Delaware’s Amended Privacy Law: Key Impacts on Adtech Contracts and Diligence Processes

Aaron J. Burstein, Alexander I. Schneider, Meaghan M. Donahue

September 13, 2026

On September 2, Delaware Gov. Matt Meyer signed H.B. 380 – a significant expansion of the Delaware Personal Data Privacy Act (DPDPA) that makes it one of the strictest state comprehensive privacy laws in the country. The amendments, which will go into effect on January 1, 2027, stand to materially impact compliance considerations for certain covered businesses, notably by introducing new third-party due diligence and contracting obligations (similar to those required in California), further restricting sensitive data processing, and expanding the law’s jurisdictional thresholds and consumer rights.

Contracting and Due Diligence Obligations for Disclosures to Third Parties

Required Contract Terms. Controllers that disclose personal data to third parties, including in a sale of personal data or for targeted advertising, must enter into binding contractual agreements that include the following terms:

- Specify that the personal data is disclosed or sold only for limited and specified purposes, including whether the purpose includes use for decisions that produce legal or similarly significant effects;
- Require the third party to comply with and provide the same level of privacy protections as required by the DPDPA;
- Allow the controller to take reasonable and appropriate steps to ensure the third party complies with their obligations under the DPDPA;
- Require the third party to notify the controller if it determines it cannot meet its obligations under the DPDPA; and
- Allow the controller to take reasonable and appropriate steps to stop and remediate any unauthorized use of personal data.

Due Diligence Requirements. On top of these contracting requirements, H.B. 380 requires controllers to conduct “reasonable due diligence” of third parties to which the controller discloses personal data, including in the context of the sale of personal data and targeted advertising. In particular, controllers must:

- Assess through the use of questionnaires and review of relevant documents (at minimum) the third party's policies and technical and organizational measures undertaken to support and demonstrate compliance with the Delaware privacy law; and
- Undertake "additional reasonable measures" commensurate with the sensitivity of the data disclosed to the third party.

Practical Takeaways. The CCPA established similar requirements for agreements with third parties, and in many instances, businesses tailored their agreements to apply only to CCPA-covered data. Once H.B. 380 goes into effect, that approach is no longer an option. Businesses will need to revisit those agreements and either add a Delaware-specific addendum alongside existing California terms, or adopt a jurisdiction-neutral framework that can accommodate additional states as this trend continues.

H.B. 380's updated requirements suggest a few specific steps that participants in the digital advertising ecosystem and businesses that monetize first-party data should consider taking:

- Digital publishers and advertisers should confirm their adtech contracts include required contracting terms. They may also need to build the law's diligence requirements into their contract onboarding flows and privacy programs.
- Businesses that monetize first-party data, including in contracts with data brokers, should ensure contracts include mandatory terms and conduct appropriate diligence of data buyers or licensees.
- Adtech vendors, data brokers, and other vendors classified as "third party" controllers should consider whether they need to update standard contracts to reflect Delaware's new requirements. Vendors should expect requests to include mandatory terms in existing and new contracts.

Changes to contracting requirements are not the only thing businesses should keep an eye on with H.B. 380. In addition, the legislature also lowered the DPDPA's applicability thresholds, narrowed existing exemptions, provided updated consumer rights, and broadened existing definitions. We break down these additional changes below:

New Categories of Sensitive Data and Broader Processing Restrictions

Updated Definition of "Sensitive Data." H.B. 380 expands the definition of "sensitive data" – a trend seen in other amendments to existing state privacy laws – to include the following additional categories of personal data:

- National origin;
- Mental or physical health condition, diagnosis, treatment, or status (including pregnancy);
- Neural data that is generated by measuring the activity of an individual's central nervous system;
- Financial account number/log-in information/credit or debit card number in combination with a password or security code that allow access to a consumer's financial account; and

- Government issued identifiers, like social security numbers or driver's license numbers.

The expansion of sensitive data to include "mental or physical health … status" mirrors a similar change to Connecticut's law that took effect this year. Businesses that collect or process health-related data should assess whether the data is now covered by Delaware's sensitive data definition.

The amendments also make clear that inferences made based on personal data, alone or in combination with other data, that are used to reveal or identify a sensitive characteristic constitute sensitive personal data, expanding the scope of what could be considered sensitive under Delaware law.

Restrictions on Processing and Selling Sensitive Data. In addition, to *process* sensitive personal data, H.B. 380 requires consumer consent, and the processing must be reasonably necessary and proportionate to the disclosed purposes for processing.

To *disclose* sensitive personal data *in a sale* under H.B. 380, 1) the disclosure must be strictly necessary to provide or maintain a product or service affirmatively requested by the consumer; and 2) the controller must provide a clear and conspicuous notice before the sale occurs, including the specific categories of sensitive data to be disclosed, the purposes of disclosure, and the specific third parties to which the sensitive data will be disclosed.

Expanded Scope of Obligations

Scope of Applicability. H.B. 380 reduces the DPDPA's applicability threshold to apply to businesses that (1) control or process the personal data of 10,000 or more consumers (previously 35,000), or (2) control or process the personal data of 5,000 or more consumers (previously 10,000) and derive more than 20% of revenue from the sale of personal data. The amendments also extend applicability to third parties that acquire personal data from a controller, regardless of the amount of personal data processed.

Narrower GLBA Exemption. H.B. 380 also narrows the exemption for entities subject to the Gramm-Leach Bliley Act (GLBA) – where the law previously provided a broad entity-level exemption, the amendments limit this exemption only to insurers principally engaged in financial activities under the GLBA, banks directly engaged in financial activities under the GLBA, and securities firms regulated by the state's Investor Protection Unit or the Securities and Exchange Commission. As such, GLBA-covered entities that fall outside of these categories, such as fintech companies and payment processors may no longer be able to assert exemption from the law.

Consumer rights. H.B. 380 amends the rights available to Delaware consumers in line with those available in other states.

- As part of a right to know request, consumers will also be able to request information about any inferences derived from the personal data by the controller, and whether the controller or processor is processing personal data for profiling in furtherance of legal or similarly significant decisions.

- Similar to CT, OR and MN, consumers will also have the right to request a list of the specific third parties that the controller has disclosed their personal data to, unless the personal data is pseudonymous, the listing of a third party would reveal a trade secret, or the controller cannot compile the list with reasonable effort (in which case the controller must disclose generally all third parties to which the controller discloses personal data).

Profiling. H.B. 380 imposes additional requirements related to “profiling” – including some that are applicable to employment data, which is otherwise exempt from the DPDPA.

Profiling. H.B. 380 imposes additional requirements related to “profiling” – including some that are applicable to employment data, which is otherwise exempt from the DPDPA.

- Controllers that process the personal data of 50,000 or more Delaware consumers and that engage in profiling in furtherance of automated decisions that produce a legal or similarly significant effect must conduct an impact assessment that includes an analysis of any known or foreseeable risk of harm, and describes, among other things, the categories of personal data processed, the outputs of the profiling, transparency measures, and steps for post-deployment monitoring.

- The law also imposes obligations on third parties that receive “reports” from controllers, which include recommendations, summaries, or automated decisions based on personal data or profiling, for use in connection with any decision that produces a legal or similarly significant effect on a consumer. For example, the third party must agree to provide Delaware residents with notice of any “adverse action” the third party takes based on a report. The third party must also respond to requests to access or correct personal data used in connection with profiling.

- “Reports” that are used in connection with employment decisions are subject to the law, despite the general exemption in the DPDPA for employee or job applicant personal data.