Rep C

EAK ROS

L.D. 1088

Date: 6/13/25 (Filing No. H-719)

REPORT C

JUDICIARY

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

STATE OF MAINE

HOUSE OF REPRESENTATIVES

132ND LEGISLATURE

FIRST SPECIAL SESSION

COMMITTEE AMENDMENT "B" to H.P. 710, L.D. 1088, "An Act to Enact the Maine Consumer Data Privacy Act"

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

'An Act to Enact the Maine Online Data Privacy 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 ONLINE DATA PRIVACY ACT

§9601. Short title

This chapter may be known and cited as "the Maine Online Data Privacy 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 person that, directly or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person, such that the person:

A. Owns or has the power to vote more than 50% of the outstanding shares of any voting class of the other person's securities;

B. Has the power to elect or influence the election of a majority of the directors, members or managers of the other person;

C. Has the power to direct the management of the other person; or

D. Is subject to the other person's exercise of the powers described in paragraph A, B or C.

2. Authenticate. "Authenticate" means to use reasonable means to determine that a request to exercise a consumer right in accordance with section 9606 is being made by, or on behalf of, a consumer who is entitled to exercise the consumer right with respect to the personal data at issue.

3. Biometric data. "Biometric data":

A. Means data generated by automatic measurements of the biological characteristics of a consumer that can be used to uniquely authenticate a consumer's identity, including a fingerprint, a voiceprint, an image of a retina or iris and any other biological characteristic that can be used to uniquely authenticate a consumer's identity; and

B. Does not include a digital or physical photograph, an audio or video recording or any data generated from a digital or physical photograph or an audio or video recording, unless the data is generated to identify a specific consumer.

4. Business associate. "Business associate" has the same meaning as in HIPAA.

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

6. Collect. "Collect" means to purchase, rent, gather, obtain, receive, access or otherwise acquire personal data.

7. Consent. "Consent":

A. Means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the collection or processing of personal data relating to the consumer for a particular purpose. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action; and

B. Does not include:

(1) Acceptance of a general or broad terms of use document or similar document that contains descriptions of personal data collection or processing along with other unrelated information;

(2) Hovering over, muting, pausing or closing a piece of content; or

(3) Agreement obtained through the use of a dark pattern.

8. Consumer. "Consumer":

A. Means an individual who is a resident of this State; and

B. Does not include an individual acting in a commercial or employment context or an individual acting as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit organization or government entity whose communications or transactions with a controller occur solely within the context of the individual's role with the company, partnership, sole proprietorship, nonprofit organization or government entity.

9. Consumer health data. "Consumer health data" means personal data that a controller uses to identify a consumer's physical or mental health status, and includes, but

is not limited to, data related to gender-affirming health care services and reproductive health care services.

10. 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 person;

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

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

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

12. Covered entity. "Covered entity" has the same meaning as in HIPAA.

13. Dark pattern. "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting 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."

14. De-identified data. "De-identified data" means data that does not identify, cannot reasonably be used to infer information about and cannot otherwise be linked to an identified or identifiable consumer, or a device that may be linked to an identified or identifiable consumer, if the controller that possesses the data:

A. Takes reasonable measures to ensure that the de-identified data cannot be linked with a consumer;

B. Commits in a publicly available terms and conditions document or in a publicly available privacy policy to maintain and use the data in its de-identified format; and

C. Contractually obligates recipients of the data to satisfy the criteria and commitments in paragraphs A and B.

15. 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.

16. Familial status. "Familial status" has the same meaning as in Title 5, section 4553, subsection 5-A.

17. Gender identity. "Gender identity" has the same meaning as in Title 5, section 4553, subsection 5-C.

18. Gender-affirming health care services. "Gender-affirming health care services" has the same meaning as in Title 14, section 9002, subsection 4.

19. Genetic data. "Genetic data" means any data, regardless of its format, that concerns a consumer's genetic characteristics. "Genetic data" includes, but is not limited to:

A. Raw sequence data that results from sequencing of a consumer's complete extracted deoxyribonucleic acid, or DNA, or a portion of the consumer's DNA;

B. Information extrapolated, derived or inferred from analyzing the raw sequence data under paragraph A, including, but not limited to, genotypic and phenotypic information; and

C. Self-reported health information submitted to a direct-to-consumer genetic testing company by a consumer regarding the consumer's health conditions that is used for scientific research or product development and analyzed in connection with the consumer's raw sequence data.

