SPONSOR: Rep. Griffith & Rep. Harris & Rep. Bush & Rep. Gorman & Rep. Heffernan & Rep. K. Johnson & Rep. Lambert & Rep. Morrison & Rep. Neal & Rep. Phillips & Rep. Romer & Rep. Berry & Sen. Pinkney & Sen. Lockman & Sen. Cruce & Sen. Seigfried & Sen. Sturgeon & Sen. Hansen
Reps. Minor-Brown, Osienski, Bolden, Burns, Carson, Chukwuocha, Cooke, Lynn, Ross Levin; Sens. Sokola, Townsend, Hoffner, Poore, Huxtable, Walsh

HOUSE OF REPRESENTATIVES
153rd GENERAL ASSEMBLY

HOUSE BILL NO. 380
AS AMENDED BY
HOUSE AMENDMENT NO. 2

AN ACT TO AMEND TITLE 6 OF THE DELAWARE CODE RELATING TO PERSONAL DATA PRIVACY.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

Section 1. Amend Chapter 12D, Subtitle II, Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows and by redesignating accordingly:

§ 12D-102. Definitions.

For purposes of this chapter, the following definitions shall apply:

( ) "Adverse action" means any denial, cancellation, unfavorable change, increase in charge, exclusion of benefit, or other action adverse to the interests of a consumer or resident in connection with a decision that produces legal or similarly significant effects.

~~(13)~~ ( ) "Decisions that produce legal or similarly significant ~~effects concerning the consumer~~" effects" means decisions ~~made by the controller~~ that result in the provision or denial ~~by the controller~~ of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

~~(28)~~ ( ) "Publicly available information" means any of the following:

b. Information that a controller has a reasonable basis to believe that the consumer has lawfully made available to the general public through widely distributed ~~media.~~ media and that does not include biometric data that can be associated with a specific consumer that was collected without the consumer's consent.

( ) "Report" means any written, oral, or other communication of any personal data by a controller or processor, including recommendations, summaries, or automated decisions based on personal data or profiling.

( ) "Resident" means any natural person residing in the State.

~~(29)~~ ( ) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include any of the following:

b. The disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer. consumer, except that the disclosure of sensitive data for monetary or other valuable consideration by the controller to a third party must comply with § 12D-106(a)(2) of this title.

~~(30)~~ ( ) "Sensitive data" means personal data that includes any of the ~~following:~~ following, and includes inferences made based on personal data, alone or in combination with other data, that are used to reveal or identify any of the following:

a. Data ~~revealing racial~~ that reveals or identifies racial, national, or ethnic origin, religious beliefs, mental or physical health ~~condition or diagnosis~~ condition, diagnosis, treatment, or status (including pregnancy), sex life, sexual orientation, treatment or status as transgender or nonbinary, citizenship status, or immigration status.

e. Neural data that is generated by measuring the activity of an individual's central nervous system.

f. A consumer's financial account number, financial account log-in information, or credit card or debit card number that, alone or in combination with any required access or security code, password, or credential, would allow access to a consumer's financial account.

g. A government-issued identification number, including a Social Security number, passport number, state identification card number, or driver's license number, that applicable law does not require to be publicly displayed.

~~(34)~~ ( ) "Third party" means, with respect to personal data controlled by a controller, any person other than the relevant consumer, the controller of such personal data, or a processor or an affiliate of the processor or the ~~controller.~~ controller, except for entities listed under § 12D-103(b) of this title.

§ 12D-103. Applicability of chapter.

(a) This chapter applies to persons that conduct business in the State or persons that produce products or services that are targeted to residents of the State and that during the preceding calendar year did any of the following:

(1) Controlled or processed the personal data of not less than ~~35,000~~ 10,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction.

(2) Controlled or processed the personal data of not less than ~~10,000~~ 5,000 consumers and derived more than 20% of their gross revenue from the sale of personal data.

(3) Third parties who acquire personal data from a controller.

