Delaware Makes a Baker's Dozen: Delaware Becomes the Thirteenth State to Enact a Comprehensive Consumer Data Privacy Law

On September 11, Delaware Governor John Carney signed into law the Delaware Personal Data Privacy Act (DPDPA) (House Bill 154), making Delaware the thirteenth state to enact a comprehensive data privacy framework. The DPDPA contains many similarities with the data privacy laws recently enacted in states such as Connecticut and Oregon, with some notable differences, as discussed further below. The DPDPA will go into effect on January 1, 2025.

Applicability Threshold for DPDPA

The DPDPA applies to any person who conducts business in the State of Delaware or produces products or services that are targeted to residents of the state and, during the preceding calendar year, controlled or processed the personal data of either:

- At least 35,000 consumers (excluding personal data controlled or processed solely for the purpose of completing a payment transaction).
- At least 10,000 consumers and derived more than 20% of its gross revenue from the sale of personal data.

It is notable that this 35,000 consumer threshold is lower than those generally found under other state laws (100,000), as Delaware appears to have instituted the lower threshold to account for its smaller population. Delaware is not the first state to make such an adjustment, with Montana setting its threshold at 50,000 consumers and Tennessee raising the threshold to 175,000 consumers to adjust for a *larger* population. The DPDPA's gross revenue threshold is also lower than those found under other recent state privacy laws, which have generally set the amount at 25%. As with other states, the DPDPA defines "personal data" as likely to include IP addresses. In calculating whether the DPDPA will apply, companies must, therefore, include hits on any websites where the IP address is received.

Exemptions to DPDPA

The DPDPA does not contain the exemption for HIPAA-covered entities or business associates that have generally been found in other state privacy laws, but it does exempt PHI, which likely includes PHI in the hands of business associates. Furthermore, and in alignment with Oregon and Colorado, the DPDPA does not contain a general exemption for nonprofits. However, there *are* two limited exemptions for (1) nonprofits that are dedicated exclusively to preventing and addressing insurance crime, and (2) data collected from a victim of or witness to child abuse, domestic violence, human trafficking or similar activities and where such data is collected, processed, or maintained by a nonprofit providing services to that victim or witness.

Other exempted entities and forms of data include:

- State governmental entities are exempt from the DPDPA. The exemption explicitly does not cover "institutions of higher education," but there is an exemption for data collected or processed in accordance with the Family Educational Rights and Privacy Act.

- Financial institutions and their affiliates to the extent subject to Title V of the Gramm–Leach–Bliley Act (GLBA). There is also an exemption for data collected or processed in accordance with the GLBA.
- National securities associations registered pursuant to the Securities Exchange Act of 1934.
- Data collected or processed in accordance with the following laws:
    - Fair Credit Reporting Act
    - Driver's Privacy Protection Act
    - Farm Credit Act
- Personal data used in clinical research that is already subject to the standards of the Common Rule or International Conference on Harmonization (ICH).

Controller Obligations under DPDPA

The DPDPA imposes fairly standard obligations on two types of entities: entities that determine the purpose and means of processing personal data (Controllers) that meet the applicability threshold; and entities that process personal data on behalf of Controllers (Processors). The DPDPA also gives individual consumers certain rights that must be fulfilled by Controllers, including rights to:

- Confirm whether a Controller is processing the consumer's personal data and accessing such personal data.
- Correct inaccuracies in the consumer's personal data.
- Delete personal data provided by, or obtained about, the consumer.
- Obtain a copy of the consumer's personal data in a portable and readily usable format that allows the consumer to easily transmit the data to another Controller.
- Obtain a list of the categories of third parties to which the Controller had disclosed the consumer's personal data.
- Opt out of the processing of personal data for targeted advertising, the sale of personal data, or profiling "in furtherance of solely automated decisions that produce legal or similarly significantly effects concerning the consumer."

The above rights largely align with the rights granted to consumers under other state privacy laws. The right to obtain a list of third parties to which a Controller has disclosed personal data is not found in similar privacy law, though it is similar to a California law. Furthermore, and like many state privacy laws, the DPDPA requires Controllers to recognize universal opt-out mechanisms (UOOMs) by January 1, 2026.

The DPDPA also creates additional administrative burdens on Controllers.

Privacy Notice

- Controllers under the DPDPA must provide consumers with a "privacy notice" that is reasonably accessible, clear, and meaningful. The notice must include all of the following:
    - The categories of personal data processed.
    - The purpose(s) for such processing.
    - The way in which a consumer can exercise their rights and appeal a decision made by a Controller with regard to the consumer's request.
    - The categories of personal data that the Controller shares with third parties.
    - The categories of third parties to whom the Controller shares personal data.
    - An email address or other online mechanism through which consumers can contact the Controller.

These components are similar to other state privacy laws, so Controllers that are already complying with the law of another state should find it relatively simple to make any updates needed to comply with the DPDPA.

Processing of Sensitive Data

- The DPDPA includes a broad definition of "sensitive data," including genetic or biometric data, precise geolocation data, the personal data of a known child, and any data revealing status as transgender or non-binary. Whereas some of the first state privacy laws did not include a definition with this breadth, the DPDPA and Oregon's law demonstrate a trend toward a more encompassing definition for sensitive data. Controllers are not permitted to process sensitive data under the DPDPA without first obtaining the consumer's consent. If the consumer is a known child, the Controllers must obtain the consent of that child's parent or lawful guardian.

Data Protection Assessments

- The DPDPA requires Controllers to conduct data protection assessments (DPAs) for processing that presents a "heightened risk of harm to a consumer." The specific instances of heightened risk and the requirements for the DPAs themselves are similar to other state privacy laws. There is, however, a grace period under the DPDPA, as it only covers processing activities beginning six months following the DPDPA effective date.

Children's Data

- Under the DPDPA, Controllers may not process personal data for purposes of targeted advertising and may not sell personal data without the consumer's consent if the Controller knows, or should know, that the consumer is between the ages of 13 and 18. This aligns with more recent state privacy laws, such as Connecticut and Oregon, but with a higher upper age limit of 18. As noted above, Controllers are not permitted to process the sensitive data of any known child without first obtaining the consent of that child's parent or guardian.

General Controller Duties

- As with other state privacy laws, the DPDPA contains a number of requirements for Controllers, such as:
    - To limit the collection and processing of personal data to only what is adequate, relevant, and reasonably necessary in relation to the purposes for the processing unless with consent.
    - To provide an effective means for a consumer to revoke their consent and stop processing the consumer's data within 15 days after receipt of that revocation.
    - To establish, implement and maintain reasonable administrative, technical, and physical data security practices to protect personal data.
    - To not process personal data in violation of state or federal non-discrimination laws.
    - As discussed above, to not process the personal data of a consumer for targeted advertising or sell personal data without consent where the consumer is between the ages of 13 and 18.
    - To not discriminate against a consumer for exercising their rights under the DPDPA.

Enforcement of DPDPA

The DPDPA does not contain a private right of action and the Delaware Department of Justice (DDOJ) has sole enforcement authority, which can seek up to $10,000 per violation. It should be noted that through December 31, 2025, the DDOJ will issue a notice of violation to the Controllers in violation of the act if such violation is capable of cure, and the Controller will have 60 days to cure the violation. This aligns with the cure periods of other states, which range from 30 to 90 days.

Important Dates for DPDPA

- **January 1, 2025**: The DPDPA goes into effect.
- **December 31, 2025**: The right to cure sunsets.
- **January 1, 2026**: UOOM recognition deadline.

Our team will continue to monitor the DPDPA. If you have any questions about the DPDPA or other state privacy laws and how they could affect your business, please contact the authors.