ROS

L.D. 1977

Date: 4/16/24 MAJORITY (Filing No. H-975)

JUDICIARY

Reproduced and distributed under the direction of the Clerk of the House.

STATE OF MAINE

HOUSE OF REPRESENTATIVES

131ST LEGISLATURE

SECOND REGULAR SESSION

COMMITTEE AMENDMENT "A" to H.P. 1270, L.D. 1977, "An Act to Create the Data Privacy and Protection Act"

Amend the bill by striking out the title and substituting the following:

'An Act to Enact the Maine Data Privacy and Protection Act'

Amend the bill by striking out everything after the enacting clause and inserting the following:

'**Sec. 1. 10 MRSA c. 1057** is enacted to read:

CHAPTER 1057

MAINE DATA PRIVACY AND PROTECTION ACT

§9601. Short title

This chapter may be known and cited as "the Maine Data Privacy and Protection Act."

§9602. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. Affiliate. "Affiliate" means a business or nonprofit organization that shares common branding with another business or nonprofit organization or controls, is controlled by or is under common control with another business or nonprofit organization.

2. Biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, retina, iris or other unique biological pattern or characteristic that is capable of being used to identify a specific individual. "Biometric data" does not include:

A. A digital or physical photograph;

ROS

B. An audio or video recording; or

C. Any data generated from a digital or physical photograph or an audio or video recording, unless the data is generated to identify a specific individual.

3. Business associate. "Business associate" has the same meaning as in 45 Code of Federal Regulations, Section 160.103.

4. Child. "Child" means an individual who has not attained 13 years of age.

5. Consent. "Consent" means 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, that is made in the language that the consumer uses to obtain a product or service from the controller and in a format that is reasonably accessible to and usable by consumers with disabilities. "Consent" does not include:

A. Acceptance of a terms of use document or similar document that contains descriptions of personal data processing along with other unrelated information;

B. Hovering over, muting, pausing or closing a given piece of content; or

C. Agreement obtained through the use of a dark pattern.

6. Consumer. "Consumer" means an individual who is a resident of this State. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit organization or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit organization or government agency.

7. Consumer health data. "Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis.

8. Control. "Control" means:

A. Ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a company;

B. Control in any manner over the election of a majority of the directors of a company or of individuals exercising similar functions in a company; or

C. Power to exercise controlling influence over the management of a company.

9. Controller. "Controller" means a person that, alone or jointly with other persons, determines the purpose and means of processing personal data.

10. Covered entity. "Covered entity" has the same meaning as in 45 Code of Federal Regulations, Section 160.103.

11. Dark pattern. "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice and includes, but is not limited to, any practice the Federal Trade Commission refers to as a "dark pattern."

12. De-identified data. "De-identified data" means 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 an individual, if the controller that possesses the data:

A. Takes reasonable measures to ensure that the de-identified data cannot be associated with an individual;

B. Publicly commits to process the de-identified data only in a de-identified fashion and not attempt to re-identify the data; and

C. Contractually obligates recipients of the de-identified data to satisfy the criteria set forth in paragraphs A and B.

13. Decisions that produce legal or similarly significant effects concerning the consumer. "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions that result in the provision or denial to the consumer 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.

14. Geofence. "Geofence" means technology that uses global positioning system coordinates, cellular tower connectivity, cellular data, radio frequency identification, wireless access point data or any other form of location detection to establish a virtual perimeter around a specific physical location.

15. Institution of higher education. "Institution of higher education" means a person that is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

16. Minor. "Minor" means an individual who has not attained 18 years of age.

17. Nonprofit organization. "Nonprofit organization" means an organization that is exempt from taxation under Section 501(c)(3), Section 501(c)(4), Section 501(c)(6) or Section 501(c)(12) of the United States Internal Revenue Code of 1986, as amended.

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

19. Precise geolocation data. "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include:

A. The content of communications; or

B. Data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

20. Process. "Process" means an operation or set of operations performed on personal data, including the collection, use, storage, transfer, analysis, deletion or modification of personal data.

21. Processor. "Processor" means a person that processes personal data on behalf of a controller.

22. Profiling. "Profiling" means any form of automated process performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

23. Protected health information. "Protected health information" has the same meaning as in the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act.

24. Pseudonymous data. "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, as long as the additional information is kept separately from the personal data and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

25. Publicly available information. "Publicly available information":

A. Means information that has been lawfully made available to the general public from:

(1) Federal, state or local government records;

(2) Widely distributed media;

(3) A website or online service made available to all members of the public, either for free or for a fee, including a website or online service in which all members of the public can log on to the website or online service either for free or for a fee, unless the individual who made the information available via the website or online service has restricted the information to a specific audience;

(4) A disclosure that has been made to the general public as required by federal, state or local law; or

(5) The visual observation of the physical presence of an individual or a device located in a public place, not including data collected by a device in the individual's possession; and

B. Does not include:

(1) Any obscene visual depiction as described in 18 United States Code, Section 1460;

(2) Biometric data;

(3) Genetic information, unless the genetic information has been made available to the general public by the individual to whom the genetic information pertains;

(4) Inferences derived from a combination of publicly available information and other personal data; or

(5) Intimate images a controller or processor knows have been created or shared without consent of the individual depicted in the images. For purposes of this subparagraph, "intimate image" means a photograph, videotape, film or digital

ROS

recording of an individual in a state of nudity or engaged in a sexual act or engaged in sexual contact for which there is no public or newsworthy purpose.

