Akin®

# Delaware Data Protection Act: What Businesses Need to Know

May 13, 2024

Reading Time : **10+ min**

By: Natasha G. Kohne, Joseph Hold

In September 2023, Delaware became the seventh state in 2023 to enact comprehensive privacy law with the Delaware Personal Data Privacy Act (DPDPA), joining Indiana, Iowa, Montana, Oregon, Tennessee and Texas. The DPDPA will go into effect on January 1, 2025.

## Key Provisions

- *Controller Requirements* – obligations for controllers include: data minimization, data security, opt in consent for sensitive data, nondiscrimination, privacy notices, agreements with processors and data protection assessments.
- *Processor Requirements* – obligations for processors include: ensuring a duty of confidentiality for each person processing data, contracts with controllers, assisting controllers with consumer rights requests, data security, deleting or returning personal data after provision of services and conducting data protection assessments.
- *Individual Rights* – consumer rights include: right to access, right to correct, right to delete, right to portability, right to opt out of certain processing, and right to categories of third parties to which the controller disclosed the consumer's personal data.
- *New Right to Third Party Categories List* – provides consumers with a right to obtain a list of categories of third parties to which the controller has disclosed that individual consumer's personal data.
- *No HIPAA Entity-level Exemption* – the law does not exempt covered entities and business associates subject to the Health Insurance Portability and Accountability Act (HIPAA).

- *Universal Opt-Out* – beginning January 1, 2026, controllers must recognize universal opt-out mechanisms.
- *Broader Profiling Opt-Out* – includes "demographic characteristics" in the list of aspects derived from profiling, from which a consumer may opt out.
- *Nonprofits are Covered* – the law generally applies to nonprofit organizations.
- *Sunsetting Right to Cure* – provides a 60-day cure period for alleged violations, which sunsets on December 31, 2025.

## Who Must Comply with the DPDPA?

Similar to other comprehensive state privacy laws and the European Union (EU) General Data Protection Regulation (GDPR), the DPDPA applies to "controllers"—persons that alone or jointly with others, determines the purposes and means of processing personal data, and "processors"—persons that processes that data on behalf of the controller. The DPDPA applies to persons who conduct business in Delaware or produce products or services targeted to Delaware residents ("consumers") and who, during the preceding calendar year, either:

- 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).
- Controlled or processed the personal data at least 10,000 consumers and derived more than 20% of their gross revenue from the sale of personal data.[1]

The 35,000-consumer threshold is among the lowest for states with enacted consumer data privacy laws, with others like Colorado, Virginia, Indiana and Connecticut featuring consumer thresholds of 100,000. The 20% of gross revenue is also comparatively small among states that set the same threshold, with Connecticut using 25% and Virginia using 50%, for example. Notably, and like other state comprehensive privacy laws, the DPDPA does not set a minimum annual revenue threshold, therefore relatively small businesses could be subject to its provisions.

## What Information Is Covered?

The DPDPA applies to "personal data" 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."[2]

Like other comprehensive privacy laws, the DPDPA has a specific definition of "sensitive data," which includes data revealing race or ethnicity, religion, mental or physical health condition or diagnosis (including pregnancy), sex life, sex orientation, status as transgender or nonbinary, citizenship or immigration status, genetic or biometric data, personal data of a known child and precise geolocation data.[3]

## What Are the Notable Exemptions?

Similar to other comprehensive state privacy laws, the DPDPA features both entity-level and data-level exemptions.

*Entity-Level Exemptions*

Comparaed to other comprehensive privacy laws, the DPDPA provides for narrow entity-level exemptions. Specifically, the law exempts (i) state entities, except for institutions of higher education; (ii) financial institutions or affiliates of a financial institution subject to the Gramm-Leach-Bliley Act (GLBA); and (iii) national securities associations or registered futures associations.[4] Notably, the DPDPA departs from other state privacy laws by **NOT** including an entity-level exemption for covered entities or business associates regulated under HIPAA.[5]

Additionally, similar to the Colorado and Oregon privacy laws, the DPDPA generally applies to nonprofit organizations, with two exemptions: (i) an entity-level exemption for nonprofits dedicated exclusively to preventing or addressing insurance crime[6], and (ii) a data-level exemption for personal data of victims of or witnesses to child abuse, domestic violence, human trafficking, sexual assault, a violent felony or stalking that is collected, processed or maintained by a nonprofit providing services to the victim or witnesses.[7]

*Data-Level Exemptions*

The DPDPA has several data-level exemptions. The law excludes data that is de-identified or publicly available from its definition of personal data. The law also excludes from its definition of consumer, individuals "acting in a commercial or employment context."[8] The DPDPA further excludes data related to individual job applicants, agents, independent contractors and employees of a controller, processor or third party for data collected and

used within the context of that role, including emergency contact information and benefits information.[9]