20. Geofence. "Geofence" means technology that establishes or monitors a virtual geographic perimeter around a specific physical location through the use of global positioning system coordinates, cellular tower connectivity, cellular data, radio frequency identification, wireless access point data or any other form of location detection technology.

21. HIPAA. "HIPAA" means 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.

22. Identified or identifiable consumer. "Identified or identifiable consumer" means a consumer who can readily be identified, either directly or indirectly.

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

24. Personal data. "Personal data" means information that is linked or can be reasonably linked to an identified or identifiable consumer or that is linked or reasonably can be linked to a device that is linked or reasonably can be linked to an identified or identifiable consumer. "Personal data" does not include de-identified data or publicly available information.

25. Physical or mental disability. "Physical or mental disability" has the same meaning as in Title 5, section 4553, subsection 7-A.

26. Precise geolocation data. "Precise geolocation data":

A. Means information derived from technology that can precisely and accurately identify the past or present specific location of a consumer within a radius of 1,750 feet. "Precise geolocation data" includes global positioning system level latitude and longitude coordinates or data from other similar mechanisms; and

B. Does not include the content of communications, data generated by or connected to advanced utility metering infrastructure systems or data generated by equipment used by a utility.

27. Process. "Process" means any operation or set of operations performed on personal data or on sets of personal data by manual or automated means, including the use, storage, disclosure, analysis, deletion or modification of personal data but not including the collection of personal data.

ROS

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

29. 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 consumer's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location or movements.

30. Protected health information. "Protected health information" has the same meaning as in HIPAA.

31. Publicly available information. "Publicly available information":

A. Means information about a consumer that a person:

(1) Lawfully obtains from a record of a governmental entity; or

(2) Reasonably believes has been lawfully made available to the general public by the consumer or by widely distributed media; and

B. Does not include:

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

(2) Biometric data;

(3) Genetic data, unless the genetic data has been made available to the general public by the consumer;

(4) Any information that is collated or combined to create a consumer profile that is made available to a user of a publicly available Internet website or mobile application either for remuneration or free of charge;

(5) Any information that is made available for sale;

(6) Inferences derived from information described in subparagraph (4) or (5) or inferences derived from a combination of publicly available information and other personal data; or

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

32. Reproductive health care services. "Reproductive health care services" has the same meaning as in Title 14, section 9002, subsection 9.

33. Sale of personal data. "Sale of personal data":

A. Means the exchange of personal data for monetary or other valuable consideration by a controller, processor or affiliate of a controller or processor to a 3rd party; and

B. Does not include:

(1) The disclosure of personal data to a processor that processes the personal data on behalf of the controller if the processing of the personal data is limited to the controller's processing purpose;

ROS

(2) The disclosure of personal data to a 3rd party for purposes of providing a product or service affirmatively requested by the consumer;

(3) The disclosure of personal data to an affiliate of the controller;

(4) The disclosure 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; or

(5) The disclosure of personal data that the consumer:

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

(b) Did not restrict to a specific audience.

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

A. Data revealing racial or ethnic origins, religious beliefs, consumer health data, sexual activity, sexual orientation, gender identity, national origin or citizenship or immigration status;

B. Genetic data or biometric data;

C. Personal data of a consumer that the controller knows or should know is a minor;

D. Precise geolocation data;

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

F. Account numbers, credit card numbers or debit card numbers, if circumstances exist wherein such numbers can be used without additional identifying information, access codes or passwords;

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

H. Data concerning a consumer'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.

35. Sex. "Sex" has the same meaning as in Title 5, section 4572-A, subsection 1.

36. Sexual orientation. "Sexual orientation" has the same meaning as in Title 5, section 4553, subsection 9-C.

37. Targeted advertising. "Targeted advertising":

A. Means displaying advertisements to a consumer or on a device identified by a unique identifier when the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications that are unaffiliated with each other in order to predict the consumer's preferences or interests; and

B. Does not include:

(1) Advertisements based on the context of a consumer's current search query or visit to a website or online application;

(2) Advertisements based on a consumer's activities within a controller's own websites or online applications;

(3) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(4) Collecting or processing personal data solely to measure or report advertising frequency, performance or reach.

38. Third party. "Third party" means a person other than the consumer, controller, processor or affiliate of the controller or processor of particular personal data.

39. Trade secret. "Trade secret" has the same meaning as in section 1542, subsection 4.

§9603. Applicability

1. Effective date. The requirements of this chapter take effect on September 1, 2026.

2. Persons affected. 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 35,000 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.

§9604. Exceptions

1. 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;

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.

