 6 Steps Employers and Businesses Should Take to Prepare 257
Vivian Isaboke

Oklahoma Enacts Nation's Twentieth State Comprehensive Privacy Law 264
Kirk J. Nahra, Ali A. Jessani and Blythe Riggan

Alabama Enacts Nation's Twenty-First State Comprehensive Privacy Law 268
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 273
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 277
Usama Kahf

Charting New Waters: English High Court Confines Effect of *Three Rivers (No 5)*, Confirming Privilege Can Apply to Intra-Client Communications 283
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 288
Huw Beverley-Smith, Charlotte H N Perowne and James Ford

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
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*, [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.lexisnexis.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 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 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.

Delaware's Privacy Law Is About to Expand: 6 Steps Employers and Businesses Should Take to Prepare

By Vivian Isaboke*

In this article, the author discusses a new Delaware law that, among other things, imposes significant new obligations on employers on the use of artificial intelligence in the workplace.

Just over a year after Delaware's privacy law took effect, state lawmakers have expanded its reach by passing a bill, House Bill 380,[1] covering more businesses, narrowing a key exemption, and expanding the definition of sensitive data. Most notably for employers, the legislation also imposes significant new obligations on the use of artificial intelligence (AI) in the workplace, capturing resume screeners, interview scoring tools, workforce analytics platforms, and similar technology. These amendments take effect on January 1, 2027.

This article discusses what businesses need to know about this law and six steps they should take to prepare.

KEY CHANGES

House Bill 380 amends Delaware's Personal Data Privacy Act (DPDPA), which passed in 2023 but took effect in 2025. Here is a list of the key changes that all employers and businesses should know about.

Applicability Thresholds and Expanded Scope

House Bill 380 substantially lowers the applicability thresholds related to data controlled or processed. A business conducting business in Delaware, or producing products or services targeted to Delaware residents, will be covered by the state privacy law if, during the preceding calendar year, it:

- Controlled or processed the personal data of at least 10,000 consumers (lowered from 35,000), excluding data processed solely to complete a payment transaction; or
- Controlled or processed the personal data of at least 5,000 consumers (lowered from 10,000) and derived more than 20% of its gross revenue from the sale of personal data.

* The author, an attorney with Fisher Phillips, may be contacted at visaboke@fisherphillips.com.

[1] https://legis.delaware.gov/BillDetail/143105.

House Bill 380 also adds a new applicability category for any third party that acquires personal data from a controller, with no numerical threshold. A vendor, service provider, data broker, advertising partner, or analytics provider that receives Delaware consumer data from a controller will be directly subject to the DPDPA regardless of size.

Narrower GLBA Exemption

The current DPDPA provides a full entity-level exemption for any financial institution or affiliate subject to Title V of Gramm-Leach Bliley Act (GLBA). House Bill 380 replaces that with a narrower framework where the exemption will be limited to:

- *Insurers*: Insurance companies and the agents, brokers, and administrators in the insurance business, including health insurers and the organizations that support them, plus their affiliates and subsidiaries, that are *principally*, rather than *directly*, engaged in financial activities as described in the GLBA.
- *Banks*: Federal or state-chartered banks, credit unions, savings associations, or their affiliates and subsidiaries that are directly engaged in financial activities as described under the GLBA.
- *Securities Firms*: Investment advisers and broker-dealers, along with their representatives and agents, that are regulated by the Delaware Investor Protection Unit or the Securities and Exchange Commission.

Accordingly, financial services providers that are not traditional banks or insurers, such as fintech companies, non-bank lenders, mortgage servicers, and payment processors, will need to reassess whether they still qualify for the entity-level GLBA exemption.

Healthcare and HIPAA Data Exclusions

House Bill 380 also adds several new data-level exclusions for healthcare information in addition to the DPDPA's existing treatment of HIPAA-covered entities and Protected Health Information. Specifically, the bill carves out information:

- Created for and maintained by a medical device manufacturer when collected, used, or disclosed for treatment, payment, or healthcare operations purposes under HIPAA;
- Created for purposes of the federal Health Care Quality Improvement Act;
- Derived from HIPAA-PHI, or from research data, once it has been stripped of identifiers to meet HIPAA's de-identification standards; and
- Included in a Limited Data Set under HIPAA, to the extent it is used, disclosed, and maintained as required.