Other data-based exemptions include data subject to the GLBA, as well as data collected, processed, sold or disclosed in compliance with the Family Education Rights and Privacy Act (FERPA), Fair Credit Reporting Act (FCRA), Driver's Privacy Protection Act (DPPA), the Farm Credit Act and the Airline Deregulation Act.[10]

Additionally, while the DPDPA lacks an entity-level exemption for HIPAA covered entities and business associates, it does contain data-level exemptions for certain types of health information. These exemptions include protected health information under HIPAA and patient-identifying information for purposes of 42 U.S.C. § 290dd-2. The law also contains carve-outs for identifiable information pertaining to human subject research, patient safety work product created for the Patient Safety and Quality Improvement Act (PSQIA), and information used for HIPAA-authorized public health purposes.[11]

The DPDPA also provides that controllers and processors that comply with the verifiable parental consent requirements under the Children's Online Privacy Protection Act (COPPA) will be deemed in compliant with any obligation to obtain parental consent required under the DPDPA with respect to a consumer who is a child.[12]

## What Rights Do Delaware Consumers Have?

The DPDPA provides Delaware consumers with a list of rights similar to those found in other comprehensive state privacy laws. Consumers under the law have the right to (1) confirm whether a controller is processing their personal data and access such personal data; (2) correct inaccuracies in the consumer's personal data; (3) delete personal data provided by, or obtained about, the consumer; (4) obtain a copy of their personal data processed by the controller in a format that allows the consumer to transmit that data to another controller, provided the controller is not required to reveal any trade secret; (5) opt out of processing for the purposes of targeted advertising, sale of personal data (with limited exceptions[13]) or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.[14]

Varying from several other state comprehensive privacy laws, the DPDPA also permits consumers to obtain a list of the categories of third parties to which the controller disclosed the personal data *of that specific consumer*(though we note Oregon's law provides a similar right). Comparatively, other state privacy laws give consumers the right to obtain only the categories of third parties to which the controller discloses personal data generally, not specific to the requesting consumer.[15]

Similar to some other state comprehensive privacy laws, the DPDPA requires that controllers grant consumer the right to appeal any refusal to take action on requests to exercise their rights. In providing this right, controllers must establish a process that is conspicuously available to the consumer and respond withing 60 days of receipt of an appeal. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Department of Justice to submit a complaint.[16]

## What Obligations Do Controllers and Processors Have?

The DPDPA contains a familiar list of requirements for both controllers and processors, broadly similar to those found in other state comprehensive privacy laws and the GDPR.

*Controller Requirements*

- **Data Minimization and Purpose Specification**: Controllers are required to limit collection of personal data to what is adequate, relevant and reasonably necessary in relation to the disclosed purposes for which the personal data is processed. Controllers generally may not process personal data for purposes not reasonably necessary for, nor compatible with, the disclosed purpose without obtaining consumer consent.[17]
- **Data Security**: Controllers must establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of consumers' personal data as appropriate for the volume and nature of the data.[18]
- **Sensitive Data**: Controllers may only process consumers' sensitive data after obtaining the consumer's consent. In the case of processing sensitive data concerning a known child, consent from the child's parent or lawful guardian is required.[19]

- **Nondiscrimination**: As with other state laws, controllers must not process personal data in violation of federal or state laws against unlawful discrimination.[20]
- **Transparency**: Controllers must provide a reasonably accessible, clear and meaningful privacy notice that includes: (1) the categories of personal data processed by the controller; (2) the purpose for processing personal data; (3) the categories of personal data shared with third parties; (5) the categories of third parties to whom personal data is shared; (6) an active email address or other online mechanism that the consumer may use to contact the controller; and (7) the manner in which consumers may exercise their rights, including how a consumer may appeal a controller's decision regarding requests to exercise their rights.[21] In the event the controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose such processing, and provide an opportunity to opt out via a clear and conspicuous link on the controller's website.[22]
- **Processor Agreements**: Controllers and processors are required to enter into binding contracts that, among other things, detail the nature and purpose of the processing, the type of data to be processed, instructions for the processing and the rights and obligations of both parties.[23]
- **Opt-Out Preference Signal Requirement**: By no later than **January 1, 2026**, controllers must allow consumers to opt out of the selling or processing of their personal data for the purposes of targeted advertising or any sale of such personal data, through an opt-out preference signal.[24]
- **Data Protection Impact Assessments**: Controllers that control or process the data of at least 100,000 consumers, excluding data controlled or processed solely for completing payment transactions, must regularly conduct a data protection impact assessment (referred to as "data protection assessments" under the law) on the processing of personal data that presents a heightened risk of harm to consumers, including: (1) targeted advertising; (2) the sale of personal data; (3) processing sensitive data; and (4) processing for profiling that presents a reasonably foreseeable risk of unfair or deceptive treatment, unlawful disparate impact, financial or physical injury, reputational injury, intrusion upon seclusion or other substantial injury to consumers.[25] These assessments apply to processing activities that occur **on or after July 1, 2025**, and are not retroactive.[26]

