

MAINE STATE LEGISLATURE

The following document is provided by the
LAW AND LEGISLATIVE DIGITAL LIBRARY
at the Maine State Law and Legislative Reference Library
<http://legislature.maine.gov/lawlib>



Reproduced from electronic originals
(may include minor formatting differences from printed original)



132nd MAINE LEGISLATURE

FIRST REGULAR SESSION-2025

Legislative Document

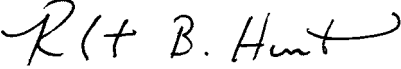
No. 1088

H.P. 710

House of Representatives, March 18, 2025

An Act to Enact the Maine Consumer Data Privacy Act

Received by the Clerk of the House on March 14, 2025. Referred to the Committee on Judiciary pursuant to Joint Rule 308.2 and ordered printed pursuant to Joint Rule 401.


ROBERT B. HUNT
Clerk

Presented by Representative HENDERSON of Rumford.
Cosponsored by Representatives: POIRIER of Skowhegan, ROBERTS of South Berwick.

1 **Be it enacted by the People of the State of Maine as follows:**

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

3 **CHAPTER 1057**

4 **MAINE CONSUMER DATA PRIVACY ACT**

5 **§9601. Short title**

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

7 **§9602. Definitions**

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

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

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

17 A. A digital or physical photograph;

18 B. An audio or video recording;

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

21 D. Data collected, used or stored for health care treatment, payment or operations under
22 the federal Health Insurance Portability and Accountability Act of 1996, 42 United
23 States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and
24 exemptions adopted pursuant to that Act.

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

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

28 **5. Consent.** "Consent" means a clear affirmative act signifying a consumer's freely
29 given, specific, informed and unambiguous agreement to allow the processing of personal
30 data relating to the consumer. "Consent" may include a written statement, including by
31 electronic means, that is made in the language that the consumer uses to obtain a product
32 or service from the controller and in a format that is reasonably accessible to and usable by
33 consumers with disabilities. "Consent" does not include:

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

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

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

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

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

10 **8. Control.** "Control" means:

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

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

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

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

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

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

24 **12. Decisions that produce legal or similarly significant effects concerning the**
25 **consumer.** "Decisions that produce legal or similarly significant effects concerning the
26 consumer" means decisions that result in the provision or denial to the consumer of
27 financial or lending services, housing, insurance, education enrollment or opportunity,
28 criminal justice, employment opportunities, health care services or access to essential
29 goods or services.

30 **13. De-identified data.** "De-identified data" means data that cannot reasonably be
31 used to infer information about or otherwise be linked to an identified or identifiable
32 individual, or a device linked to an individual, if the controller that possesses the data:

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

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

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

39 **14. Federally recognized Indian tribe in this State.** "Federally recognized Indian
40 tribe in this State" means the Houlton Band of Maliseet Indians, the Mi'kmaq Nation, the
41 Passamaquoddy Tribe or the Penobscot Nation when the band, nation or tribe is acting in
42 a governmental capacity and not in a business capacity. "Federal recognized Indian tribe

1 in this State" does not include a business entity, including any federally chartered tribal
2 corporation or other business entity owned or partly owned by the Houlton Band of
3 Maliseet Indians, the Mi'kmaq Nation, the Passamaquoddy Tribe or the Penobscot Nation.

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

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

11 **17. Personal data.** "Personal data" means information that is linked or reasonably
12 linkable to an identified or identifiable individual. "Personal data" does not include de-
13 identified data or publicly available information.

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

19 A. The content of communications; or

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

22 **19. Process.** "Process" means an operation or set of operations performed on personal
23 data, including the collection, use, storage, disclosure, analysis, deletion or modification of
24 personal data.

25 **20. Processor.** "Processor" means a person that processes personal data on behalf of
26 a controller.

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

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

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

40 **24. Publicly available information.** "Publicly available information":

41 A. Means information that is:

- 1 (1) Lawfully made available to the general public through federal, state or local
2 government records;
- 3 (2) Made available to the general public through widely distributed media;
- 4 (3) Made available through a website or online service made available to all
5 members of the public, either for free or for a fee, including a website or online
6 service in which all members of the public can log on to the website or online
7 service either for free or for a fee, unless the individual who made the information
8 available via the website or online service has restricted the information to a
9 specific audience;
- 10 (4) Disclosed to the general public as required by federal, state or local law; or
- 11 (5) Collected through the visual observation of the physical presence of an
12 individual or by a device located in a public place, not including data collected by
13 a device in the individual's possession; and