2. 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;

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

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

E. Identifiable private information to the extent that it is 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 or in accordance with the standards for the protection of human subjects in research under 21 Code of Federal Regulations, Parts 50 and 56;

F. 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;

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 HIPAA;

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 HIPAA;

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 collected, processed or maintained:

(1) In the course of an individual's applying to, being 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 subparagraph (1) and used for the purposes of administering those benefits;

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; or

Q. Personal data collected and used pursuant to the federal Controlled Substances Act, 21 United States Code, Section 830.

3. Compliance with COPPA. 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.

§9605. Consumer health data

1. Confidentiality. A person may not provide an employee or a contractor access to consumer health data unless:

A. The employee or contractor is subject to a contractual or statutory duty of confidentiality; or

B. Confidentiality is required as a condition of employment of the employee.

2. Processor duties. A person may not provide a processor access to consumer health data unless the person providing access to the consumer health data and the processor comply with section 9609.

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

§9606. Consumer rights

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

A. Confirm whether a controller is collecting or processing the consumer's personal data;

B. If a controller collects or processes a consumer's personal data, access the consumer's personal data;

C. 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;

D. Require a controller to delete personal data provided by, or obtained about, the consumer unless retention of the personal data is required by law;

E. When processing of personal data is done by automatic means, obtain a copy of the consumer's personal data collected and 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 easily and without hindrance;

F. Obtain a list of the 3rd parties to which the controller has sold the consumer's personal data or, if the controller does not maintain information about the 3rd parties to which the controller has sold the personal data of the specific consumer, obtain a list of the 3rd parties to which the controller has sold any consumer's personal data; and

G. Opt out of the collection and processing of the consumer's personal data for purposes of:

(1) Targeted advertising;

(2) The sale of personal data; or

(3) Profiling in furtherance of any automated decision that produces any legal or similarly significant effect concerning the consumer.

2. Exception; trade secrets. This section may not be construed to require a controller to reveal a trade secret.

3. Exercise of consumer rights. This subsection governs the exercise of the consumer rights established in subsection 1.

A. A controller shall establish a secure and reliable method pursuant to section 9608, subsection 6 for a consumer to exercise a consumer right under this section.

B. A consumer may exercise a consumer right under this section, including through another individual who has authority under subsection 4 to exercise the consumer's rights, using the method established by the controller under paragraph A.

4. Exercise of consumer rights by agent or guardian. The following persons may exercise the rights established in subsection 1 on behalf of a consumer.

A. A consumer may designate an agent in accordance with section 9607 to exercise the consumer's right under subsection 1, paragraph G to opt out of the collection and processing of personal data.

B. If the consumer is a child, a parent or legal guardian may exercise the consumer's rights under subsection 1.

C. If the consumer is subject to a guardianship, conservatorship or other protective arrangement, the guardian or conservator of the consumer may exercise the consumer's rights under subsection 1.

5. Response to exercise of consumer rights. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer or other person authorized to exercise the consumer's rights under subsection 1 as follows.

A. A controller shall respond to a request not later than 45 days after the controller receives the request. The controller may extend the response period by a period of 45 days if:

(1) It is reasonably necessary to extend the period to complete the request based on the complexity and number of the requests; and

(2) The controller informs the consumer of the extension and the reason for the extension within the initial 45-day response period.

B. If a controller declines to take action regarding the request, the controller shall inform the consumer without undue delay, but not later than the 45th day after receipt of the request, of:

(1) The justification for declining to take action; and

(2) Instructions for how to appeal the decision.

C. A controller shall provide information to a consumer in response to a request, free of charge, once during any 12-month period, except that, if requests from a consumer or other person authorized to exercise the consumer's rights are manifestly unfounded, excessive, technically infeasible or repetitive, the controller may:

(1) Charge the consumer a reasonable fee to cover the administrative costs of complying with the request; or

(2) Decline to act on the request.

The controller bears the burden of demonstrating the manifestly unfounded, excessive, technically infeasible or repetitive nature of the request.

D. If a controller is unable to authenticate a request to exercise a consumer right under subsection 1 using commercially reasonable efforts, the controller:

(1) Is not required to comply with a request to initiate an action in accordance with this section; and

(2) Shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right until the consumer or other person authorized to exercise the consumer's rights provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the right.

E. Notwithstanding paragraph D and except as provided in section 9607, a controller is not required to authenticate an opt-out request.

F. A controller that has obtained personal data about a consumer from a source other than the consumer is in compliance with a request to delete that data pursuant to

ROS.

subsection 1, paragraph D by retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data:

(1) Remains deleted from the controller's records; and

(2) Is not used for any other purpose.

