THOMPSON HINE

Privacy & Cybersecurity Update

September 2023

Delaware Personal Data Privacy Act Signed Into Law With 2025 Effective Date

On September 11, 2023, Governor John Carney signed into law the Delaware Personal Data Privacy Act (DPDPA), which affords Delaware residents a broad range of data protection rights and requires certain covered businesses to comply with new data privacy and information security requirements. The law will enter into force on January 1, 2025.

The DPDPA does not create a private right of action. Rather, the Delaware Department of Justice will have exclusive authority to enforce the law and penalties which could range up to $10,000 per violation following applicable judicial proceedings.

Scope of Applicability. The DPDPA applies to any organization that conducts business in Delaware, or that provides products or services that are targeted to residents of the state *and* during the preceding calendar year meet any of the following criteria:

- 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 not less than 10,000 consumers and derived more than 20% of its gross revenue from the sale of personal data.

Under the DPDPA, personal data is defined as "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." De-identified data is defined as data that cannot reasonably be used to infer information about, or otherwise be linked to an individual, or a device linked to such individual.

The DPDPA defines "sensitive data" as personal data that reveals a consumer's racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis (including pregnancy), sexual orientation, status as transgender or non-binary, citizenship or immigration status, personal data of a known child, genetic or biometric data, or precise geolocation data (i.e., information derived from technology that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet).

The DPDPA includes several exemptions that are standard in data privacy frameworks, including exemptions for data processing activities governed by federal law (e.g., HIPAA, GLBA) and data processing conducted in the HR/employee and business-to-business contexts.

Consumer Data Privacy Rights. DPDPA provides consumers residing in Delaware with the following rights:

- The right to confirm whether a controller is processing the consumer's personal data and to access such personal data, unless such confirmation or access would require the controller to reveal a trade secret.
- The right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.
- The right to delete personal data provided by, or obtained about, the consumer.
- The right to obtain a copy of the consumer's personal data processed by the controller, in a portable and (if

technically feasible) readily usable format that allows the consumer to transmit the personal data to another controller.
- The right to obtain a list of the categories of third parties to which the controller has disclosed the consumer's personal data.
- The right to opt out from a controller's processing of personal data for the purposes of targeted advertising, sale, or profiling in furtherance of *solely* automated decisions that produce legal or similarly significant effects concerning the consumer.

The DPDPA defines a "sale of personal data" as the exchange of personal data for monetary or other valuable consideration by the controller to a third party. However, sale of personal data does not include the disclosure of personal data to data processors and other common data disclosure practices (e.g., disclosure of personal data to an affiliate, at the request of a consumer, or as part of a corporate restructuring).

The DPDPA creates a framework for how controllers must intake, authenticate, and respond to consumer data privacy requests and mandates that organizations "establish a process" to allow a consumer to "appeal" a controller's refusal to take action on a data rights request within a reasonable period of time after the consumer receives the decision.

In particular, a controller must establish one or more secure and reliable means for consumers to exercise their data privacy rights, and which must include posting a conspicuous link on the controller's internet website that enables consumers (either directly or via a third-party agent) to opt out of targeted advertising or the sale of the consumer's personal data. In turn, controllers must comply with opt-out requests that originate from the consumer or the consumer's agent. The consumer may designate an authorized agent via a platform, technology, or mechanism (e.g., an internet link or a browser setting, browser extension, or global device setting).

With respect to appealing a controller's decision, the DPDPA specifies that the process must be "conspicuously available and similar to the process" for submitting data privacy rights requests. The DPDPA requires controllers to inform consumers in writing about any action taken or not taken in response to an appeal, including the reasons for the decision, and if an appeal is denied, the manner in which the consumer may contact the attorney general to submit a complaint.

Privacy Policies and Other Notices. Controllers are required to provide consumers with a "accessible, clear, and meaningful" privacy notice that describes their data processing activities (e.g., categories of personal data collected and processed, purposes of processing, categories of personal data shared with third parties, categories of recipients). The notice must also describe how consumers can exercise their data privacy rights, including how they can appeal a controller's decision and must provide an active electronic mail address or other online mechanism that the consumer may use to contact the controller. A controller that sells personal data or uses it for targeted purposes has the additional obligation to "clearly and conspicuously disclose" such processing and how consumers can exercise their opt-out rights.

Processor Obligations and Contracts. The DPDPA places affirmative obligations on processors, such as those related to compliance with a controller's instructions, assistance in responding to consumer rights requests, and the implementation of security controls to safeguard personal data from unauthorized use.

Like many other data protection laws, the DPDPA also requires controllers and processors to execute written agreements that contain certain data protection clauses, which must address, among other things, the nature and purpose of data processing, duration of the processing, the type of data subject to processing, rights and obligations of parties, duty of confidentiality, and compliance assessments. The DPDPA requires these controller-to-processor contracts to include clauses requiring the processor to delete or return the personal data in its custody at the end of the data processing services unless retention is required by law. In addition, the DPDPA mandates written contracts between processors and subcontractors that require the subcontractor to meet the processor's obligations with respect to personal data processing.

Data Protection Assessments. Generally, the DPDPA requires a controller that processes the data of at least 100,000 consumers to regularly conduct and document a data processing assessment that "presents a heightened risk of harm to a consumer." The DPDPA defines this category of processing broadly to address a variety of common business activities, such as targeted advertising, selling of personal data, processing of sensitive data, and certain types of profiling. The assessment must be made available to the Delaware attorney general upon request.

Rewards Programs and Anti-Discrimination. The DPDPA, like other state data protection laws, permits controllers to offer consumers different services or similar services at different prices that are related to loyalty or rewards programs. However, a controller may not discriminate against a consumer for exercising a data privacy right (e.g., by denying the consumer a good or service or charging a different price, or by providing a different level of quality of a good or service).

Consent. The DPDPA limits how a controller can use personal data without a consumer's consent. For example, an organization may not "process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent." A controller is also prohibited from processing sensitive data or personal data for the purposes of sale or targeted advertising without obtaining appropriate consent.

Data Security Requirements. The DPDPA places affirmative data security obligations on controllers to protect the confidentiality, integrity, and accessibility of personal data. It requires them to 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.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)
216.566.5646, 202.263.4126
Steve.Stransky@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
Certified Information Privacy Professional/United States (CIPP/US)
312.998.4253
Marla.Izbicky@ThompsonHine.com

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com