14 B. Does not include:

- 15 (1) Any obscene visual depiction as described in 18 United States Code, Section
16 1460;
- 17 (2) Biometric data;
- 18 (3) Genetic information, unless the genetic information has been made available to
19 the general public by the individual to whom the genetic information pertains;
- 20 (4) Inferences derived from a combination of publicly available information and
21 personal data; or
- 22 (5) Intimate images a controller or processor knows have been created or shared
23 without consent of the individual depicted in the images. For purposes of this
24 subparagraph, "intimate image" means a photograph, videotape, film or digital
25 recording of an individual in a state of nudity or engaged in a sexual act or engaged
26 in sexual contact for which there is no public or newsworthy purpose.

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

- 30 A. The disclosure of personal data to a processor that processes the personal data on
31 behalf of the controller;
- 32 B. The disclosure of personal data to a 3rd party for purposes of providing a product
33 or service requested by the consumer;
- 34 C. The disclosure or transfer of personal data to an affiliate of the controller;
- 35 D. The disclosure of personal data when the consumer directs the controller to disclose
36 the personal data or intentionally uses the controller to interact with a 3rd party;
- 37 E. The disclosure of personal data that the consumer:
 - 38 (1) Intentionally made available to the general public via a channel of mass media;
39 and
 - 40 (2) Did not restrict to a specific audience; or

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

5 **26. Sensitive data.** "Sensitive data" means personal data that includes:

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

8 B. Genetic or biometric data;

9 C. Consumer health data;

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

11 E. Precise geolocation data;

12 F. A social security number, driver's license number or nondriver identification card
13 number, except that "sensitive data" does not include the last 4 digits of a social security
14 number, driver's license number or nondriver identification card number;

15 G. A consumer's account number, log-in information, financial account number or
16 credit or debit card number that, in combination with any required security code, access
17 code or password, permits access to a consumer's financial account; or

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

21 **27. Targeted advertising.** "Targeted advertising" means displaying an advertisement
22 to a consumer when the advertisement is selected based on personal data obtained or
23 inferred from that consumer's activities over time and across nonaffiliated publicly
24 accessible websites or online applications to predict that consumer's preferences or
25 interests. "Targeted advertising" does not include:

26 A. Advertisements based on activities within a controller's own publicly accessible
27 websites or online applications;

28 B. Advertisements based on the context of a consumer's current search query, visit to
29 a publicly accessible website or online application;

30 C. Advertisements directed to a consumer in response to the consumer's request for
31 information or feedback; or

32 D. Processing personal data solely to measure or report advertising frequency,
33 performance or reach.

34 **28. Trade secret.** "Trade secret" has the same meaning as in section 1542, subsection
35 4.

36 **§9603. Scope**

37 **1. Applicability; July 1, 2026 to December 31, 2027.** From July 1, 2026 to December
38 31, 2027, the provisions of this chapter apply to persons that conduct business in this State
39 or persons that produce products or services that are targeted to residents of this State and
40 that during the preceding calendar year:

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

4 B. Controlled or processed the personal data of not less than 25,000 consumers and
5 derived more than 25% of gross revenue from the sale of personal data.

6 **2. Applicability; beginning January 1, 2028.** Beginning January 1, 2028, the
7 provisions of this chapter apply to persons that conduct business in this State or persons
8 that produce products or services that are targeted to residents of this State and that during
9 the preceding calendar year:

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

13 B. Controlled or processed the personal data of not less than 25,000 consumers and
14 derived more than 25% of gross revenue from the sale of personal data.

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

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

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

20 C. A financial institution or affiliate of a financial institution, including a service
21 corporation, that is subject to the federal Gramm-Leach-Bliley Act, 15 United States
22 Code, Section 6801 et seq. (1999) only if that institution or affiliate is directly and
23 solely engaged in financial activities as described in 12 United States Code, Section
24 1843(k) (2023). For purposes of this paragraph, "service corporation" has the same
25 meaning as in Title 9-B, section 131, subsection 37; or

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

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

30 A. Nonpublic personal information regulated under and collected, processed, sold or
31 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,
32 15 United States Code, Section 6801 et seq. (1999);

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

36 C. Patient-identifying information as described in 42 United States Code, Section
37 290dd-2;

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

40 E. Identifiable private information that is otherwise information collected as part of
41 human subjects in research pursuant to the good clinical practice guidelines issued by

1 the International Council for Harmonisation of Technical Requirements for
2 Pharmaceuticals for Human Use or successor organization;

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

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

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

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

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

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

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

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

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

38 O. Data processed or maintained:

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

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

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

4 P. Personal data collected, processed, sold or disclosed in relation to price, route or
5 service, as such terms are used in the federal Airline Deregulation Act of 1978, 49
6 United States Code, Section 40101 et seq., by an air carrier subject to that Act, to the
7 extent this chapter is preempted by the federal Airline Deregulation Act of 1978, 49
8 United States Code, Section 41713.