(b) This chapter does not apply to any of the following entities:

(2) ~~Any financial institution or affiliate of a financial institution, all as defined in 15 U.S.C. § 6809, to the extent that the financial institution or affiliate is subject to Title V of the Gramm Leach Bliley Act (15 U.S.C. § 6801, et seq., as amended) and the rules and implementing regulations promulgated thereunder.~~ Any insurer, insurance company, insurance producer, surplus lines broker, third-party administrator of self-insurance, health carrier, health services corporation, insurance-support organization, or insurance agent, or any affiliate or subsidiary thereof that is principally engaged in financial activities as described in 12 U.S.C. § 1843(k).

(5) Any federal or state chartered bank, credit union, savings association, or any affiliate or subsidiary thereof that is principally engaged in financial activities as described in 12 U.S.C. § 1843(k).

(6) Any agent, broker-dealer, investment adviser, or investment adviser representative, as defined under § 73-203 of Title 6, who is regulated by the Delaware Investor Protection Unit or the Securities and Exchange Commission.

(c) This chapter does not apply to the following information and data:

(11) Data processed or maintained in any of the following ways:

a. 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.~~ role, except for personal data processed in connection with profiling and reports under § 12D-106(f) of this title.

(15) Information created specifically for and collected and maintained by a manufacturer, as defined under 21 C.F.R. 820.3(o), when collected, used, or disclosed for treatment, payment, or health care operations purposes as specified under the Health Insurance Portability and Accountability Act of 1996.

(16) Information created for purposes of the Federal Health Care Quality Improvement Act of 1986 and related regulations.

(17) Information derived from protected health information regulated under the Health Insurance Portability and Accountability Act of 1996 or the Federal Policy for the Protection of Human Subjects under 45 C.F.R. Part 46, and deidentified as provided under 45 C.F.R. § 164.514.

(18) Information included in a Limited Data Set as described under 45 CFR § 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified under 45 CFR § 164.514(e).

§ 12D-104. Consumer personal data rights.

(a) A consumer has the right to do all of the following:

(1) Confirm whether a controller is processing the consumer's personal data and access such personal data, including any inferences about the consumer derived from such personal data and whether a controller or processor is

processing a consumer's personal data for the purpose of profiling to make a decision that produces any legal or similarly significant effect concerning the consumer, unless such confirmation or access would require the controller to reveal a trade secret.

(4) 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~~ the controller ~~shall not be~~ is not required to reveal any trade secret.

(5) Obtain a list of ~~the categories of~~ third parties to which the controller has disclosed the consumer's personal ~~data.~~ data unless any of the following apply:

a. The disclosed personal data is pseudonymous data.

b. The controller cannot compile such a list with reasonable effort, in which case the controller must disclose all third parties to which the controller discloses personal data.

c. The listing of a third party would reveal a trade secret.

(6) Opt out of the processing of the personal data for purposes of any of the following:

c. Profiling in furtherance of ~~solely-automated~~ automated decisions that produce legal or similarly significant effects concerning the consumer.

(c) Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights ~~authorized pursuant to said sections~~ under this chapter as follows:

(6) Notwithstanding the right of access provided in paragraph (a)(1) of this section, a controller may not disclose the following personal data in response to a consumer's request and may only inform the consumer or the person exercising such right on behalf of the consumer, with sufficient particularity, that the controller processes any of the following personal data:

a. The consumer's Social Security number.

b. The consumer's driver's license number, state identification card number, or other government-issued identification number.

c. The consumer's financial account number.

d. The consumer's health insurance identification number or medical identification number.

e. The consumer's account password.

f. The consumer's security question or answer thereto.

g. The consumer's biometric data.

§ 12D-106. Duties of controllers.

(a) A controller shall do all of the following:

(1) Limit the ~~collection~~ processing of personal data to what is ~~adequate, relevant, and~~ reasonably necessary and proportional in relation to the purposes for which such data is processed, as disclosed to the consumer.

(2) Except as otherwise permitted by this chapter, not process personal data for any additional ~~purposes~~ purpose that ~~are neither~~ is not reasonably necessary ~~to, nor compatible with,~~ and proportionate to the disclosed purposes for which such personal data is processed, as disclosed to the ~~consumer,~~ consumer at the time of collection, unless the controller obtains the consumer's consent.