6. Appeals. A controller shall establish a process in accordance with the requirements of this subsection for a consumer or other person authorized to exercise the consumer's rights to appeal the controller's inaction on a request within a reasonable period of time after the consumer's receipt of the decision.

A. The appeal process must be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section.

B. Not later than the 60th day after receipt of an appeal, a controller shall inform the consumer or other person authorized to exercise the consumer's rights in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions.

C. If a controller denies an appeal, the controller shall provide the consumer with an online mechanism, if available, through which the consumer or other person authorized to exercise the consumer's rights may contact the Attorney General to submit a complaint.

§9607. Authorized agent

1. Authority to designate agent to opt out of collection and processing. 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 right under section 9606, subsection 1, paragraph G to opt out of the collection and processing of personal data.

2. Method of designating agent. 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 exercise the consumer's right under section 9606, subsection 1, paragraph G to opt out of the collection and processing of personal data.

3. Authentication of agent's opt-out request. A controller shall comply with a request received from an authorized agent to exercise the consumer's right under section 9606, subsection 1, paragraph G to opt out of the collection and processing of personal data if, using commercially reasonable efforts, the controller is able to authenticate:

A. The identity of the consumer; and

B. The authorized agent's authority to act on the consumer's behalf.

§9608. Actions of controllers

1. Prohibitions. A controller may not:

A. Collect, process or share sensitive data concerning a consumer, unless the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer;

B. Sell sensitive data;

C. Collect or process personal data in violation of state or federal laws that prohibit unlawful discrimination;

D. If the controller knows or reasonably should know that the consumer is a minor:

(1) Collect or process personal data of the consumer for the purpose of targeted advertising; or

(2) Sell the personal data of the consumer;

E. Retaliate against a consumer for exercising a consumer right granted in this chapter, 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;

F. Collect, process or disclose personal data or publicly available information in a manner that unlawfully discriminates in or otherwise unlawfully makes unavailable the equal enjoyment of 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 paragraph does not apply to the collection, processing or disclosure of personal data for:

(1) The purpose of self-testing to prevent or mitigate unlawful discrimination;

(2) The purpose of diversifying an applicant, participant or customer pool; or

(3) A private establishment described in 42 United States Code, Section 2000a(e); or

G. Unless the controller obtains the consumer's consent, process personal data for a purpose that is neither reasonably necessary to nor compatible with the disclosed purposes for which the personal data is processed, as disclosed to the consumer.

2. Duties. A controller shall:

A. Limit the collection 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, including any routine administrative, operational, website or account-servicing activity that is consistent with the reasonable expectations of the consumer under the circumstances. This paragraph does not prevent a controller from processing personal data collected in accordance with this paragraph to provide advertising to a consumer based on the consumer's activities within the controller's own websites or online applications;

B. Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue. These processes must include the disposal of personal data in accordance with a retention schedule that requires 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. For purposes of this paragraph, "disposal of personal data" means the destruction or permanent deletion of the data or other modification of the data to make the data unreadable and unrecoverable; and

C. Provide an effective mechanism for a consumer to revoke the consumer's consent to processing personal data under this section that is at least as easy to use as the mechanism by which the consumer provided the consumer's consent and, upon revocation of the consent, shall cease to process the data as soon as practicable, but not later than 30 days after the receipt of the request.

3. Exceptions; loyalty programs. Subsection 1 and 2 may not be construed to:

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

B. Prohibit a controller from offering 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, as long as the sale of personal data is not a condition of participation in the program.

4. Privacy notice. A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes the following information:

A. The categories of personal data, including sensitive data, collected or processed by the controller;

B. The controller's purpose for collecting and processing personal data;

C. How consumers may exercise their consumer rights under this chapter, including how a consumer may appeal a controller's decision regarding the consumer's request and how a consumer may revoke consent;

D. The categories of 3rd parties with which the controller shares personal data, with a level of detail that enables a consumer to understand the type of, business model of or processing conducted by each category of 3rd party;

E. The categories of personal data, including sensitive data, the controller shares with any 3rd party;

F. The length of time the controller intends to retain each category of personal data or, if it is not possible to identify the length of time, the criteria used to determine the length of time the controller intends to retain each category of personal data; and

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

5. Notice of sale of personal data, targeted advertising or profiling; opt-out mechanism. If a controller sells personal data to 3rd parties, collects or processes personal data for the purposes of targeted advertising or processes personal data for the purposes of profiling the consumer in furtherance of decisions that produce legal or similarly significant effects concerning the consumer, the controller shall clearly and conspicuously disclose the sale, collection or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale, collection or processing. The disclosure required under this subsection must be prominently displayed on the controller's publicly accessible website and the language used must be clear, easy to understand and unambiguous.