26. Sale of personal data. "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a 3rd party. "Sale of personal data" does not include:

A. The transfer of personal data to a processor that processes the personal data on behalf of the controller;

B. The transfer of personal data to a 3rd party for purposes of providing a product or service requested by the consumer;

C. The transfer of personal data to an affiliate of the controller;

D. The transfer of personal data when the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a 3rd party;

E. The transfer of personal data that the consumer:

(1) Intentionally made available to the general public via a channel of mass media; and

(2) Did not restrict to a specific audience; or

F. The transfer of personal data to a 3rd party as an asset that is part of a merger, acquisition, bankruptcy or other transaction or a proposed merger, acquisition, bankruptcy or other transaction in which the 3rd party assumes control of all or part of the controller's assets.

27. Sensitive data. "Sensitive data" means personal data that includes:

A. Data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions or diagnoses, sexual orientation, gender identity or citizenship or immigration status;

B. Genetic or biometric data;

C. Consumer health data;

D. Personal data collected from a consumer known to be a minor;

E. Precise geolocation data;

F. A social security number, driver's license number or nondriver identification card number;

G. Billing, financial or payment method information, except that "sensitive data" does not include the last 4 digits of a debit card or credit card number;

H. Account or device log-in credentials or security or access codes, including passwords, for an account or device; or

I. Data concerning an individual's status as a victim of a crime. For the purposes of this paragraph, "victim" has the same meaning as in Title 17-A, section 2101, subsection 2.

28. Targeted advertising. "Targeted advertising" means displaying an advertisement to a consumer or on any device reasonably linkable to a consumer when the advertisement

is selected in response to the consumer's request for information or feedback or based on personal data obtained or inferred:

A. From the consumer's activities within a controller's own publicly accessible websites or online applications; or

B. Based on the context of a consumer's current search query, visit to a publicly accessible website or online application.

"Targeted advertising" does not include processing personal data solely to measure or report advertising frequency, performance or reach.

29. Third party. "Third party" means a person, such as a public authority, agency or body, other than the consumer, the controller or the processor or an affiliate of the controller or the processor.

30. Trade secret. "Trade secret" has the same meaning as in Title 10, section 1542, subsection 4.

31. Transfer. "Transfer" means to disclose, release, disseminate, make available, license, rent or share personal data orally, in writing, electronically or by any other means. For purposes of this chapter, the transfer of personal data does not include the sale of personal data.

§9603. Scope

1. Applicability; July 1, 2025 to December 31, 2026. Beginning July 1, 2025 and until December 31, 2026, the provisions of this chapter apply to persons that conduct business in this State or persons that produce products or services that are targeted to residents of this State and that during the preceding calendar year:

A. Controlled or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

B. Controlled or processed the personal data of not less than 10,000 consumers and derived more than 20% of gross revenue from the sale of personal data.

2. Applicability; beginning January 1, 2027. Beginning January 1, 2027, the provisions of this chapter apply to persons that conduct business in this State or persons that produce products or services that are targeted to residents of this State and that during the preceding calendar year:

A. Controlled or processed the personal data of not less than 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

B. Controlled or processed the personal data of not less than 10,000 consumers and derived more than 20% of gross revenue from the sale of personal data.

3. Exempt entities. The provisions of this chapter do not apply to:

A. A body, authority, board, bureau, commission, district or agency of this State, a political subdivision of this State or a federally recognized Indian tribe in this State;

ROS

B. An organization that is exempt from taxation under Section 501(c)(3), Section 501(c)(4), Section 501(c)(6) or Section 501(c)(12) of the United States Internal Revenue Code of 1986, as amended;

C. An institution of higher education;

D. A national securities association that is registered under the federal Securities Exchange Act of 1934, 15 United States Code, Section 78a et seq.;

E. A supervised financial organization or a service corporation. For purposes of this paragraph, "supervised financial organization" has the same meaning as in Title 9-A, section 1-301, subsection 38-A and "service corporation" has the same meaning as in Title 9-B, section 131, subsection 37;

F. A health care facility, a health care practitioner or an affiliate of a health care facility or health care practitioner that qualifies both as a business associate of that health care facility or health care practitioner and provides services only to covered entities. For purposes of this paragraph, "health care facility" and "health care practitioner" have the same meaning as in Title 22, section 1711-C, subsection 1, paragraphs D and F, respectively;

G. A person or entity that qualifies as a "licensee" under Title 24-A, section 2263, subsection 8, to the extent the person or entity is in compliance with any applicable data security and data privacy requirements of Title 24-A; or

H. A person or entity that is a provider of broadband Internet access service as defined in Title 35-A, section 9301, but only to the extent that the person or entity is providing broadband Internet access service.