(3) Establish, implement, and maintain reasonable administrative, technical, and physical data security and privacy practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

(4) Not process sensitive data concerning a consumer ~~without obtaining the consumer's consent, or, in~~ unless all of the following conditions are met:

a. The consumer consents to the processing of sensitive data.

b. The processing of sensitive data is reasonably necessary and proportionate to the disclosed purposes for processing sensitive data.

(5) ~~the case of the processing of sensitive data concerning a known child,~~ Not process personal data of a consumer when the controller has actual knowledge or wilfully disregards that the consumer is a child, without first obtaining consent from the child's parent or lawful guardian and otherwise complying with § 1204C of this title.

~~(5)~~ (6) Not process personal data or engage in profiling in violation of the laws of this State and federal laws that prohibit unlawful discrimination. Evidence or lack of evidence concerning proactive anti-bias testing or any similar proactive effort to avoid processing personal data in violation the laws of this State, including evidence or lack of evidence concerning the quality, efficacy, recency, and scope of any such testing or effort, the results of such testing or effort, and the response to the results of such testing or effort, are relevant to any claim for a violation of the laws of this State and any available defense to such claims.

~~(6)~~ (7) Provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than 15 days after the receipt of such request.

~~(7)~~ (8) 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,~~ without the consumer's consent for any purpose listed in § 12D-104(a)(6) of this title under circumstances where a controller has actual knowledge or wilfully disregards that the consumer is at least 13 years of age but younger than 18 years of age.

~~(8)~~ (9) Not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, 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.

(10) Enter into binding contractual agreements with third parties to whom personal data is disclosed, including in a sale of personal data or for targeted advertising. The contractual agreement must include all of the following terms and conditions:

a. Specifying that the personal data is sold or disclosed by the controller only for limited and specified purposes, including whether the purpose includes use for decisions that produce legal or similarly significant effects.

b. Obligating the third party to comply with this chapter and obligating the third party to provide the same level of privacy protection as is required by this chapter.

c. Granting the controller rights to take reasonable and appropriate steps to ensure that the third party uses the personal data transferred by the controller in a manner consistent with the controller's obligations under this chapter.

d. Requiring the third party to notify the controller if it makes a determination that it can no longer meet its obligations under this chapter.

e. Granting the controller the right upon notice to take reasonable and appropriate steps to stop and remediate unauthorized use of personal data.

(11) Conduct reasonable due diligence, either by the controller or through a designated assessor, of third parties to whom the controller discloses personal data, including the sale of personal data and targeted advertising, to assess the third party's policies and technical and organizational measures undertaken to support compliance with the obligations under this chapter and to demonstrate compliance under this chapter as it relates to the personal data that the controller discloses to the third party or that the controller anticipates disclosing to third party. Reasonable due diligence involves, at a minimum, assessing the third party through the use of questionnaires and review of relevant documents of the third party. Additional reasonable measures must be undertaken in a manner that is commensurate with the sensitivity of the data disclosed by the controller to the processor or third party.

(12) Not disclose sensitive data in a sale of personal data unless all of the following apply:

a. The disclosure of sensitive data is strictly necessary to provide or maintain a product or service affirmatively requested by the consumer to whom the sensitive data pertains.

b. The controller provides a clear and conspicuous notice of the sale of personal data before the sale of personal data, which must include the specific categories of sensitive data to be disclosed, the purpose of the disclosure, and identifies the third parties to which sensitive data will be disclosed.

c. The controller obtains the consumer's consent.

d. The controller maintains a record of the consumer's consent for a period of 5 years.

e. The record of consent of Delaware consumers must be provided with any data protection assessment produced under § 12-108(c) of this title.

(c) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice reasonably particular to the product or service offered to the consumer that includes all of the following:

(6) ~~An~~ Identification of the controller and an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

(7) A description of the consumer personal data rights under § 12D-104(a) of this title.