6. Method for exercising consumer rights. A controller shall establish, and shall describe in the privacy notice as required by subsection 4, paragraph C, one or more secure

and reliable mechanisms for a consumer to submit a request to exercise each consumer right under this chapter.

A. The design of the secure and reliable mechanism for a consumer to submit a request must take into account:

(1) The ways in which consumers normally interact with the controller;

(2) The need for secure and reliable communication of consumer requests; and

(3) The ability of the controller to verify the identity of a consumer making the request.

B. A controller may not require a consumer to create a new account to exercise a consumer right. A controller may require a consumer to use an existing account to exercise a consumer right.

C. A controller may satisfy the controller's obligation under this subsection to establish a secure and reliable mechanism for a consumer to exercise the right to opt out under subsection 5 by:

(1) Providing a clear and conspicuous link on the controller's publicly accessible website to a webpage that allows a consumer, an authorized agent of the consumer or a person authorized by section 9606, subsection 4 to exercise the consumer's rights to opt out of any collection or processing of the consumer's personal data for the purposes of targeted advertising or profiling or any sale of personal data; and

(2) No later than September 1, 2026, allowing a consumer to opt out of any collection or 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 the collection, processing or sale as described in section 9607, subsection 2. The platform, technology or mechanism:

(a) Must be consumer-friendly and easy to use by the average consumer;

(b) Must use clear, easy to understand and unambiguous language;

(c) Must be as consistent as possible with any other similar platform, technology or mechanism required by federal or state law, rule or regulation;

(d) Must enable the controller to reasonably determine whether the consumer is a resident of the State, which reasonable determination may be based on the location associated with the consumer's Internet protocol address, and whether the consumer has made a legitimate request to opt out of any such collection, processing or sale of the consumer's personal data;

(e) May not unfairly disadvantage another controller; and

(f) 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 collection, processing or sale of the consumer's personal data.

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

ROS

D. If a consumer's decision to opt out of any collection or processing of the consumer's personal data for the purposes of targeted advertising or profiling or any sale of personal data through an opt-out preference signal sent in accordance with paragraph C, subparagraph (2) conflicts with the consumer's existing controller-specific privacy setting or the consumer's voluntary participation in a controller's bona fide loyalty, rewards, premium features, discounts or club card program, the controller may notify the consumer of the conflict and provide the consumer a choice to confirm the controller-specific privacy setting or participation that program.

§9609. Responsibilities of processors and controllers

1. Contract required. If a controller uses a processor to process personal data of a consumer, the controller and the processor shall enter into a contract in accordance with the requirements of this section that governs the processor's data processing procedures with respect to processing performed on behalf of the controller.

A. The contract must be binding and must clearly set forth:

(1) Instructions for processing personal data;

(2) The nature and purpose of the processing;

(3) The type of personal data subject to processing;

(4) The duration of the processing; and

(5) The rights and obligations of the processor and the controller.

B. The contract must require that the processor:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(2) Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data, considering the volume and nature of the personal data;

(3) Stop processing personal data on request by the controller made in accordance with a consumer's authenticated request;

(4) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of service, unless retention of the personal data is required by law;

(5) 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;

(6) Engage any subcontractor to assist with processing personal data on the controller's behalf only in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data under the processor's contract with the controller;

(7) Allow and cooperate with reasonable assessments by the controller, the controller's designated assessor or a qualified and independent assessor arranged for by the processor to assess the processor's policies and technical and

organizational measures in support of the obligations under this chapter. An assessment conducted under this subparagraph must be conducted using an appropriate and accepted control standard framework and assessment procedure; and

(8) On request of the controller, provide the controller with a report of an assessment conducted under subparagraph (7).

2. Processor responsibilities. A processor shall:

A. Adhere to a contract with a controller and the instructions of the controller;

B. Assist the controller in meeting the controller's obligations under this chapter, including:

(1) By employing appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to requests to exercise consumer rights, considering the nature of processing and the information available to the processor; and

(2) By assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data under this chapter and in relation to the notification of a breach of the security of a system, as required by chapter 210-B; and

C. Provide necessary information to enable the controller to conduct and document data protection assessments as required by section 9610.

3. Processing relationship liability. This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship in accordance with this section.