4. Exempt data. The provisions of this chapter do not apply to:

A. Nonpublic personal information regulated under and collected, processed, sold or disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act, 15 United States Code, Section 6801 et seq. (1999);

B. Protected health information under the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

C. Patient-identifying information as described in 42 United States Code, Section 290dd-2;

D. Identifiable private information for the protection of human subjects in research under 45 Code of Federal Regulations, Part 46;

E. Identifiable private information that is otherwise information collected as part of human subjects in research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or successor organization;

F. The protection of human subjects in research under 21 Code of Federal Regulations, Parts 50 and 56, or personal data used or shared in research, as defined in 45 Code of Federal Regulations, Section 164.501, that is conducted in accordance with the standards set forth in paragraphs D and E, or other research conducted in accordance with applicable law;

ROS

G. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 United States Code, Section 11101 et seq.;

H. Information derived from health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

I. Information that originates from information described in paragraphs B to H, or information that is intermingled so as to be indistinguishable from information described in paragraphs B to H, that a covered entity, business associate or program or activity relating to substance use disorder as described in 42 United States Code, Section 290dd-2, creates, processes or maintains in the same manner as is required under the applicable laws and regulations cited in paragraphs B to H;

J. Information used for public health activities and purposes as authorized by the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

K. The collection, maintenance, disclosure, sale, communication or use of personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 United States Code, Section 1681 et seq.;

L. Personal data collected, processed, sold or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 United States Code, Section 2721 et seq.;

M. Personal data regulated by the federal Family Educational Rights and Privacy Act of 1974, 20 United States Code, Section 1232g et seq.;

N. Personal data collected, processed, sold or disclosed in compliance with the federal Farm Credit Act of 1971, 12 United States Code, Section 2001 et seq.;

O. Data processed or maintained:

(1) In the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or 3rd party, to the extent that the data is collected and used within the context of that role;

(2) As the emergency contact information of an individual under this chapter used for emergency contact purposes; or

(3) That is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under paragraph A and used for the purposes of administering those benefits; or

P. Personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the federal Airline Deregulation Act of 1978, 49 United States Code, Section 40101 et seq., by an air carrier subject to that Act, to the

extent this chapter is preempted by the federal Airline Deregulation Act of 1978, 49 United States Code, Section 41713.

4. Compliance with the federal Children's Online Privacy Protection Act of 1998. Controllers and processors that comply with the verifiable parental consent requirements of the federal Children's Online Privacy Protection Act of 1998, 15 United States Code, Section 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act are compliant with an obligation to obtain parental consent pursuant to this chapter.

§9604. Consumer rights

1. Consumer rights. A consumer has a right to:

A. Confirm whether or not a controller is processing the consumer's personal data and to access that personal data, unless confirmation or access would require the controller to reveal a trade secret;

B. 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;

C. Delete personal data provided by, or obtained about, the consumer;

D. 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, when the processing is carried out by automated means, as long as the controller is not required to reveal a trade secret; and

E. Opt out of the processing of the consumer's personal data for purposes of:

(1) Targeted advertising;

(2) The sale of personal data, except as provided in section 9606, subsection 4; or

(3) Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

2. Exercise of consumer rights. A consumer may communicate and access the information necessary to exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A controller may not condition, attempt to condition or effectively condition a consumer's exercise of the rights under this section through the use of any false, fictitious, fraudulent or materially misleading statement or representation or through the use of a dark pattern. A consumer may designate an authorized agent in accordance with section 9605 to exercise the consumer's rights.

3. Responding to exercise of consumer rights. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer's rights authorized pursuant to this chapter as follows.

A. A controller shall respond to the consumer without undue delay, but not later than the 45th day after receipt of the request. The controller may extend the response period by 45 days when reasonably necessary considering the complexity and number of the consumer's requests, as long as the controller informs the consumer of the extension within the initial 45-day response period and of the reason for the extension.

B. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than the 45th day after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

C. The controller shall provide information in response to a consumer's request, free of charge, once per consumer during any 12-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

D. If a controller is unable to authenticate a request to exercise a right afforded under subsection 1 using commercially reasonable efforts, the controller is not required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the right. A controller is not required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes the request is fraudulent, the controller shall send a notice to the person who made the request disclosing that the controller believes the request is fraudulent, explaining why the controller believes the request is fraudulent and explaining that the controller will not comply with the request.

E. A controller that has obtained personal data about a consumer from a source other than the consumer is in compliance with a consumer's request to delete that data pursuant to subsection 1, paragraph C by:

(1) Retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted from the controller's records and not using the retained data for any other purpose pursuant to the provisions of this chapter; or

(2) Opting the consumer out of the processing of the personal data obtained from a source other than the consumer for any purpose except for any purpose exempt from the restrictions of this chapter under section 9611.

4. Appeals. A controller shall establish a process for a consumer to appeal the controller's inaction 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. Not later than the 60th day after receipt of an appeal, a controller shall inform the consumer in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons 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 contact the Attorney General to submit a complaint.

§9605. Authorized agent

A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to exercise the consumer's rights under this chapter. The consumer may designate an authorized agent by way of, among other methods, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating the consumer's intent to opt out of certain processing of the consumer's data.

In the case of processing personal data of a consumer known to be a child, the parent or legal guardian may exercise consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise rights on the consumer's behalf.

A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, using commercially reasonable efforts, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

§9606. Actions of controllers

1. Data minimization. A controller shall comply with the requirements of this subsection.

A. A controller shall limit the processing of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains.

B. A controller shall limit the processing of sensitive data to what is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the data pertains.

C. A controller may not collect biometric data concerning a consumer without obtaining the consumer's consent.

D. Except as otherwise provided in this chapter, a controller may not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer.

A controller is not required to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain.

2. Duties. A controller shall:

A. In the case of the processing of sensitive data concerning a consumer known to be a child, process the data in accordance with the federal Children's Online Privacy Protection Act of 1998, 15 United States Code, Section 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act; and

B. 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 the consent, cease to process the data as soon as practicable, but not later than 15 days after the receipt of the request.