As these are data-level exclusions rather than entity level exemptions, healthcare organizations, employers, and vendors will need to identify specifically which datasets fall within these exclusions and ensure the remaining data maintains DPDPA compliance.

Inclusion of Some Employment-Related Data

The DPDPA will continue to follow the majority approach taken by almost every other state by excluding individuals acting in an employment context from the definition of "consumer." California remains the only state where comprehensive consumer privacy law applies to employment data on the same terms as consumer data.

However, House Bill 380 carves out a narrow exception so that some types of automated decision-making will be covered by state privacy law. Specifically, rather than exempting employment data across the board as other state privacy laws do, the bill brings personal information of employees, applicants, and contractors within scope of the DPDPA whenever that data is used for profiling or to generate reports in connection with decisions producing legal or similarly significant effects.

In other words, employers using AI resume screeners, interview scoring tools, workforce analytics platforms, or vendors that generate a "report" used in hiring, promotion, discipline, or termination decisions will fall within the DPDPA's obligations.

Expanded Vendor Obligations and Fair Credit Reporting Act Safe Harbor

In relation to AI and automated decision-making, House Bill 380 introduces two new definitions, "report" and "decisions that produce legal or similarly significant effects."

- "Report" is defined broadly to include any written, oral, or other communication of personal data by a controller or processor, including recommendations, summaries, or automated decisions based on personal data or profiling.
- "Decisions that produce legal or similarly significant effects" is defined to include, among others, employment opportunities, housing, insurance, education, financial and lending services, criminal justice, healthcare services, and access to essential goods or services.

These definitions are particularly important because they trigger additional obligations for third-party processors beyond what state privacy laws currently require. Currently, third parties operate under the direction of the controllers on whose behalf they process data, with their compliance duties limited to operational requirements such as purpose limitation and security. House Bill 380 keeps that baseline but adds duties tied directly to residents. Specifically, the controller must contractually require the third party to:

- Provide the affected resident with notice of any adverse action taken based in whole or in part on the report;

- Describe the personal data relied upon in making the decision;
- Inform the resident of the right to obtain further information from the controller; and
- Inform the resident of the right to request a human review of the decision, where technically feasible and not contrary to the resident's best interest.

Controllers will also retain direct, ongoing obligations to residents. Upon request, a controller will have 30 days to provide a resident with the personal data the controller maintains about them, the source of the data used in profiling, and a list of all third parties that received a report about the resident within the past 24 months. The controller will also need to provide the resident with an opportunity to correct any inaccurate data.

These expanded vendor obligations, however, will not apply to activity already governed by the Fair Credit Reporting Act (FCRA). House Bill 380 provides a safe harbor where the report or personal data is a score, model, algorithm, or similar output that is a consumer report, or would be a consumer report if furnished to a third-party and is furnished or disclosed in compliance with the FCRA. Products and services regulated by the FCRA, such as background screening and credit scoring, therefore will be shielded from the new adverse action and human review obligations.

Data Protection Assessments

House Bill 380 lowers the mandatory Data Protection Assessment (DPA) threshold from 100,000 to 50,000 consumers and adds a standalone impact assessment requirement for profiling used in automated decisions producing legal or similarly significant effects, such as applicant screening or loan approvals. Controllers will need to document the assessment, including purpose, foreseeable risks of harm and mitigation steps, input and output data categories, performance metrics, transparency measures, and post-deployment monitoring.

Importantly, purchasing third-party AI tools does not transfer compliance responsibility. Deploying off-the-shelf software, such as an applicant tracking system that ranks or scores candidates, falls within the bill's definition of profiling. Controllers will not be able to rely on vendor compliance representations alone and will remain directly responsible for conducting the required impact assessments and ensuring the deployment meets House Bill 380's other obligations.