4. Fact-based determination of role. The determination of whether a person is acting as a controller or a processor with respect to a specific processing of personal data is a fact-based determination that depends on the context in which the personal data is being processed as described in this subsection.

A. A person is considered to be a controller if:

(1) The person is not limited in the person's processing of specific personal data in accordance with a controller's instructions; or

(2) The person fails to adhere to a controller's instructions with respect to a specific processing of personal data.

B. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

C. If a processor or 3rd party begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under section 9613.

5. Controller's duties unaffected. This section may not be construed to alter a controller's obligation to limit a person's processing of personal data or to take steps to ensure that a processor adheres to the controller's instructions.

§9610. Data protection assessments

1. Definition. For the purposes of this section, "processing activities that present a heightened risk of harm to a consumer" means:

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

B. The sale of personal data;

C. The collection or processing of sensitive data; and

D. The processing of personal data for the purposes of profiling, in which the profiling presents a reasonably foreseeable risk of:

(1) Unfair, abusive or deceptive treatment of a consumer;

(2) Having an unlawful disparate impact on a consumer;

(3) Financial, physical or reputational injury to a consumer;

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

(5) Other substantial injury to a consumer.

2. Data protection assessments required. A controller shall conduct and document a data protection assessment for each of the controller's collection or processing activities that present a heightened risk of harm to a consumer. A single data protection assessment may address a comparable set of collection or processing operations that include similar activities.

3. Required elements. A data protection assessment required by subsection 2 must be conducted in accordance with the requirements of this subsection.

A. The data protection assessment must identify and weigh the benefits that may flow directly and indirectly from the collection or processing to the controller, the consumer, other interested parties and the public against:

(1) The potential risks to the rights of the consumer associated with the collection or processing as mitigated by safeguards that may be employed by the controller to reduce these risks; and

(2) The necessity and proportionality of collection or processing in relation to the stated purpose of the collection or processing.

B. The controller shall factor into a data protection assessment:

(1) The use of de-identified data;

(2) The reasonable expectations of consumers;

(3) The context of the collection or processing; and

(4) The relationship between the controller and the consumer whose personal data will be collected or processed.

4. Disclosure to Attorney General. The Attorney General may require that a controller disclose to the Attorney General a data protection assessment that is relevant to

an investigation conducted by the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter.

5. Confidentiality. A data protection assessment is confidential and exempt from disclosure under Title 1, chapter 13 but may be used by the Attorney General in an action to enforce this chapter. To the extent that any information contained in a data protection assessment disclosed to the Attorney General pursuant to this section includes information subject to attorney-client privilege or work product protection, the disclosure does not constitute a waiver of that privilege or protection.

6. 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 in accordance with this section.

7. Deadlines 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 collection or processing activity that presents a heightened risk of harm to a consumer; and

B. Within 6 months of making a material change to any collection or processing activity that presents a heightened risk of harm to a consumer.

8. Application. The requirement to conduct a data protection assessment under this section applies only to collection or processing activities that occur on or after September 1, 2026.

§9611. De-identified data

1. Re-identification not required. This chapter may not be construed to require a controller or processor to:

A. Re-identify de-identified data;

B. Maintain data in an identifiable form; or

C. Collect, obtain, retain or access any data or technology in order to be capable of associating an authenticated consumer request with personal data.

2. Consumer requests. This chapter may not 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;

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; and

C. Does not sell the personal data to a 3rd party or otherwise voluntarily disclose the personal data to a 3rd party other than a processor, except as otherwise allowed in this chapter.

3. Contractual oversight. A controller that discloses de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the de-identified data is subject and shall take appropriate steps to address breaches of those contractual commitments. Whether oversight is reasonable and whether steps taken to address breaches of contractual commitments are appropriate depends in part on whether the disclosed de-identified data would be considered sensitive data if the data were re-identified.

§9612. Exemptions

1. Exempt activities. This chapter may not be construed to restrict a controller's or processor's ability to:

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

B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by a federal or Maine governmental authority, including a governmental authority 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, the laws and rules of the State or local laws and ordinances;

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, investigate, prosecute those responsible for or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any other type of illegal activity;

J. Preserve the integrity or security of systems;

K. Assist another controller or processor or a 3rd party with an obligation under this chapter; or

L. 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, but 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 of the receiving entity; and

(2) A reasonable opportunity to:

(a) Withdraw any previous consent related to the consumer's personal data; and

(b) Request deletion of the consumer's personal data.

