Delaware Personal Data Privacy Act Summary

On September 11, 2023, Governor John Carney (D) signed HB 154, the "Delaware Personal Data Privacy Act" (DPDPA) into law. The Act's provisions take effect on January 1, 2025. A non-comprehensive summary of significant elements of the Act follows:

Covered Entities	The **Delaware Personal Data Privacy Act (DPDPA)** applies to persons that conduct business in Delaware or persons that produce products or services that are targeted to the residents of Delaware and that during the preceding calendar year did any of the following: (a) controlled or processed the personal data of not less than 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; (b) 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.
Covered Data	***"Personal information"***: 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. ***"Sensitive data"***: personal data that includes any of the following: (a) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis (including pregnancy), sex life, sexual orientation, status as transgender or nonbinary, citizenship status, or immigration status; (b) genetic or biometric data; (c) personal data of a known child; and (d) precise geolocation data. ***"Genetic data":*** any data regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. "Genetic material" includes deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.
Key Definitions	***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. ***"Dark Pattern":*** a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice or any practice the Federal Trade Commission refers to as a dark pattern. ***"De-Identified Data"***: data that cannot reasonably be used to infer information about or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data does all of the following: (a) take reasonable measures to ensure that such data cannot be associated with an individual; (b) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data; (c) contractually obligates any recipients of such data to comply with all of the provisions of this chapter applicable to the controller with respect to such data. ***"Pseudonymous Data"***: personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual. ***"Targeted Advertising"***: displaying advertisements to a consumer where the advertisement is selected

	based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated internet web sites or online applications to predict such consumer's preferences or interests. ***"Sale of Personal Data"***: the exchange of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include: (a) 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; (b) the disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer; (c) the disclosure or transfer of personal data to an affiliate of the controller; (d) the disclosure of personal data where the consumer directs the controllers to disclose the personal data or intentionally uses the controller to interact with a third party; (e) the disclosure of personal data that the consumer intentionally made available to the general public via a channel of mass media, and did not restrict to a specific audience; and (f) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other similar transaction in which the third party assumes control of all or part of the controller's assets, or a proposed merger, acquisition, bankruptcy or other similar transaction in which the third party assumes control of all or part of the controller's assets.
Consumer Rights	• **Access:** A consumer has 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. • **Affirmative Consent:** A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing data concerning a known child, without first obtaining consent from the child's parent or lawful guardian. • **Correction:** A consumer has 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. • **Deletion**: A consumer has the right to delete personal data provided by, or obtained about, the consumer. • **Portability:** A consumer has the right to obtain a copy of the consumer's personal data 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. • **Third-Parties:** A consumer has the right to obtain a list of the categories of third parties to which the controller has disclosed the consumer's personal data. • **Opt Out Rights**: A consumer has the right to opt out of the processing of the personal data for purposes of: (i) targeted advertising; (ii) the sale of personal data; or (iii) profiling in furtherance of solely automated decisions that produce a legal or similarly significant effect concerning a consumer.
Business Obligations	• **Responding to Consumer Requests**: A controller shall respond to a consumer request without undue delay, but not later than 45 days after the date of receipt of the request. The controller may extend the response period by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial 45-day response period and of the reason for the extension. A consumer has the right to a free response once during any 12-month period. The controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of any denied requests and may charge the consumer a reasonable fee to cover such administrative costs of complying with the request or may decline to act on such requests. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process must be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Within 60

	days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reason for the decisions. 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 contract the Department of Justice to submit a complaint. • **Recognizing Universal Opt-Out Mechanisms**: A consumer may designate an authorized agent to act on the consumer's behalf to opt out of the processing of such consumer's personal data for one or more of the permissible purposes. The consumer may designate such authorized agent by way of, among other things, a platform, technology, or mechanism, including an Internet link or a browser setting, browser extension, or global device setting, indicating such consumer's intent to opt out of such processing. For the purposes of such designation, the platform, technology, or mechanism may function as the agent for purposes of conveying the consumer's decision to opt-out. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf. The Department of Justice may publish or reference on its website a list of agents who presumptively shall have such authority unless the controller has established a reasonable basis to conclude that the agent lacks such authority. • **Data Minimization**: A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer. • **Avoid Secondary Use**: A controller shall 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. • **Data Security**: A controller shall 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. • **No Unlawful Discrimination:** A controller shall not process personal data in violation of the laws of Delaware and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any consumer rights. • **Transparency**: A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes all of the following information: (a) the categories of personal data processed by the controller; (b) the purpose of processing personal data; (c) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request; (d) the categories of personal data that the controller shares with third parties, if any; (e) the categories of third parties with whom the controller shares personal data, if any; and (f) an active electronic mail address or other online mechanism that the consumer may use to contact the controller. • **Purpose Specification:** A controller 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. Personal data may be processed to the extent that such processing is reasonably necessary and proportionate to the listed purposes, and is adequate, relevant, and limited to what is necessary in relation to the specific list purposes. • **Disclosure**: If a controller sells personal data to third parties or processes personal data for targeted advertising a controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.
Data Protection Assessments	A controller that controls or processes the data of at least 100,000 consumers, excluding data controlled or processed solely for the purpose of completing a payment transaction, shall conduct and document, on a regular basis, a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. Data protection assessments must

	identify and weigh the benefits that may flow, directly or indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing as mitigated by safeguard that can be employed by the controller to reduce such risks. The controller must factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed. The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general. Data protection assessment requirements shall apply to processing activities created or generated on or after six months following the DPDPA effective date and are not retroactive.
Controller / Processor Distinction	• **A processor shall adhere to the instructions of a controller and shall assist the controller** in meeting the controller's obligations under the DPDPA. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. • The contract must include requirements that the processor: (a) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (b) at the controller's direction, delete or return all personal information to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law; (c) upon the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance; (d) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data; and (e) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the Act's obligations, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.
Exceptions and Exemptions	• A controller that discloses pseudonymous or deidentified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breach of those contractual commitments. The determination of the reasonableness of such oversight and the appropriateness of contractual enforcement must take into account whether the disclosed data includes data that would be sensitive data if it were re-identified. • DPDPA shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) cooperate with law enforcement agencies concerning conduct that the controller or processor reasonably and in good faith believes may violate, federal, state, or local laws, rules, or regulations; (d) prepare for and defend legal claims; (e) provide a product or service requested by a consumer; (e) protect interests essential for life or physical safety of the consumer; (f) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty; (g) take immediate steps to protect and interest that is essential for the life and physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis; (h) prevent, detect and protect against security incidents; (g) preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security; (h) engage in scientific or statistical research in the public interest. • Data exempt from DPDPA includes: protected information under the Health Care Quality

	Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, any licensed insurance company, any nonprofit organization dedicated exclusively to preventing and addressing insurance crime, and COPPA.
Enforcement	• DPDPA does not establish a private cause of action. The Department of Justice has enforcement authority over the DPDPA and may investigate and prosecute violations. • **Right to Cure**: Between January 1, 2025 and December 31, 2025, the Department of Justice shall, prior to initiating any action for a violation, issue a notice of violation to the controller if the Department of Justice determines that a cure is possible if the controller fails to cure such a violation with 60 days of receipt of the notice of violation, the Department of Justice may bring an enforcement proceeding. Beginning on January 1, 2026, the Department of Justice may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation, may consider all of the following: (a) the number of violations; (b) the size and complexity of the controller or processor; (c) the nature and extent of the controller's or processor's processing activities; (d) the substantial likelihood of injury to the public; (e) the safety of persons or property; (f) whether such alleged violation was likely caused by human or technical error; (g) the extent to which the controller or processor has violated this or similar laws in the past.