(d) If a controller ~~sells personal data to third parties or processes personal data for targeted advertising,~~ processes personal data for any purpose under § 12D-104(a)(6) of this title, the controller ~~shall~~ must 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.

(e) (1) A controller shall establish, and shall describe in the privacy notice required by subsection (c) of this section, 1 or more secure and reliable means for consumers to submit a request to exercise their consumer rights ~~pursuant to~~ under this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to verify the identity of the consumer making the request. A controller ~~shall~~ may not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer or the consumer's authorized agent to use an existing account. Any such means shall include all of the following:

a.1. Providing a clear and conspicuous link on the controller's Internet website or application to an Internet web page or interface that enables a consumer, or an agent of the consumer, to opt out of ~~the targeted advertising or the sale of the consumer's personal data.~~ the processing of personal data for any purpose listed in § 12D-104(a)(6) of this title.

(f) A controller disclosing to any third party a report for use in connection with any decision that produces legal or similarly significant effects concerning a resident must:

(1) In addition to the requirements of §12D-106(a)(10) of this title, enter into a contractual agreement with the third party requiring the third party to do the following:

a. Provide notice to a resident of any adverse action that is based in whole or in part on any information contained in the report.

b. Provide a description of the personal data relied upon in making the adverse action.

c. Include a statement that the resident may obtain the information described under paragraph (f)(2) of this section from the controller with appropriate contact information for the controller.

d. Include a statement that the resident may request the third party, where technically feasible, perform a human review of the adverse action concerning the resident, unless providing the opportunity for review is not in the best interest of the resident, including instances in which any delay might pose a risk to the life or safety of the resident.

(2) Upon request from a resident, provide the following information within 30 days:

a. Personal data maintained by the controller concerning the resident at the time of the request.

b. The source of the personal data used in profiling.

c. Identification of all third parties who obtained a report concerning the resident within the previous 24-months.

(3) Provide the resident an opportunity to correct any incorrect personal data.

(g) Nothing in subsection (f) of this section applies to a controller or third party when the report or personal data consists of a score, a model, an algorithm, or similar output that is a consumer report, or would be a consumer report if furnished to a third party, and is furnished or disclosed in compliance with the Fair Credit Report Act, 15 U.S.C. § 1681 et. seq.

§ 12D-107. Duties of processors.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Such assistance must include all of the following:

(4) Providing necessary information for the controller or the controller's designated assessor to assess the processor in order to conduct due diligence.

(b) A contract between a controller and a processor must 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 also require that the processor do all of the following:

(3) Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this ~~chapter.~~ chapter and cooperate with reasonable assessments by the controller or the controller's designated assessor in order to conduct due diligence.

(6) Identify each limited and specific purpose for which the processor is processing personal data. The contract must specify that the controller is disclosing the personal data to the processor only for the limited and specific purposes set forth within the contract. The specific purposes may not be described in generic terms, such as referencing the entire contract generally, but must be described with specificity and particularity.

§ 12D-107A. Duties of third parties.

(a) A third party that receives personal data from a controller or processor and does not have a contract as required by this chapter may not further process personal data disclosed to the third party.

(b) A third party must comply with the terms of any contract required by this chapter.

(c) A third party must provide necessary information to enable the controller to conduct and document data protection assessments as required under this chapter.

(d) A third party must provide necessary information for the controller or the controller's designated assessor to assess the third party consistent with § 12D-106(a)(11) of this title.

(e) A third party subject to this chapter under § 12D-103(a)(1) or (2) of this title must comply with all provisions of this chapter.

§ 12D-108. Data protection assessments.

(a) A controller that ~~controls or~~ processes the data of not less than ~~100,000~~ 50,000 consumers, excluding data controlled or processed solely for the purpose of completing a payment transaction, ~~shall~~ must do the following:

(1) ~~conduct~~ 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. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes any of the following:

~~(1)~~ a. The processing of personal data for the purposes of targeted advertising.

~~(2)~~ b. The sale of personal data.

~~(3)~~ c. The processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of any of the following:

~~a.~~ 1. Unfair or deceptive treatment of, or unlawful disparate impact on, consumers.