- **De-identified Data**: When in possession of de-identified data, controllers must take reasonable measures to ensure that the data cannot be associated with an individual, publicly commit to processing the data only in a de-identified fashion and contractually obligate any recipients of the data to comply with DPDPA.[27]

*Processor Requirements*

Much like other state privacy laws, processors must assist the controller in meeting its obligations under the law, including its obligations regarding consumer rights requests and security of data processing.[28] All processing must be governed by a contract between the controller and processor that outlines relevant consumer privacy provisions. Under this contract, processors must delete or return all personal data to the controller as requested at the end of the provision of services.[29] Processors must also ensure each person processing personal data is subject to a duty of confidentiality with respect to the data.[30]

## Who Enforces the Law?

Like the majority of state privacy laws, the DPDPA does not provide a private right of action and is solely enforced by the state's office of the attorney general (AG), the Delaware Department of Justice.[31] Until December 31, 2025, the AG must issue notices of violation and give controllers 60 days to cure, prior to initiating an enforcement action.[32] This cure period is not permanent and will sunset on January 1, 2026, after then granting an opporutnity to cure will be at the AG's discretion.[33]

You can learn about the other state laws in Akin's State Data Privacy Law Series, as well as our CCPA Report:

1. Virginia Consumer Data Protection Act: What Businesses Need to Know | Akin (akingump.com)
2. Colorado Privacy Act: What Businesses Need to Know | Akin (akingump.com)
3. Connecticut Data Privacy Act: What Businesses Need to Know | Akin (akingump.com); Businesses and Consumers Prepare as the CTDPA Takes Effect on July 1 | Akin Gump Strauss Hauer & Feld LLP
4. Utah Consumer Privacy Act: What Businesses Need to Know | Akin (akingump.com)

5. Iowa Data Protection Act: What Businesses Need to Know | Akin Gump Strauss Hauer & Feld LLP

6. Tennessee Information Protection Act: What Businesses Need to Know | Akin Gump Strauss Hauer & Feld LLP

7. Texas Data Privacy Act: What Businesses Need to Know | Akin Gump Strauss Hauer & Feld LLP

8. Indiana Data Protection Act: What Businesses Need to Know | Akin Gump Strauss Hauer & Feld LLP

9. Key Takeaways from Akin's CCPA Litigation and Enforcement Report | Akin (akingump.com)

---

1 6 Del. C. § 12D-103(a).

2 *Id.* § 12D-102(21).

3 *Id.* § 12D-102(30).

4 *Id.* § 12D-103(b).

5 "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and their implementing regulations (codified at 45 C.F.R. parts 160 and 164).

6 *Id.* § 12D-103(b)(3).

7 *Id.* § 12D-103(c)(13).

8 *Id.* § 12D-102(8).

9 *Id.* § 12D-103(c)(11).

10 *Id.* § 12D-103(c).

11 *Id.* § 12D-103(c)(1-6).

12 *Id.* § 12D-103(d).

13 *Id.* § 12D-102(29) the DPDPA provides typical exemptions from the definition of "sale," including: (1) the disclosure of personal data to a processor that processes the personal data on behalf of the controller where limited to the purpose of such processing; (2) the disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer; (3) the disclosure or transfer of personal data to an affiliate of the controller or as part of a merger or similar transaction; and (4) other intentional disclosures made by the consumer.

14 *Id.* § 12D-104(a).

15 *Id.* § 12D-104(a)(5).

16 *Id.* § 12D-104(d).

17 *Id.* § 12D-106(a)(1-2).

18 *Id.* § 12D-106(a)(3).

19 *Id.* § 12D-106(a)(4).

20 *Id.* § 12D-106(a)(5).

21 *Id.* § 12D-106(c).

22 *Id.* § 12D-106(d), (e)(1)(a).

23 *Id.* § 12D-107(b).

24 *Id.* § 12D-106(e)(1)(a).

25 *Id.* § 12D-108(a).

26 *Id.* § 12D-108(f).

27 *Id.* § 12D-102(14).

28 *Id.* § 12D-107(a).

29 *Id.* § 12D-107(b)(2) there is an exemption for when retention of the personal data is required by law.

30 *Id.* § 12D-107(b)(1).

31 *Id.* § 12D-111(a).

32 *Id.* § 12D-111(b).

33 *Id.* § 12D-111(c).

## Categories

Cybersecurity, Privacy & Data Protection

Consumer Privacy

Consumer Data Protection

Privacy & Data Protection