9 **5. Compliance with federal Children's Online Privacy Protection Act of 1998.**

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

15 **§9604. Consumer rights**

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

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

20 B. Correct inaccuracies in the consumer's personal data, taking into account the nature
21 of the personal data and the purposes of the processing of the consumer's personal data;

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

23 D. Obtain a copy of the consumer's personal data processed by the controller, in a
24 portable and, to the extent technically feasible, readily usable format that allows the
25 consumer to transmit the data to another controller without hindrance, when the
26 processing is carried out by automated means, as long as the controller is not required
27 to reveal a trade secret; and

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

29 (1) Targeted advertising;

30 (2) The sale of personal data; or

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

33 **2. Exercise of consumer rights.** A consumer may communicate and access the
34 information necessary to exercise rights under this section by a secure and reliable means
35 established by the controller and described to the consumer in the controller's privacy
36 notice. A consumer may designate an authorized agent in accordance with section 9605 to
37 exercise the rights of the consumer to opt out of the processing of the consumer's personal
38 data as specified in subsection 1, paragraph E. In the case of processing personal data of a
39 consumer known to be a child, the parent or legal guardian may exercise consumer rights
40 on the child's behalf. In the case of processing personal data concerning a consumer subject
41 to a guardianship, conservatorship or other protective arrangement, the guardian or the
42 conservator of the consumer may exercise rights on the consumer's behalf.

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

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

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

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

19 D. If a controller is unable to authenticate a request to exercise a right afforded under
20 subsection 1, using commercially reasonable efforts, the controller is not required to
21 comply with a request to initiate an action pursuant to this section and shall provide
22 notice to the consumer that the controller is unable to authenticate the request to
23 exercise the right until the consumer provides additional information reasonably
24 necessary to authenticate the consumer and the consumer's request to exercise the right.

25 E. A controller that has obtained personal data about a consumer from a source other
26 than the consumer is in compliance with a consumer's request to delete that data
27 pursuant to subsection 1, paragraph C by retaining a record of the deletion request and
28 the minimum data necessary for the purpose of ensuring that the consumer's personal
29 data remains deleted from the controller's records and not using the retained data for
30 any other purpose pursuant to the provisions of this chapter.

31 **4. Appeals.** A controller shall establish a process for a consumer to appeal the
32 controller's inaction on a request within a reasonable period of time after the consumer's
33 receipt of the decision. The appeal process must be conspicuously available and similar to
34 the process for submitting requests to initiate action pursuant to this section. Not later than
35 the 60th day after receipt of an appeal, a controller shall inform the consumer in writing of
36 action taken or not taken in response to the appeal, including a written explanation of the
37 reasons for the decisions. If the appeal is denied, the controller shall also provide the
38 consumer with an online mechanism, if available, or other method through which the
39 consumer may contact the Attorney General to submit a complaint.

40 **§9605. Authorized agent**

41 A consumer may designate another person to serve as the consumer's authorized agent,
42 and act on the consumer's behalf, to opt out of the processing of the consumer's personal
43 data for the purposes specified in section 9604, subsection 1, paragraph E. The consumer
44 may designate an authorized agent by way of, among other methods, technology, including,

1 but not limited to, an Internet link or a browser setting, browser extension or global device
2 setting, indicating the consumer's intent to opt out of such processing. A controller shall
3 comply with an opt-out request received from an authorized agent if the controller is able
4 to verify, using commercially reasonable efforts, the identity of the consumer and the
5 authorized agent's authority to act on the consumer's behalf.

6 **§9606. Actions of controllers**

7 **1. Data minimization.** A controller must comply with the requirements of this
8 subsection.

9 A. A controller shall limit the collection of personal data to what is adequate, relevant
10 and reasonably necessary in relation to the purposes for which the data is processed, as
11 disclosed to the consumer.