2. Internal use. The obligations imposed on a controller or processor under this chapter do not restrict a controller's or processor's ability to collect, use or retain personal data for internal use to:

A. Effectuate a product recall;

B. Identify and repair technical errors that impair existing or intended functionality; or

C. Perform internal operations that:

(1) Are reasonably aligned with the expectations of the consumer or can be reasonably anticipated based on the consumer's existing relationship with the controller; or

(2) Are otherwise compatible with processing data to provide a product or service specifically requested by a consumer or performing under a contract to which the consumer is a party.

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 state law. This chapter may not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under state law as part of a privileged communication.

4. Exceptions to liability. This subsection limits the liability of a controller, processor or 3rd-party controller for violations of this chapter by other persons.

A. A controller or processor that discloses personal data to a processor or a 3rd-party controller in compliance with this chapter has not violated this chapter if the processor or 3rd-party controller that receives the personal data violates this chapter as long as:

(1) 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; and

(2) At the time the disclosing controller or processor disclosed the personal data, the disclosing controller or processor was, and remained, in compliance with its obligations as the discloser of the personal data.

B. A 3rd-party controller or processor that receives personal data from a controller or processor in compliance with this chapter is not in violation of this chapter for the independent misconduct of the controller or processor from which the 3rd-party controller or processor received the personal data.

5. Freedom of speech; freedom of the press; personal or household use. This chapter may not be construed to:

A. Impose an obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person to freedom of speech or freedom to engage in political activity or the right of freedom of the press guaranteed in the United States Constitution, Amendment I; or

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

6. Burden of proof. If a controller collects or processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the collection or processing qualifies for the exemption and complies with the limitations in subsection 7.

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

A. Subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and reduce reasonably foreseeable risks of harm to consumers relating to the collection, use or retention of personal data;

B. Reasonably necessary and proportionate to the purposes listed in this section; and

C. Adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section.

8. Collecting or processing personal data pursuant to an exemption. A person that collects or processes personal data pursuant to an exemption in this section may not be considered a controller solely based on that collection or processing of personal data.

§9613. 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 213 do not apply to this chapter and except as provided in subsection 2. The Attorney General has the exclusive authority to enforce violations of this chapter under the Maine Unfair Trade Practices Act.

2. Discretionary notice and right to cure. Notwithstanding any provision of the Maine Unfair Trade Practices Act to the contrary, before initiating any action under subsection 1 for an alleged violation that occurs on or before April 1, 2027, if the Attorney General believes that it is possible to cure the alleged violation, the Attorney General may issue a notice of violation to the controller or processor that is allegedly violating this chapter. If the Attorney General issues a notice of violation to a controller or processor under this subsection, the Attorney General may not bring an action to enforce the violation unless the controller or processor fails to cure the violation within 60 days of receiving the notice of violation. The Attorney General shall consider the following factors in deciding whether to issue a notice of violation under this subsection:

A. The number of alleged violations;

B. The size and complexity of the controller or processor;

C. The nature and extent of the controller's or processor's collection or processing activities;

D. The likelihood of injury to the public;

E. The degree to which the alleged violations affect the safety of persons and property;

F. Whether the alleged violation was likely caused by a human or technical error; and

G. The extent to which the controller or processor has previously violated this chapter or similar laws.

§9614. Report

By February 1, 2027 and annually thereafter, the Attorney General shall submit a report to the joint standing committee of the Legislature having jurisdiction over judiciary matters regarding the implementation and operation of this chapter. The report must include, at a minimum, the following information:

1. Number of notices. The number of notices the Attorney General has issued under section 9613, subsection 2 and the nature of the violations alleged in the notices;

2. Number of persons sent a notice. The number of persons sent a notice described in subsection 1 that conferred with the Attorney General during the notice period described in section 9613, subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair Trade Practices Act;

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

4. Recommendations. Any recommendations the Attorney General has for improving the operation of this chapter.

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

Sec. 2. Appropriations and allocations. The following appropriations and allocations are made.

ATTORNEY GENERAL, DEPARTMENT OF THE

Administration - Attorney General 0310

Initiative: Provides funding for one Assistant Attorney General position, one Paralegal position, one Technician position and related costs to administer and enforce the Maine Online Data Privacy Act.

GENERAL FUND	**2025-26**	**2026-27**
POSITIONS - LEGISLATIVE COUNT	0.000	3.000
Personal Services	$0	$420,508
All Other	$0	$20,000
GENERAL FUND TOTAL	$0	$440,508

Sec. 3. Effective date. This Act takes effect September 1, 2026.