~~b.~~ 2. Financial, physical, or reputational injury to consumers.

~~c.~~ 3. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person.

~~d.~~ 4. Other substantial injury to consumers.

~~(4)~~ d. The processing of sensitive data.

(2) Conduct and document, on a regular basis, an impact assessment if a controller engages in profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning a consumer. The impact assessment must include, to the extent reasonably known by or available to the controller, as applicable:

a. A statement by the controller disclosing the purpose, intended use cases, deployment context of, and benefits afforded by, such profiling.

b. An analysis of whether profiling poses any known or reasonably foreseeable heightened risk of harm to a consumer, and, if so, a description of both of the following:

1. The nature of the heightened risk of harm to a consumer.

2. The steps that have been taken to mitigate the heightened risk of harm to a consumer.

c. A description of the main categories of personal data processed as inputs for the purposes of profiling and the outputs the profiling produces.

d. An overview of the main categories of personal data the controller used to customize profiling, if the controller used personal data to customize profiling.

e. Any metrics used to evaluate the performance and known limitations of profiling.

f. A description of any transparency measures taken concerning the use of profiling, including any measures taken to disclose to consumers that the controller is engaged in profiling while the controller is engaged in profiling.

g. A description of the post-deployment monitoring and user safeguards provided concerning profiling, including the oversight, use, and learning processes established by the controller to address issues arising from profiling.

(c) The Attorney General may require that a controller disclose any data protection assessment conducted in compliance with this chapter or conducted for the purpose of complying with another applicable law or regulation that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with

the responsibilities set forth in this chapter. Data protection assessments must be treated as confidential and are not public records within the meaning of § 10002(o) of Title 29. Notwithstanding the foregoing, a controller's data protection assessment may be used in an action to enforce this chapter. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes and conspicuously identifies information subject to attorney-client privilege or work product protection, such disclosure by itself does not constitute a waiver of such privilege or protection.

§ 12D-109. De-identified data.

(d) A controller that discloses pseudonymous data or de-identified data ~~shall~~ must exercise reasonable oversight to monitor ~~compliance with any~~ compliance, including entering contractual commitments to ~~which the~~ ensure the proper and limited use of pseudonymous data or de-identified ~~data is subject~~ data, and ~~shall~~ must take appropriate steps to address any breaches 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.

§ 12D-110. Exclusions.

(c) The obligations imposed on controllers or processors under this chapter ~~shall~~ do not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this State. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this State as part of a privileged communication.

(d) A controller or processor that discloses personal data to a processor or third-party controller in compliance with this chapter ~~shall~~ may not be deemed to have violated this chapter if the processor or third-party controller that receives and processes such personal data violates this chapter, provided ~~that:~~ all of the following apply:

(1) At the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller had violated or would violate this ~~chapter; and~~ chapter.

(3) The disclosing controller or processor undertook reasonable diligence and oversight to ensure compliance with contractual commitments to which the disclosed personal data is subject.

(e) A third-party controller or processor receiving personal data from a controller or processor in compliance with this chapter is ~~likewise~~ not in violation of this ~~chapterfor~~ chapter for the independent misconduct of the controller or processor from which such third-party controller or processor receives such personal data.

~~(e)~~ (f) Nothing in this chapter may be construed to do any of the following:

~~(f)~~ (g) Personal data processed pursuant to this section may be processed to the extent that such processing is reasonably necessary and proportionate to the purposes listed in this section, and is adequate, relevant, and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used, or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

~~(g)~~ (h) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in ~~subsection (f)~~ subsection (g) of this section.

~~(h)~~ (i) Processing personal data for the purposes expressly identified in this section ~~shall~~ does not solely make a legal entity a controller with respect to such processing.

§ 12D-111. Enforcement.

(c) 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 of any provision of this chapter, ~~may~~ consider all of the following:

(e) A violation of this chapter shall be deemed an unlawful practice under § 2513 of this title and a violation of subchapter II of Chapter 25 of this title, and shall be enforced solely by the Department of Justice.

Section 2. This Act is effective January 1, 2027.