12 B. Except as otherwise provided in this chapter, a controller may not process personal
13 data for purposes that are neither reasonably necessary for, nor compatible with, the
14 disclosed purposes for which the data is processed, as disclosed to the consumer, unless
15 the controller obtains the consumer's consent. For purposes of this paragraph, a
16 controller's sale of sensitive data to one person or entity is neither necessary to nor
17 compatible with the controller's sale of sensitive data to a different person or entity.

18 C. A controller shall process the minimum amount of personal data that is reasonably
19 necessary, adequate or relevant for each purpose for which data is processed, as
20 disclosed to the consumer.

21 D. A controller shall maintain documentation sufficient to demonstrate compliance
22 with paragraphs A to C for as long as a processing activity continues and for a least 24
23 months after the controller ceases to engage in the processing activity.

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

26 **2. Duties.** A controller shall:

27 A. Establish and implement a retention schedule that requires the deletion or de-
28 identification of personal data when the retention of that data is no longer reasonably
29 necessary and relevant to the purposes for which the data is processed, as disclosed to
30 the consumer, or as otherwise permitted by this chapter or required by law;

31 B. Establish, implement and maintain reasonable administrative, technical and physical
32 data security practices to protect the confidentiality, integrity and accessibility of
33 personal data appropriate to the volume and nature of the personal data;

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

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

42 **3. Prohibitions.** A controller may not:

1 A. Process sensitive data concerning a consumer unless the controller obtains the
2 consumer's consent prior to processing. Consent is not valid under this paragraph
3 unless the controller has disclosed:

4 (1) The controller's identity;

5 (2) The reason consent is required, described in plain language that is
6 understandable by a reasonable consumer;

7 (3) The specific processing purposes for which consent is sought;

8 (4) The categories of sensitive data the controller must process to effectuate the
9 processing purpose and the categories of personal data that will be processed with
10 the sensitive data to effectuate the processing purpose; and

11 (5) If applicable, the identity of all 3rd parties to whom the sensitive data may be
12 sold.

13 If a consumer has not interacted with a controller for a period of 24 months, the
14 controller may not continue to process the consumer's sensitive data unless the
15 controller obtains a new consent from the consumer in accordance with the
16 requirements of this paragraph;

17 B. Process personal data in violation of the laws of this State and federal laws that
18 prohibit unlawful discrimination against consumers;

19 C. When the controller, under the circumstances, has actual knowledge or willfully
20 disregards that the consumer is at least 13 years of age but has not attained 16 years of
21 age:

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

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

25 D. Retaliate against a consumer for exercising a consumer right in this chapter or for
26 not agreeing to the collection or processing of personal data for a separate product or
27 service, including by denying goods or services, charging different prices or rates for
28 goods or services or providing a different level of quality of goods or services to the
29 consumer.

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

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

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

38 B. The purpose for processing personal data;

39 C. How consumers may exercise their consumer rights, including how a consumer
40 may appeal a controller's decision with regard to the consumer's request;

41 D. The categories of personal data that the controller shares with 3rd parties, if any;

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

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

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

13 **7. Notice of sale and targeted advertising; opt-out mechanism.** If a controller sells
14 personal data to a 3rd party or processes personal data for targeted advertising, the
15 controller shall clearly and conspicuously disclose such processing, as well as the manner
16 in which a consumer may exercise the right to opt out of such processing. The disclosure
17 required under this section must include:

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

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

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

40 **8. Universal opt-out mechanism.** No later than December 1, 2027, a controller shall
41 allow a consumer to opt out of any processing of the consumer's personal data for the
42 purposes of targeted advertising or any sale of personal data through an opt-out preference
43 signal sent, with the consumer's consent, by a platform, technology or mechanism to the
44 controller indicating the consumer's intent to opt out of any such processing or sale. The
45 platform, technology or mechanism:

- 1 A. Must be consumer-friendly and easy to use by the average consumer;
- 2 B. May not unfairly disadvantage another controller;
- 3 C. May not make use of a default setting but must require the consumer to make an
- 4 affirmative, freely given and unambiguous choice to opt out of any such processing or
- 5 sale of the consumer's personal data;
- 6 D. Must be as consistent as possible with another similar platform, technology or
- 7 mechanism required by federal or state law; and
- 8 E. Must enable the controller to reasonably determine whether the consumer is a
- 9 resident of this State and whether the consumer has made a legitimate request to opt
- 10 out of to the sale of the consumer's personal data or targeted advertising.