3. Prohibitions. A controller may not:

A. When the controller, under the circumstances, has actual knowledge or willfully disregards that the consumer is a minor;

(1) Process the personal data of the consumer for purposes of targeted advertising; or

(2) Sell the consumer's personal data without the consumer's consent; or

B. Retaliate against a consumer for exercising a consumer right in this chapter or for not agreeing to the collection or processing of personal data for a separate product or service, including by 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.

4. Loyalty and rewards programs. A controller may offer a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.

5. Privacy notice. A controller shall provide consumers with an accessible, clear and meaningful privacy notice in plain language that is understandable by a reasonable consumer that includes:

A. The categories of personal data processed by the controller;

B. The purpose for 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 3rd parties, if any;

E. The categories of 3rd parties, if any, with which the controller shares personal data; and

F. An active e-mail address or other mechanism that the consumer may use to contact the controller.

6. Advance notice of material change to privacy notice. Before implementing a material change for previously collected personal data with respect to any of the items described in the privacy notice, a controller shall take reasonable measures to notify each consumer affected by the material change and to provide each affected consumer with a reasonable opportunity to withdraw consent for the materially different processing of the consumer's previously collected personal data.

7. Consumer rights request mechanism. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise a consumer right pursuant to this chapter. The design of the secure and reliable means must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of requests and the ability of the controller to verify the identity of the consumer making the request. A controller may not require a consumer to create a new account in order to exercise a consumer right, but may require a consumer to use an existing account.

8. Notice of sale and targeted advertising; opt-out mechanism. If a controller sells personal data to a 3rd party or processes personal data for targeted advertising, the

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. The disclosure required under this section must include:

A. A clear and conspicuous link titled "Do Not Sell My Personal Data" or bearing a substantially similar title on the controller's publicly accessible website that directs the consumer, or an agent of the consumer, to a publicly accessible website that enables the consumer, or an agent of the consumer, to opt out of the sale of the consumer's personal data; and

B. A clear and conspicuous link titled "Opt Me Out of Targeted Advertising" or bearing a substantially similar title on the controller's publicly accessible website that directs the consumer, or an agent of the consumer, to a publicly accessible website that enables the consumer, or an agent of the consumer, to opt out of processing of the consumer's personal data for targeted advertising.

In lieu of providing the 2 links described in paragraphs A and B, a controller may satisfy the requirements of this subsection by providing a single conspicuous and clearly labeled link on the controller's publicly accessible website that allows a consumer, or an agent of the consumer, both to opt out of the sale of the consumer's personal data and to opt out of the processing of the consumer's personal data for targeted advertising. If the controller maintains a specific section or page of its publicly accessible website that allows a consumer, or an agent of the consumer, to opt out of the sale of the consumer's data or the processing of the consumer's data for targeted advertising and to select additional privacy controls, the controller may satisfy the requirements of this subsection by providing a single conspicuous and clearly labeled link on the controller's publicly accessible website titled "Your Privacy Choices" or bearing a substantially similar title that directs the consumer, or an agent of the consumer, to that specific section or page of its publicly accessible website.

9. Universal opt-out mechanism. No later than July 1, 2025, a controller shall allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or any sale of personal data through an opt-out preference signal sent, with the consumer's consent, by a platform, technology or mechanism to the controller indicating the consumer's intent to opt out of any such processing or sale. The platform, technology or mechanism:

A. Must be consumer-friendly and easy to use by the average consumer;

B. May not unfairly disadvantage another controller;

C. May not make use of a default setting but must require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any such processing or sale of the consumer's personal data;

D. Must be as consistent as possible with another similar platform, technology or mechanism required by federal or state law; and

E. Must enable the controller to reasonably determine whether the consumer is a resident of this State and whether the consumer has made a legitimate request to opt out of the sale of the consumer's personal data or targeted advertising.

A controller that recognizes an opt-out preference signal that has been approved by the laws of another state is in compliance with this subsection.

If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or any sale of such personal data through an opt-out preference signal sent in accordance with the provisions of this subsection conflicts with the consumer's preexisting controller-specific privacy setting or voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller shall comply with the consumer's opt-out preference signal but may notify the consumer of the conflict and provide the consumer a choice to confirm the controller-specific privacy setting or participation in that program.

§9607. Responsibilities of processors and controllers

1. Processor responsibilities. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Assistance provided under this section must include:

A. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, so far as is reasonably practicable, to fulfill the controller's obligation to respond to a consumer rights request;

B. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as defined in chapter 210-B, of the system of the processor, in order to meet the controller's obligations; and

C. Providing necessary information to enable the controller to conduct and document data protection assessments.

2. Contractual requirements. 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 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 require 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 data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

C. On 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 with the obligations in this chapter;

D. Allow and cooperate with reasonable assessments by the controller or the controller's designated assessor. 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 obligations in this chapter, using an appropriate and accepted control standard or framework and assessment procedure for the assessment. The processor shall provide a report of the assessment to the controller upon request; and

E. Provide the controller an opportunity to object before engaging a subcontractor and, if no objection is made, engage the subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

3. Processing relationship liability. Nothing in this section may be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship as described in this chapter.

4. Fact-based determination. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in the person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with other persons, determining the purposes and means of the processing of personal data, the processor acts as a controller with respect to the processing and may be subject to an enforcement action under section 9612.

