Insights, News & Events

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

Insights
Jun 5, 2026

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

Just over a year after Delaware's privacy law took effect, state lawmakers are close to expanding its reach by passing a bill that could soon cover more businesses, narrow a key exemption, and expand the definition of sensitive data. Most notably for employers, the pending legislation would also impose significant new obligations on the use of AI in the workplace, capturing resume screeners, interview scoring tools, workforce analytics platforms, and similar technology. If the bill passes as expected, these amendments would take effect on January 1, 2027. What do you need to know about this bill and what are the six steps you should take to prepare?

Quick Status Update

House Bill 380 would amend Delaware's Personal Data Privacy Act (DPDPA), which passed in 2023 but took effect in 2025 (you can read a summary here). The bill passed the House on May 21 by a 30-9 vote and now sits in the state Senate, where it is expected to soon pass given its strong momentum and institutional backing. The legislative session wraps on June 30, so we'll have the definitive word on the bill in the next few weeks.

Given that HB 380 was developed in partnership with the Delaware Department of Justice, odds are high that

Related People

Vivian Isaboke, CIPP/US, CIPM

Associate

908.516.1028

Service Focus

Consumer Privacy Team

Privacy and Cyber

Governor Matt Meyer will sign it when it lands on his desk.

Key Changes the Bill Would Bring About

Here is a list of the key changes that all employers and businesses should know about.

Applicability Thresholds and Expanded Scope

HB 380 would substantially lower the applicability thresholds related to data controlled or processed. If the bill passes, a business conducting business in Delaware, or producing products or services targeted to Delaware residents, would 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 bill 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 would 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). HB 380 would replace that with a narrower framework where the exemption would 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-charted 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, would need to reassess whether they still qualify for the entity-level GLBA exemption if the bill passes.

Healthcare and HIPAA Data Exclusions

HB 380 would also add 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 would carve 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 would 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 would remain the only state where

comprehensive consumer privacy law would apply to employment data on the same terms as consumer data.

However, HB 380 would carve a narrow exception so that some types of automated decision-making would be covered by state privacy law. Specifically, rather than exempting employment data across the board as other state privacy laws do, the bill would bring 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 would fall within the DPDPA's obligations.

Expanded Vendor Obligations and Fair Credit Reporting Act Safe Harbor

In relation to AI and automated decision-making, HB 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. HB 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 would also retain direct, ongoing obligations to residents. Upon request, a controller would 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 would also need to provide the resident with an opportunity to correct any inaccurate data.

These expanded vendor obligations, however, would not apply to activity already governed by the Fair Credit Reporting Act (FCRA). HB 380 would provide 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, would therefore be shielded from the new adverse action and human review obligations.

Data Protection Assessments

HB 380 would lower the mandatory Data Protection Assessment (DPA) threshold from 100,000 to 50,000 consumers and add 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 would 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 would not be able to rely on vendor compliance representations alone and would remain directly responsible for conducting the required impact assessments and ensuring the deployment meets HB 380's other obligations.

Expanded Definition of "Sensitive Data"

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

- 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 would 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 would need to obtain consent before generating or using these outputs on Delaware-resident employees and applicants. If the bill passes, you 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 you may not have previously classified as sensitive.

Disclosure Requirements for Sensitive Data

HB 380 would also impose 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;
- 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.

Conclusion

We will continue to monitor HB 380 as it moves through the legislature and will provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Privacy and Cyber Practice Group or Consumer Privacy Team.