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

13 **§9607. Responsibilities of processors and controllers**

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

- 17 A. Taking into account the nature of processing and the information available to the
- 18 processor, by appropriate technical and organizational measures, so far as is reasonably
- 19 practicable, to fulfill the controller's obligation to respond to a consumer rights request;
- 20 B. Taking into account the nature of processing and the information available to the
- 21 processor, by assisting the controller in meeting the controller's obligations in relation
- 22 to the security of processing the personal data and in relation to the notification of a
- 23 breach of security, as required by chapter 210-B, of the system of the processor, in
- 24 order to meet the controller's obligations; and
- 25 C. Providing necessary information to enable the controller to conduct and document
- 26 data protection assessments.

27 **2. Contractual requirements.** A contract between a controller and a processor must
28 govern the processor's data processing procedures with respect to processing performed on
29 behalf of the controller. The contract must clearly set forth instructions for processing data,
30 the nature and purpose of processing, the type of data subject to processing, the duration of
31 processing and the rights and obligations of both parties. The contract must require that the
32 processor:

- 33 A. Ensure that each person processing personal data is subject to a duty of
- 34 confidentiality with respect to the data;
- 35 B. At the controller's direction, delete or return all personal data to the controller as
- 36 requested at the end of the provision of services, unless retention of the personal data
- 37 is required by law;
- 38 C. On the reasonable request of the controller, make available to the controller all
- 39 information in the processor's possession necessary to demonstrate the processor's
- 40 compliance with the obligations in this chapter;
- 41 D. Allow and cooperate with reasonable assessments by the controller or the
- 42 controller's designated assessor or arrange for a qualified and independent assessor to

1 conduct an assessment of the processor's policies and technical and organizational
2 measures in support of the obligations in this chapter, using an appropriate and
3 accepted control standard or framework and assessment procedure for the assessment.
4 The processor shall provide a report of the assessment to the controller upon request;
5 and

6 E. Engage a subcontractor pursuant to a written contract that requires the subcontractor
7 to meet the obligations of the processor with respect to the personal data.

8 **3. Processing relationship liability.** This section may not be construed to relieve a
9 controller or processor from the liabilities imposed on the controller or processor by virtue
10 of the controller's or processor's role in the processing relationship as described in this
11 chapter.

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

22 **§9608. Data protection assessments**

23 **1. Documentation.** A controller shall conduct and document a data protection
24 assessment for each of the controller's processing activities that presents a heightened risk
25 of harm to a consumer. For the purposes of this section, "processing that presents a
26 heightened risk of harm to a consumer" includes:

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

28 B. The sale of personal data;

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

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

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

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

36 (4) Other substantial injury to consumers; and

37 D. The processing of sensitive data.

38 **2. Required elements.** Data protection assessments conducted pursuant to subsection
39 1 must identify and weigh the benefits that may flow, directly and indirectly, from the
40 processing to the controller, the consumer, other stakeholders and the public against the
41 potential risks to the rights of the consumer associated with the processing, as mitigated by
42 safeguards that can be employed by the controller to reduce the risks. The controller shall

1 factor into the data protection assessment the use of de-identified data and the reasonable
2 expectations of consumers, as well as the context of the processing and the relationship
3 between the controller and the consumer whose personal data will be processed.

4 **3. Attorney General disclosure; exemption from public records.** The Attorney
5 General may require that a controller disclose a data protection assessment that is relevant
6 to an investigation conducted by the Attorney General, and the controller shall make the
7 data protection assessment available to the Attorney General. The Attorney General may
8 evaluate the data protection assessment for compliance with the responsibilities set forth in
9 this chapter. A data protection assessment is confidential and exempt from disclosure under
10 Title 1, chapter 13. To the extent information contained in a data protection assessment
11 disclosed to the Attorney General includes information subject to attorney-client privilege
12 or work product protection, the disclosure does not constitute a waiver of that privilege or
13 protection.

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

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

21 **6. Application.** A controller is not required to conduct a data protection assessment
22 under this section for any processing activity created or initiated before July 1, 2026.

23 **§9609. De-identified and pseudonymous data**

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

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

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

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

32 **2. De-identified data and pseudonymous re-identification of data.** This chapter
33 may not be construed to require a controller or processor to:

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

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

38 **3. Consumer requests.** This chapter may not be construed to require a controller or
39 processor to comply with an authenticated consumer rights request if the controller:

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

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

4 C. Does not sell the personal data to a 3rd party or otherwise voluntarily disclose the
5 personal data to a 3rd party other than a processor, except as otherwise permitted in
6 this section.

