PUBLICATION

The Delaware Effect: Five Privacy and AI Law Changes That General Counsel, HR, and Marketing Need to Know

Authors: Alisa L. Chestler, Vivien F. Peaden, Scott M. Douglass, Bruce C. Doeg
September 10, 2026

Delaware has re-entered the privacy conversation. Governor Meyer signed HB 380 on September 2, 2026, amending the Delaware Personal Data Privacy Act (DPDPA) to become one of the most restrictive privacy and artificial intelligence (AI) laws in the United States.

The amendment takes effect January 1, 2027, giving businesses a narrow window to assess compliance and renegotiate supplier agreements. Following California's lead as an early mover in privacy legislation, the amended DPDPA is poised to become a blueprint for future state laws. Given the attention to privacy regulation as a generally bipartisan focus, we should expect more enforcement in the coming years. While the law does not have a private right of action, these changes might encourage plaintiff attorneys to enhance class-action privacy litigation efforts and join some of the other states in such cases. Below, we explore the **top five** changes and what they mean.

1. Lower Applicability Thresholds

Most state privacy laws set a two-tier applicability threshold: the first tier applies when a business processes personal data of a specified number of state residents (**Data Volume Threshold**). The second tier applies when a business processes a lower volume of personal data and derives a specific percentage of revenue from selling it (**Data Sales Threshold**). The amended DPDPA dramatically lowers both thresholds:

- **The Data Volume Threshold** falls from 35,000 to **10,000 Delaware** residents, i.e., roughly 1 percent of the state's population and among the lowest thresholds in the nation.
- **The Data Sales Threshold** falls from 10,000 to **5,000 Delaware residents** if more than 20 percent of the business's gross revenue is derived from data sales.

Most significantly, the amendment adds a third tier **covering any** "*third party who acquires personal data from a controller*." This is a paradigm shift bringing entities that receive personal data from a controller within the DPDPA, regardless of size, revenue, or processing volume. Unlike California, the DPDPA does **not** exempt *most* non-profit organizations.

Key Takeaways: *For corporate marketing teams that share consumer data with advertising platforms, analytics providers, or data brokers, the compliance implications are imminent. The same is true for non-profit fundraising teams at universities or religious institutions that process large volumes of donor and constituent data.*

2. Game-Changing Implications for Marketing Teams and AdTech

The amended DPDPA brings the entire AdTech ecosystem within Delaware's jurisdiction.

a. Marketing's Blind Spot: Additional Contractual and Due Diligence Requirements

Historically, marketing teams and their vendor relationships received less compliance scrutiny, as many of these agreements are seen as "just a click-through" or "non-negotiable," so the contractual language is not reviewed. That assumption is changing rapidly. Under the amendment, when a marketing team shares personal data with a third party, the parties must enter into a written contract with specified privacy terms. This requirement covers many routine data exchanges that support marketing operations, including:

- **Customer list sharing**: combining a customer mailing list with one provided by a trade association or co-marketing partner for a joint campaign;
- **MarTech platforms**: feeding personal data into MarTech and AdTech tools, such as HubSpot, Salesforce, Google Analytics, and Meta Pixel, to track, score, or segment an audience;
- **Data brokers**: purchasing third-party datasets to supplement a CRM or sourcing lookalike audiences from a data aggregator; and
- **Advertising partners**: sharing audience segments with ad networks or retargeting vendors to automate advertising based on individuals' browsing activity across channels, a practice known as "**Targeted Advertising**."

If these recipients use personal data for their own purposes, they are "**third parties**" under the DPDPA. Marketing contracts with these partners must limit data use to defined purposes, require compliance with additional privacy obligations, and provide remedies for unauthorized use. **Without a written contract,** these **third parties are prohibited from further processing** personal data. Organizations should not assume their partners always understand their obligations.

The Delaware amendment requires **documented measures and due diligence efforts on all data recipients** commensurate with the sensitivity of the data being disclosed.

b. Broad Consumer Rights: Disclosure of Specific Third Parties

The amendment also gives consumers the right to request that a business disclose information about the third parties that receive their personal data. Previously, Delaware, like most states, required only a high-level description of data recipients *by category* (e.g., "advertising partners" or "analytics providers").

This change requires greater transparency and accountability when a consumer asks, "Who has my data?" Subject to certain exceptions, a company must maintain a **current, detailed list** of each third-party partner that receives personal data, rather than a general category list, unless an exemption applies.

Key Takeaways: *Compliance and marketing teams must collaborate to track all third parties that process consumer data. Generic disclosures will no longer satisfy the DPDPA. This will require updating privacy policies, additional data mapping, and consumer-request workflows.*

3. AI Meets Privacy: HR and B2B Data Now Partially in Scope

The most forward-looking changes in the DPDPA address the intersection of AI and automated decision-making. The DPDPA previously regulated "**Profiling**," or data processing based on a person's finances, health, behavior, background, or location to inform high-stakes decisions in employment, education, lending, health care, insurance, and other essential services, if such profiling was "solely" automated. The amendment removes the "solely" limitation, such that Delaware residents can opt out of automated Profiling even if a human reviews or approves the high-stakes decision. The amended DPDPA also identifies these high-stakes decisions as "Decisions that produce legal or similarly significant effects," or what other states often refer to as

"Consequential Decision(s)." This definition aligns Delaware with AI laws in the EU and California that respectively designate these use cases as "High-Risk" or "Significant Decisions."

a. Notice and Disclosure for Adverse Decisions

When a company discloses a Delaware **resident**'s data for making a high-stakes automated decision based on that person's finances, health, behavior, demographics, or location, that information constitutes a "**Report**." Notably, while the amended DPDPA continues to use "consumer" as its primary defined term in most provisions, it introduces the broader term "resident," referring to any natural person residing in Delaware. This distinction is critical: personal data collected in human resources (HR) and B2B contexts is now partially in scope when a company feeds it into AI-enabled decision-making tools for a Consequential Decision. As a result, the amended DPDPA extends protection beyond consumers to cover employees, job applicants, and business contacts.