5. Data security and deletion. Controllers and processors 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. These processes must include the disposal of personal data in accordance with a retention schedule that requires:

A. The disposal of personal data by the controller when the data is required to be deleted by law or when the data is no longer necessary for the purpose for which the data was processed unless the consumer has consented to the retention of the data for a longer period of time or retention of the data is required by law; and

B. The disposal of personal data by the processor or return of that personal data to the controller as requested at the end of the processor's provision of services to the controller unless retention of the data is required by law.

For purposes of this subsection, "disposal of personal data" means the destruction or permanent deletion of the data or other modification of the data to make the data unreadable or indecipherable and unrecoverable.

6. Consent required to transfer sensitive data. Controllers and processors may not transfer sensitive data to a 3rd party unless the consumer consents to the transfer.

7. Discrimination prohibited. Controllers and processors may not, unless it is necessary to comply with other applicable law, process personal data in a manner that discriminates against individuals, or otherwise makes unavailable the equal enjoyment of the controller's or processor's goods or services, on the basis of an individual's actual or perceived race, color, sex, sexual orientation or gender identity, physical or mental disability, religion, ancestry, national origin, age or familial status. This subsection does not apply to:

A. The processing of personal data by a controller or processor for the purpose of self-testing to prevent or mitigate unlawful discrimination or for the purpose of diversifying an applicant, participant or customer pool; or

(1) A private establishment described in 42 United States Code, Section 2000a(e).

For purposes of this subsection, "familial status," "gender identity," "physical or mental disability," and "sexual orientation," have the same meanings as in Title 5, section 4553, subsections 5-A, 5-C, 7-A and 9-C, respectively. For purposes of this subsection, "sex" has the same meaning as in Title 5, section 4572-A, subsection 1.

§9608. Data protection assessments

1. Documentation. A controller shall conduct and document 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:

A. The processing of personal data for the purposes of targeted advertising;

B. The sale of personal data;

C. The processing of personal data for the purposes of profiling, when profiling presents a reasonably foreseeable risk of:

(1) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(2) Financial, physical or reputational injury to consumers;

(3) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, when the intrusion would be offensive to a reasonable person; or

(4) Other substantial injury to consumers; and

D. The processing of sensitive data.

2. Required elements. Data protection assessments conducted pursuant to subsection 1 must identify and weigh the benefits that may flow, directly and 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 the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The controller shall factor into the 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.

3. Attorney General disclosure; exemption from public records. The Attorney General may require that a controller disclose a data protection assessment 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. A data protection assessment is confidential and exempt from disclosure under Title 1, chapter 13. To the extent information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, the disclosure does not constitute a waiver of that privilege or protection.

4. Processing activity. A single data protection assessment may address a comparable set of processing operations that include similar activities.

5. Reciprocity. If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment satisfies the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

6. Deadline for performing data protection assessments. A controller shall conduct and document a data protection assessment as required by this section:

A. Within 6 months of the date that the controller first engages in a processing activity that presents a heightened risk of harm to a consumer as described in subsection 1; and

B. Within 6 months of making a material change to any processing activity that presents a heightened risk of harm to a consumer as described in subsection 1.

§9609. De-identified and pseudonymous data

1. De-identified data requirements. A controller in possession of de-identified data shall:

A. Take reasonable measures to ensure that the data cannot be associated with an individual;

B. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

C. Contractually obligate recipients of the de-identified data to comply with all provisions of this chapter.

2. De-identified data and pseudonymous re-identification of data. Nothing in this chapter may be construed to require a controller or processor to:

A. Re-identify de-identified data or pseudonymous data; or

B. Maintain data in identifiable form, or collect, obtain, retain or access data or technology, in order to be capable of associating an authenticated consumer request with personal data.

3. Consumer requests. Nothing in this chapter may be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

A. Is not reasonably capable of associating the request with the personal data, or it would be unreasonably burdensome for the controller to associate the request with the personal data; and

B. Does not use the personal data to recognize or respond to the consumer who is the subject of the personal data, or associate the personal data with other personal data about the same consumer.

4. Pseudonymous data requirements. The rights afforded under section 9604, subsection 1, paragraphs A to D do not apply to pseudonymous data in cases when the controller is able to demonstrate that information necessary to identify the consumer is kept

separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

5. Contractual oversight. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address breaches of those contractual commitments.

§9610. Geofence

A person may not use a geofence to establish a virtual perimeter within 1,750 feet of any facility that provides in-person health care services for the purpose of identifying, tracking, collecting data from or sending any notification regarding the consumer's consumer health data to a consumer that enters within that virtual perimeter. This subsection does not prohibit the operator of a facility that provides in-person health care services from implementing a geofence around the facility.