Expanded Definition of "Sensitive Data"

The "sensitive data" category is also expanded under the bill. The amended definition includes:

- Inferences based on personal data that reveal or identify sensitive characteristics, alone or in combination with other data;

- National origin, pregnancy, treatment status, status as transgender or nonbinary, citizenship status, and immigration status (in addition to the existing categories of racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, and sexual orientation);
- Neural data generated by measuring activity of the central nervous system;
- Financial data, including account numbers, financial account login information, and credit or debit card numbers that, alone or with a required access or security code, password, or credential, would allow access to a financial account; and
- Government-issued identification numbers, including Social Security, passport, state ID, and driver's license numbers, unless applicable law requires public display.

Processing sensitive data generally requires consumer consent and must be reasonably necessary and proportionate to the disclosed purpose. The inclusion of inferences as sensitive data will largely impact employers using workforce analytics, because outputs such as performance scores, productivity measures, and predictions about who is likely to be promoted or hired can be regulated as sensitive data even when the underlying inputs are not.

In practice, this means employers will need to obtain consent before generating or using these outputs on Delaware-resident employees and applicants. Businesses should update vendor contracts with HRIS providers, performance management platforms, talent analytics vendors, and AI hiring tools accordingly, particularly where these providers generate inferences about employees or candidates that businesses may not have previously classified as sensitive.

Disclosure Requirements for Sensitive Data

House Bill 380 also imposes specific conditions before a controller may disclose sensitive data in a sale of personal data. All of the following must apply:

- The disclosure must be strictly necessary to provide or maintain a product or service the consumer affirmatively requested; the controller must give clear and conspicuous notice before the sale that identifies the specific categories of sensitive data, the purpose of the disclosure, and the third parties that will receive it;
- The controller must obtain the consumer's consent, and the controller must keep a record of that consent for five years; and
- The consent records for consumers must be provided with any data protection assessment.

As such, organizations that sell sensitive data will need to capture consent at the point of sale and retain those consent records for five years, in addition to pairing them with the relevant data protection assessment.

Defending Employment Decisions Based on Profiling

Employers deploying AI in hiring, promotion, compensation, performance evaluation, or termination decisions must be prepared to show that their profiling systems have been tested for bias and that the testing is current, methodologically sound, and documented, including how the employer responded to the results. The bill adds new evidentiary language making proactive anti-bias testing (and the lack of it) statutorily relevant in any discrimination claim under Delaware law involving profiling.

Consequently, employers that cannot demonstrate disciplined testing and a documented response will face a harder time defending the resulting employment decisions in court. That's because plaintiffs may point to the absence of testing as evidence of discrimination, while the defense benefit of testing is only available where the program actually exists and meets the statutory criteria. The provision does not create a new cause of action, but raises the bar for defending profiling-based employment decisions and effectively penalizes employers without a testing program.

SIX STEPS EMPLOYERS AND BUSINESSES SHOULD TAKE TO PREPARE

Employers and businesses with Delaware operations, employees, or customers should begin preparing now by:

1. *Re-Evaluate DPDPA Applicability*. Reassess DPDPA coverage under the new thresholds, especially if you market to Delaware residents, have Delaware-based employees, or use tracking technologies on visitors who may be residents.

2. *Assess Third-Party Status*. If you are a vendor, service provider, or data recipient, separately assess whether this would be classified as a third-party acquiring data from a controller (which triggers coverage regardless of the 10,000 or 5,000 consumer thresholds).

3. *Inventory AI and Profiling Tools*. Take inventory of automated tools used to profile employees or consumers, including AI hiring platforms, workforce analytics, underwriting models, fraud scoring systems, and dynamic pricing engines.

4. *Map Data Flows and Update Contracts*. Map third-party data flows and review vendor contracts to confirm alignment with the new contracting and due diligence requirements.

5. *Establish Bias Testing Policies and Procedures*. Implement a bias testing process for profiling tools used in consequential decisions, and document the methodologies used and results found.

6. *Audit Compliance Workflows and Notices*. Audit current workflows to identify where privacy notices, consent tracking, opt-out mechanisms, and adverse action processes fall short of the new disclosure, human review, and correction rights.