Companies that use or license AI-powered decision-making tools now face additional compliance obligations under the amendment. Both companies and any third-party providers must execute written agreements, provide adverse-action notices and opportunities for human review concerning the resident, respond to data requests within 30 days, and disclose all third-party recipients during the prior 24 months.

In practice:

HR: A company uses an AI tool to screen resumes, rank employee performance, or identify positions for elimination. If the output leads to a Delaware resident's rejection, denial of a promotion, or termination, the resident must receive an adverse-action notice, a description of the data used, and an opportunity to request human review.

B2B: A fintech platform denies a loan to a Delaware-resident business owner, or a vendor-onboarding platform rejects a contractor, based on an automated risk score. The same notice and human review requirements apply in such a B2B context.

b. Broad Consumer Rights to Opt Out of AI-Enabled Consequential Decisions

In addition to requesting human review of adverse actions, Delaware residents may now **opt out of having their personal data used in automated, high-stakes use cases.**

Previously, consumers could opt out only when a decision was "solely automated," meaning no human involvement at all in making Consequential Decisions. By removing "solely," the DPDPA now covers AI-assisted and hybrid decision-making, even when a human reviews the output but AI performs most of the work.

In practice:

Insurance: An insurer uses AI to set premiums for homeowners' policies. Previously, a resident could not opt out if an underwriter reviewed the rate before issuance. Now, the resident may opt out of **Profiling** even if a human signs off.

Education: A university shares alumni records with an analytics vendor that uses AI to score donors and predict giving capacity. Previously, alumni could not opt out if a development officer reviewed the output. Now, they may opt out of **Profiling** even if an alumni-relations professional makes the final contact decision.

4. Heightened Protection for Sensitive Data

The amendment significantly expands the definition of "**Sensitive Data**" and the requirements for processing or selling it. The definition now includes three new categories: **(1) neural data** (brain activity measurements); **(2) financial account credentials**; and **(3) government-issued IDs**, such as SSNs and passports. It also clarifies that inferences derived from personal data that reveal Sensitive Data are treated as Sensitive Data themselves.

The amendment tightens restrictions against selling Sensitive Data. Unlike Maryland law, which imposes a per se ban without exceptions, Delaware permits *the sale of* **Sensitive Data** *only* if *all four conditions are met*:

1. **Strict Necessity**: Sell Sensitive Data only when necessary to provide the requested offering;
2. **Pre-Sale Notice**: Provide clear notice before the sale, specifying the categories of **Sensitive Data**, purposes, and third-party recipients;
3. **Consumer Consent**: Obtain affirmative opt-in consent from the consumer; **and**
4. **Recordkeeping**: Retain consent records and risk assessments for five years.

In addition to obtaining consumer consent, organizations must conduct a risk analysis showing that processing Sensitive Data is "reasonably necessary and proportionate to the disclosed purposes." Effective January 1, 2027, this dual requirement means that even consented processing must pass a proportionality test.

In practice: A food-delivery app collects precise geolocation data to enable online ordering and delivery. Even with the customer's consent, the app provider must document a risk analysis showing that collecting precise geolocation data is "reasonably necessary and proportionate" to the delivery purpose.

5. Enhanced Data Protection Assessments: A Preview of the EU AI Act

The DPDPA amendment lowers the threshold for **mandatory data protection assessments** from 100,000 to **50,000 consumers**. This brings more businesses into scope for data processing activities that present a "heightened risk of harm," including Targeted Advertising, the sale of personal data, certain Profiling activities, and processing **Sensitive Data**.

Companies engaged in AI-enabled data processing and decision-making must conduct regular risk assessments for qualifying processing activities. These assessments must document the purpose and intended uses, risk analysis, categories of input and output data, performance metrics, transparency measures, and post-deployment monitoring procedures.

This framework closely resembles the EU AI Act's requirements for high-risk AI systems. Companies deploying AI tools for automated decision-making or Targeted Advertising should prepare to meet both regimes, which will take effect in approximately four months on January 1, 2027, for Delaware and on December 2, 2027, for the EU AI Act.

In practice: An e-commerce company uses customers' browsing histories across multiple sites for **Targeted Advertising**, creates consumer profiles for certain purposes, or shares visitors' precise geolocation with Meta Pixel. It must now conduct and document a data protection assessment if it exceeds the 50,000-consumer threshold. A similar framework will soon apply under the EU AI Act, so multinational companies should build a compliance program that addresses all applicable laws.

Looking Ahead: A National Trend

Delaware's amendment is not an isolated development. It signals the second wave of state privacy law evolution, a trend pioneered by California's 2025 amendment and now being accelerated by Delaware and

other states taking up such provisions. U.S. states are moving beyond first-generation privacy frameworks to regulate modern data ecosystems, AI-driven decision-making, and pervasive third-party data sharing. Because virtually all organizations operate in multiple data protection regimes, Delaware's framework should be utilized to revisit compliance obligations and related operations. Failure to act could result in enforcement actions or litigation exposure.