§9611. Construction of controller and processor duties and obligations

1. Exempt controller and processor activities. Nothing in this chapter may be construed to restrict a controller's or processor's ability to:

A. Comply with federal laws or regulations or the laws and rules of the State;

B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal or Maine governmental authorities or governmental authorities of a federally recognized Indian tribe in the State;

C. Cooperate with federal, tribal or Maine law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal laws or regulations or the laws and rules of the State;

D. Investigate, establish, exercise, prepare for or defend legal claims;

E. Provide a product or service specifically requested by a consumer;

F. Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

G. Take steps at the request of a consumer prior to entering into a contract;

H. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis;

I. Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or illegal activity or preserve the integrity or security of systems or investigate, report or prosecute those responsible for an action described in this paragraph;

J. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine:

(1) Whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

(2) Whether the expected benefits of the research outweigh the privacy risks; and

(3) Whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with re-identification;

K. Assist another controller, processor or 3rd party with obligations under this chapter;

L. Process personal data for reasons of public interest in the area of public health, but solely to the extent that the processing is:

(1) Subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

(2) Under the responsibility of a professional subject to confidentiality obligations under federal or state laws or local ordinances;

M. Deliver a communication that is not an advertisement to a consumer if the communication is reasonably anticipated by the consumer within the context of the consumer's interactions with the controller;

N. Transfer assets to a 3rd party in the context of a merger, acquisition, bankruptcy or similar transaction when the 3rd party assumes control, in whole or in part, of the controller's assets, only if the controller, in a reasonable time prior to the transfer, provides an affected consumer with:

(1) A notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies; and

(2) A reasonable opportunity to withdraw previously given consent related to the consumer's personal data, and a reasonable opportunity to request the deletion of the consumer's personal data;

O. Transfer a password if the transfer is necessary to use a designated password manager or the transfer is made to a controller for the sole purpose of identifying passwords being reused across sites or accounts; or

P. Transfer genetic information if the transfer is necessary to conduct medical research or to make a medical diagnosis or provide medical treatment specially requested by the consumer.

2. Internal use; advertising. The obligations imposed on controllers or processors under this chapter do not restrict a controller's or processor's ability to use personal data that is collected in a lawful manner:

A. To conduct internal research to develop, improve or repair products, services or technology;

B. To effectuate a product recall;

C. To identify and repair technical errors that impair existing or intended functionality;

D. In a manner consistent with the reasonable expectations of a consumer based on the consumer's interactions with the controller; for another disclosed purpose that is compatible with the context in which the personal data was collected; for performance under a contract to which the consumer is a party; or as otherwise authorized by law;

E. To process data necessary to perform system maintenance or diagnostics;

F. To protect against spam. For purposes of this paragraph, "spam" means an unsolicited digital communication unrelated to a recipient's interaction with a controller sent in bulk to a large number of recipients;

G. To present an advertisement, including targeted advertising, to an individual or device via a method that includes, but is not limited to, a website or application, direct e-mail, e-mail or text message communication, as long as the controller or processor complies with any opt-out requests under section 9604, subsection 1, paragraph E, complies with the prohibition against using the personal data of a minor for targeted advertising under section 9606, subsection 3, paragraph A and the personal data processed for the advertisement does not include sensitive data.

3. Evidentiary privilege. The obligations imposed on controllers or processors under this chapter do not apply when compliance with this chapter by the controller or processor would violate an evidentiary privilege under the laws of this State. Nothing in this chapter may 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.

4. Private schools. The obligations imposed on controllers or processors under this chapter do not prohibit a private school that is not subject to the Family Educational Rights and Privacy Act of 1974, 20 United States Code, Section 1232g et seq., from denying a consumer's request to delete the consumer's personal data if the deletion of that personal data would unreasonably interfere with the provision of educational services by the school or would unreasonably interfere with the ordinary operation of the school. For purposes of this subsection, "private school" has the same meaning as in Title 20-A, section 1, subsection 22.

5. Liability. A controller or processor that discloses personal data to a processor or 3rd-party controller in accordance with this chapter has not violated this chapter if the processor or 3rd-party controller that receives and processes the personal data violates this chapter, as long as, at the time the disclosing controller or processor disclosed the personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or 3rd-party controller would violate this chapter. A 3rd-party controller or processor receiving personal data from a controller or processor in compliance with this chapter is likewise not in violation of this chapter for the transgressions of the controller or processor from which the 3rd-party controller or processor receives the personal data.

6. Exemptions. Nothing in this chapter may be construed to:

A. Impose an obligation on a controller or processor that adversely affects the rights or freedoms of a person, including, but not limited to, the rights of a person:

(1) To freedom of speech or freedom of the press guaranteed in the United States Constitution, Amendment I; or

(2) Under Title 16, section 61; or

B. Apply to an individual's processing of personal data in the course of the individual's purely personal or household activities.

7. Limitations. Personal data processed by a controller or processor pursuant to this section may be processed only to the extent that the processing is:

A. Reasonably necessary and proportionate to the purposes listed in this section or, if the controller or processor is processing sensitive data, strictly necessary to the purposes listed in this section; and

B. Adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data used pursuant to subsection 2 must, when applicable, take into account the nature and purpose of the use. The data must 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 the use of personal data.

8. Controller burden. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the limitations in subsection 7.

9. Clarification of roles. Processing personal data for the purposes expressly identified in this section does not solely make a legal entity a controller with respect to the processing.

§9612. Enforcement

1. Violation as unfair trade practice; exclusive Attorney General enforcement. A violation of this chapter constitutes an unfair trade practice under the Maine Unfair Trade Practices Act, except that the provisions of Title 5, section 207, subsection 2 do not apply to this chapter and except as provided in subsections 2 and 3. The Attorney General has the exclusive authority to enforce violations of this chapter under the Maine Unfair Trade Practices Act.