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

SUMMARY

This amendment, which is a minority report of the committee, strikes the bill and changes the title. The amendment enacts the Maine Online Data Privacy Act, which takes effect September 1, 2026. The Act regulates the collection, use, processing, disclosure,

sale and deletion of nonpublicly available personal data 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," if the personal data is linked or can be reasonably linked to an identified or identifiable individual who is a resident of this State, referred to in the Act as a "consumer," or is linked or reasonably can be linked to a device that is linked or reasonably can be linked to an identified or identifiable consumer. 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, including the collection of personal data to provide advertising to the consumer based on the consumer's activities within the controller's own websites or online applications. The controller must also 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 a 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 information; data of a minor under 18 years of age; or data concerning the consumer's status as the victim of a crime.

The Act establishes that consumers have the right to confirm whether a controller is processing their data; correct inaccuracies in their personal data; require the controller to delete any portion of their personal data that the controller is not required to maintain by law; obtain a copy of their personal data in a format that can be readily transferred to another controller; obtain a list of the 3rd parties to which the controller has sold personal data; and opt out of the processing of their personal data for purposes of targeted advertising, sale or consumer profiling. The Act also prohibits a controller from selling any sensitive data; processing the personal data of a minor for purposes of targeted advertising or sale; processing personal data in a manner that discriminates against a person in violation of state or federal law; and retaliating against a consumer for exercising a 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.

The Act also requires a controller to provide consumers with a privacy notice specifying how a consumer may exercise the consumer's rights under the Act; 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. 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 either when deletion is required by law or when the data is no longer necessary for the purpose for which it was processed and retention of the data is not required by law. The controller must also require, by contract, that any person who processes a consumer's personal data on behalf of the controller treats the personal data confidentially and deletes or returns all personal data to the controller at the end of the processing, 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 identifying and weighing the benefits and potential risks of the processing activity. 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.

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; federally registered national securities associations; supervised financial organizations and service corporations; health care facilities and health care practitioners as well as their affiliates that both qualify as business associates and provide services only to covered entities; state-licensed and authorized insurers that are in compliance with applicable Maine laws governing insurer data security and data privacy; and 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. In addition, the provisions of the Act do not apply to specifically enumerated types of data, including, for example: 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 Educational Rights and Privacy Act of 1974; personal data collected and used pursuant to the federal Controlled Substances Act; 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 Act also does not prohibit controllers from engaging in specifically enumerated activities, including, for example: complying with state or federal law; complying with investigations or subpoenas from federal, state or tribal governmental authorities; 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; preventing or responding to security incidents; and transferring data as part of a merger, acquisition or bankruptcy as long as the consumer is given advance notice and a reasonable opportunity to request deletion of the consumer's personal data. The Act also does not prohibit a controller from using personal data collected in a lawful manner to effectuate a product recall, identify and repair technical errors and perform internal operations that are reasonably aligned with a consumer's expectations or otherwise compatible with providing the product or service specifically requested by the consumer.

Violations of the Act may be enforced exclusively by the Attorney General under the Maine Unfair Trade Practices Act. If the violation occurs on or before April 1, 2027, the Attorney General may provide a potential defendant with a notice of violation at least 60 days prior to initiating an enforcement action, during which time the potential defendant may cure the violation to avoid the enforcement action. The amendment further requires the Attorney General to submit a report by February 1, 2027, and annually thereafter, to the joint standing committee of the Legislature having jurisdiction over judiciary matters

ROS.

regarding the implementation and operation of the Act. The committee may report out legislation related to the report to the 133rd Legislature in 2027.

FISCAL NOTE REQUIRED

(See attached)

Approved: 06/04/25 LRL

132nd MAINE LEGISLATURE

LD 1088 **LR 2064(02)**

An Act to Enact the Maine Consumer Data Privacy Act

Fiscal Note for Bill as Amended by Committee Amendment "B" (H-719)
Committee: Judiciary
Fiscal Note Required: Yes

Fiscal Note

	FY 2025-26	FY 2026-27	Projections FY 2027-28	Projections FY 2028-29
Net Cost (Savings)				
General Fund	$0	$440,508	$457,416	$489,920
Appropriations/Allocations				
General Fund	$0	$440,508	$457,416	$489,920

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

The bill includes a General Fund appropriation to the Office of the Attorney General of $440,508 in fiscal year 2026-27 for one Assistant Attorney General position, one Paralegal position, one Technician position and related costs to administer and enforce the Maine Online Data Privacy Act.