Delaware Passes Consumer Privacy Law: 10 Things Businesses Need to Know

Insights
9.14.23

Delaware businesses should begin preparing for a new law that will provide consumers with privacy rights over their personal data collected by covered entities and impose a series of related requirements on those entities. Governor John Carney recently approved the Personal Data Privacy Act (PDPA) on September 11, making Delaware the twelfth state — and the seventh in just 2023 alone — to pass comprehensive consumer privacy legislation. Here are the answers to your top 10 questions about Delaware's new law.

1. What Other States Have Passed Similar Laws?

Delaware's PDPA follows in the footsteps of similar laws passed in California, Virginia, Colorado, Utah, Connecticut, Iowa, Indiana, Tennessee, Montana, Texas, and Oregon.

2. When Will the PDPA Take Effect?

The PDPA will take effect on January 1, 2025.

3. Will the PDPA Apply to Your Business?

The PDPA will apply to any person that conducts business in Delaware or persons that produce products or services that target Delaware residents and that during the preceding calendar year:

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

"Consumer" is defined to mean an individual who is a resident of Delaware. However, the definition excludes "an individual acting in a commercial or employment context."

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual, and does not include de-identified data or publicly available information.

In comparison to other states, Delaware's 35,000 consumer threshold is low. For example, the laws in Colorado, Iowa, Indiana, and Oregon contain consumer thresholds of 100,000.

In addition, the 10,000 consumer / 20% revenue threshold is lower than thresholds in other states. For example, Connecticut and Montana each have a 25,000 consumer / 25% revenue threshold, and Indiana has a 25,000 consumer / 50% revenue threshold.

4. How Are Nonprofit, HIPAA, and Gramm-Leach-Bliley Organizations Treated?

Nonprofit Organizations – Similar to the laws passed in Colorado and Oregon, the PDPA does not provide a full exemption for nonprofit organizations. However, it does exempt nonprofit organizations dedicated exclusively to preventing and addressing insurance crime. It also exempts the personal data of a victim or witness of certain crimes (e.g., child abuse, domestic violence, and stalking) that is collected, processed, or maintained by a nonprofit organization that provides services to victims or witnesses.

HIPAA – The PDPA does not provide an entity-level exemption for organizations subject to the Health Insurance Portability and Accountability Act (HIPAA) but it does contain a data-level exemption for protected health information under HIPAA.

GLBA – The PDPA includes entity-level and data-level exemptions for institutions and information governed by the Gramm-Leach-Bliley Act.

5. Are Employees Treated as Consumers?

No. The PDPA's definition of "consumer" excludes those acting in an employment context. Moreover, the PDPA specifies that it does not apply to data processed or maintained in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.

6. What Rights Will Consumers Have?

Under the PDPA, a consumer will have the right to:

- Confirm whether a controller is processing the consumer's personal data and access such personal data (unless such confirmation or access would require the controller to reveal a trade secret);
- 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 processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the

data to another controller without hindrance, where the processing is carried out by automated means (provided such controller shall not be required to reveal any trade secret);

- Obtain a list of the categories of third parties to which the controller has disclosed the consumer's personal data;
- Opt-out of the processing of the personal data for the purposes of targeted advertising; the sale of personal data; and/or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

7. What Duties Will Controllers Have?

A "controller" is defined to mean a person that, alone or jointly, determines the purpose and means of processing personal data. The PDPA requires that controllers:

- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer;
- Not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;
- Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue;
- Not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of processing sensitive data concerning a known child, without first obtaining parental/guardian consent and complying with Delaware law regarding online marketing or advertising to a child;
- Not process personal data in violation of Delaware state law and federal laws that prohibit unlawful discrimination;
- Provide an effective mechanism for a consumer to revoke the consumer's consent and, upon revocation of consent, cease to process the data as soon as practicable but not later than 15 days after receipt of such request;
- Not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge or willfully disregards that the consumer is between 13 and 18 years old; and
- Not discriminate against a consumer for exercising any rights in the PDPA, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

Controllers are also required to provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

- The categories of personal data processed by the controller;
- The purpose for processing personal data;
- How consumers can exercise their rights, including how a consumer may appeal a controller's decision regarding a consumer's request;
- The categories of personal data that the controller shares with third parties;
- The categories of third parties with which the controller shares personal data; and
- An active email address or other online mechanism that the consumer may use to contact the controller.

8. How is Sensitive Data Treated?

Delaware's definition of "sensitive data" is broader than the definitions used in other states' consumer privacy laws. While it includes traditional categories such as data pertaining to racial/ethnic origin and religious beliefs, it also includes data revealing status as transgender or nonbinary. Similarly, Oregon's law also includes status as transgender or nonbinary in its definition of sensitive data.

The PDPA also includes biometric data in its definition of sensitive data. Biometric data is defined as "data generated by automatic measurements of an individual's unique biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual." The definition excludes a digital or physical photograph; an audio or video recording; and any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

9. Can an Individual Bring an Action for Violation of the PDPA?

No. There is no private right of action that permits an individual to bring a claim for violations.

The Delaware Department of Justice has sole enforcement authority and may investigate and prosecute violations. The PDPA includes a 60-day cure period for violations, but this provision has a sunset date of December 31, 2025.

10. What Should Businesses Do?

If your business will be subject to the PDPA, you should be taking immediate action to prepare for compliance. This may include:

- Assessing your organization's current data collection and privacy practices;
- Conducting an inventory of data that your organization has historically collected about consumers;

- Considering the types of data that your organization will likely collect about consumers in the future;
- Identifying the information that your organization collects about minors;
- Developing policies and procedures for responding to consumer requests; and
- Working with data privacy counsel to ensure that your organization is in compliance with the PDPA.

Your compliance plan can be fast-tracked with the help of Fisher Phillips' Consumer Privacy Team. We are prepared to work with your organization on steps such as a privacy gap assessment, data inventory, and preparing templates for, or helping to draft customized versions of, compliant privacy notices and policies.

Conclusion

For further information, contact your Fisher Phillips attorney, the author of this Insight, or any attorney on the firm's Consumer Privacy Team. Fisher Phillips will continue to monitor consumer privacy law developments 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 direct to your inbox.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email

Service Focus

Data Security and Workplace Privacy