2. Notice. Notwithstanding any provision of Title 5, section 209 to the contrary, at least 30 days prior to commencement of any action under the Maine Unfair Trade Practices Act to enforce this chapter, the Attorney General shall notify the person against whom an action may be brought of the intended action and give the person an opportunity to confer with the Attorney General in person or by counsel or other representative as to the intended action. Notice must be sent by mail, postage prepaid, to the person's usual place of business, or if the person has no usual place of business, to the person's last known address. The Attorney General may proceed without notice as required by this subsection upon a showing of facts by affidavit of immediate irreparable harm to the consumers of the State.

3. No private right of action. Notwithstanding Title 5, section 213, this chapter may not be construed as creating a private right of action against any person based on a violation of any provision of this chapter.

Sec. 2. Report. By February 1, 2027, the Attorney General shall submit a report to the joint standing committee of the Legislature having jurisdiction over judiciary matters regarding the operation and implementation of the Maine Revised Statutes, Title 10, chapter 1057. The report must include, at a minimum, the following information:

1. The number of notices the Attorney General has issued under Title 10, section 9612, subsection 2 and the nature of the violations alleged in the notices;

2. The number of persons sent a notice described in subsection 1 that conferred with the Attorney General during the notice period described in Title 10, section 9612, subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair Trade Practices Act;

3. The number of civil actions brought by the Attorney General under the Maine Unfair Trade Practices Act to enforce violations of Title 10, chapter 1057; and

4. Any recommendations the Attorney General has for improving the operation of Title 10, chapter 1057.

The joint standing committee of the Legislature having jurisdiction over judiciary matters may report out legislation related to the report to the 133rd Legislature in 2027.

Sec. 3. Deadline for certain actions. The first data protection assessments required by the Maine Revised Statutes, Title 10, section 9608 must be completed no later than January 1, 2026.

Sec. 4. Appropriations and allocations. The following appropriations and allocations are made.

ATTORNEY GENERAL, DEPARTMENT OF THE

Administration - Attorney General 0310

Initiative: Provides ongoing funding for 2 Assistant Attorney General positions, one Paralegal position and one Technician position effective January 1, 2025.

GENERAL FUND	**2023-24**	**2024-25**
POSITIONS - LEGISLATIVE COUNT	0.000	4.000
Personal Services	$0	$224,428
All Other	$0	$14,143
GENERAL FUND TOTAL	$0	$238,571

Sec. 5. Effective date. This Act takes effect July 1, 2025.'

Amend the bill by relettering or renumbering any nonconsecutive Part letter or section number to read consecutively.

SUMMARY

This amendment, which is the majority report of the committee, replaces the bill and enacts the Maine Data Privacy and Protection Act, which takes effect July 1, 2025. The Act regulates the collection, use, processing, transfer, sale and deletion of nonpublicly available personal data that is linked or reasonably linkable to an individual who is a resident of this State or to a device that is reasonably linkable to an individual who is a resident of this State, referred to in the Act as a "consumer," by a person that conducts business in this State or that produces products or services targeted to residents of this State, referred to in the Act as a "controller." Under the Act, a controller must limit the collection and processing of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer, except that the controller must limit the collection and processing of certain sensitive data to what is strictly necessary to provide or maintain a specific product or service requested by the consumer. Under the Act, "sensitive data" includes data revealing the consumer's race or ethnic origins, religious beliefs, mental or physical health conditions or diagnoses, sexual orientation, gender identity, citizenship or immigration status; genetic or biometric data; precise geolocation data; social security, driver's license or nondriver identification card numbers; specific financial or account access information; data of a known minor; or data

concerning the consumer's status as the victim of a crime. A controller is also required to obtain a consumer's affirmative consent before collecting any biometric data. If the controller knows that the consumer has not attained 13 years of age, the controller may not process the consumer's data for any purpose without parental consent. If the controller knows or willfully disregards that the consumer is a minor, the controller may not process the consumer's data for targeted advertising in any circumstances and must obtain consent before processing the consumer's data for sale.

The Act requires a controller to provide consumers with a privacy notice specifying the categories of personal data processed by the controller, the purposes for processing the personal data, the categories of personal data transferred to 3rd parties and the categories of 3rd parties to whom personal data is shared. A consumer has the right, under the Act, to confirm whether a controller is processing the consumer's personal data; to require the controller to correct inaccuracies in or delete the consumer's personal data; to obtain a copy of the consumer's personal data; and to opt out of the processing of the consumer's personal data for purposes of targeted advertising, sale or profiling in furtherance of decisions about the consumer's access to financial or lending services, housing, insurance, education, criminal justice, employment opportunities, health care services and essential goods and services. The privacy notice must describe how a consumer may exercise these rights. A controller is also required to notify each affected consumer before implementing a material change for previously collected personal data with respect to any items described in the privacy notice.

The Act prohibits a controller from processing data in a manner that discriminates against a person in violation of state or federal law. A controller is also prohibited from retaliating against a consumer for exercising the consumer's rights under the Act, except that a controller may offer different prices or selection of goods in connection with a consumer's voluntary participation in a bona fide loyalty or discount program. A controller and any person that processes data for the controller, must establish, implement and maintain reasonable data security practices and a retention schedule that requires the disposal of personal data by the controller when deletion is required by law or the data is no longer necessary for the purpose for which it was processed unless retention of the data is required by law. The retention schedule must also require the disposal of data by or the return of the data to the controller by a person who processes data for the controller, unless retention of the data is required by law. If a controller engages in a data processing activity that presents a heightened risk of harm to a consumer, including processing any data for targeted advertising, sale or profiling or any processing of sensitive data, the controller must conduct and document a data protection assessment within 6 months of the effective date of the Act to identify and weigh the benefits and potential risks of the processing activity. After the effective date of the Act, a controller must also conduct a data protection assessment within 6 months of making a material change to an existing processing activity or initiating a new processing activity that presents a heightened risk of harm to a consumer. The controller may be required to disclose the data protection assessment to the Attorney General, who must keep it confidential, when the assessment is relevant to an investigation conducted by the Attorney General. The Act further prohibits any person from establishing a geofence within 1,750 feet of any in-person health care facility in the State, other than the operator of the facility, for the purpose of identifying, tracking, collecting data from or sending a notification regarding consumer health data to consumers who enter that area.

ROS

The provisions of the Act do not apply to specifically enumerated persons, including the State, political subdivisions of the State and federally recognized Indian tribes in the State; nonprofit organizations; institutions of higher education; supervised financial organizations and service corporations; health care facilities and health care practitioners as well as an affiliate of a health care facility or health care practitioner that qualifies both as a business associate and that provides services only to covered entities, as the terms "business associate" and "covered entity" are defined in the federal Health Insurance Portability and Accountability Act of 1996; state-licensed and authorized insurers that are in compliance with applicable Maine laws governing insurer data security and data privacy; broadband Internet service providers to the extent those providers are subject to the data privacy requirements of the Maine Revised Statutes, Title 35-A, section 9301; and persons that both processed the personal data of fewer than 10,000 consumers in the preceding calendar year and derived no more than 20% of gross revenue from the sale of personal data. The Act also does not apply to persons that controlled or processed the personal data for purposes other than completing payment transactions of fewer than 100,000 consumers in the preceding calendar year, except that, beginning January 1, 2027, this exception applies only to persons that controlled or processed the personal data for purposes other than completing payment transactions of fewer than 50,000 consumers in the preceding calendar year.

In addition, the provisions of the Act do not apply to specifically enumerated types of data, including: nonpublic personal information regulated under the federal Gramm-Leach-Bliley Act; protected health information under the federal Health Insurance Portability and Accountability Act of 1996; personal data regulated by the Family Education Rights and Privacy Act of 1974; data processed and maintained by the controller regarding an applicant for employment or employee to the extent the data is collected and used within the context of that role; and data necessary for the controller to administer benefits. The Maine Data Privacy and Protection Act also does not prohibit controllers from engaging in specifically enumerated activities, including complying with Maine or federal law; complying with investigations or subpoenas from governmental authorities, including the Federal Government and the government of the State or a federally recognized Indian tribe in the State; cooperating with federal, tribal or Maine law enforcement agencies; providing a product or service specifically requested by the consumer; protecting life and physical safety of consumers and preventing or responding to security incidents; delivering a reasonably anticipated communication that is not an advertisement to a consumer, for example a product survey; transferring assets to a 3rd party in the context of a merger or similar transaction if certain notice requirements are met; transferring passwords if necessary for use of a password manager; and transferring genetic information if necessary to conduct medical research or provide medical treatment specifically requested by the consumer. The Act also does not prohibit a controller from using personal data collected in a lawful manner: for internal product research; to effectuate a product recall; in a manner consistent with a consumer's reasonable expectations or for a disclosed purpose that is compatible with the context in which the personal data was collected; and to present an advertisement, including a targeted advertisement, to an individual or device, as long as the consumer's targeted advertising opt-out request, if any, is honored and the personal data processed for purposes of the advertisement does not include sensitive data.

Violations of the Act may be enforced exclusively by the Attorney General under the Maine Unfair Trade Practices Act. Absent a showing of immediate irreparable harm, the Attorney General is required to provide a potential defendant with at least 30 days' notice prior to initiating an enforcement action, during which time the potential defendant may confer with the Attorney General to avoid the action. The Act further requires the Attorney General to submit a report by February 1, 2027 to the joint standing committee of the Legislature having jurisdiction over judiciary matters regarding the operation and implementation of the Act. The committee may report out legislation related to the report to the 133rd Legislature in 2027.

FISCAL NOTE REQUIRED

(See attached)

Revised: 04/12/24 mac

131st MAINE LEGISLATURE

LD 1977 **LR 2156(02)**

An Act to Create the Data Privacy and Protection Act

Fiscal Note for Bill as Amended by Committee Amendment "A" (H-975)
Committee: Judiciary
Fiscal Note Required: Yes

Fiscal Note

	FY 2023-24	FY 2024-25	Projections FY 2025-26	Projections FY 2026-27
Net Cost (Savings)				
General Fund	$0	$238,571	$493,301	$510,042
Appropriations/Allocations				
General Fund	$0	$238,571	$493,301	$510,042

Correctional and Judicial Impact Statements

This bill may increase the number of civil suits filed in the court system. The additional workload associated with the minimal number of new cases filed in the court system does not require additional funding at this time. The collection of additional filing fees will increase General Fund revenue by minor amounts.

Fiscal Detail and Notes

This bill includes ongoing General Fund appropriations to the Office of the Attorney General of $238,571 in fiscal year 2024-25 to establish 2 Assistant Attorney General positions, one Paralegal position and one Technician position in the Consumer Protection Division beginning January 1, 2025 for implementation, administration and enforcement of the provisions of the Maine Data Privacy and Protection Act.