7 **4. Pseudonymous data requirements.** The rights afforded under section 9604,
8 subsection 1 do not apply to pseudonymous data in cases when the controller is able to
9 demonstrate that information necessary to identify the consumer is kept separately and is
10 subject to effective technical and organizational controls that prevent the controller from
11 accessing the information.

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

16 **§9610. Geofence**

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

23 **§9611. Controller and processor; duties and obligations**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26 A. Conduct internal research to develop, improve or repair products, services or
27 technology;

28 B. Effectuate a product recall;

29 C. Identify and repair technical errors that impair existing or intended functionality;
30 or

31 D. Perform internal operations that are reasonably aligned with the expectations of the
32 consumer or reasonably anticipated based on the consumer's existing relationship with
33 the controller, or are otherwise compatible with processing data in furtherance of the
34 provision of a product or service specifically requested by a consumer or the
35 performance of a contract to which the consumer is a party.

36 **3. Evidentiary privilege.** The obligations imposed on controllers or processors under
37 this chapter do not apply when compliance with this chapter by the controller or processor
38 would violate an evidentiary privilege under the laws of this State. This chapter may not
39 be construed to prevent a controller or processor from providing personal data concerning
40 a consumer to a person covered by an evidentiary privilege under the laws of this State as
41 part of a privileged communication.

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

11 **5. Exemptions.** This chapter may not be construed to:

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

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

16 **(2)** Under Title 16, section 61; or

17 **B.** Apply to a person's processing of personal data in the course of the person's purely
18 personal or household activities.

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

21 **A.** Reasonably necessary and proportionate to the purposes listed in this section; and

22 **B.** Adequate, relevant and limited to what is necessary in relation to the specific
23 purposes listed in this section. Personal data collected, used or retained pursuant to
24 subsection 2 must, when applicable, take into account the nature and purpose of the
25 collection, use or retention. The data must be subject to reasonable administrative,
26 technical and physical measures to protect the confidentiality, integrity and
27 accessibility of the personal data and to reduce reasonably foreseeable risks of harm to
28 consumers relating to the collection, use or retention of personal data.

29 **7. Controller burden.** If a controller processes personal data pursuant to an
30 exemption in this section, the controller bears the burden of demonstrating that the
31 processing qualifies for the exemption and complies with the limitations in subsection 6.

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

35 **§9612. Enforcement**

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

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

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

13 **§9613. Maine Privacy Fund established**

14 **1. Establishment; purpose.** The Maine Privacy Fund, referred to in this section as the
15 "fund," is established within the Department of the Attorney General as a nonlapsing fund
16 to providing funding for the staff and activities of the department necessary to enforce the
17 provisions of this chapter.

18 **2. Administration.** The Department of the Attorney General shall administer the
19 fund. The fund must be established and held separate and apart from any other funds or
20 money of the State or the department and must be used and administered exclusively for
21 purposes authorized in this section. The fund consists of:

22 A. Any civil penalties, attorney's fees or costs awarded to the State in an action brought
23 by the Attorney General to enforce a violation of this chapter;

24 B. Sums that may be appropriated by the Legislature to the fund or transferred by the
25 Treasurer of State to the fund;

26 C. Interest earned on fund balances; and

27 D. Other funds received from any public or private source, including grants, gifts,
28 bequests and donations.

29 **Sec. 2. 35-A MRSA c. 94,** as amended, is repealed.

30 **Sec. 3. Report.** By January 1, 2028, the Attorney General shall submit a report to the
31 joint standing committee of the Legislature having jurisdiction over judiciary matters
32 regarding the operation and implementation of the Maine Revised Statutes, Title 10,
33 chapter 1057. The report must include, at a minimum, the following information:

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

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

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

1 4. Any recommendations the Attorney General has for improving the operation of Title
2 10, chapter 1057.

3 The joint standing committee of the Legislature having jurisdiction over judiciary
4 matters may report out legislation related to the report to the Second Regular Session of the
5 133rd Legislature.

6 **Sec. 4. Effective date.** This Act takes effect July 1, 2026.

7 SUMMARY

8 This bill enacts the Maine Consumer Data Privacy Act, which takes effect July 1, 2026.
9 The Act regulates the collection, use, processing, disclosure, sale and deletion of
10 nonpublicly available personal data that is linked or reasonably linkable to an individual
11 who is a resident of the State, referred to in the Act as a "consumer," by a person that
12 conducts business in this State or that produces products or services targeted to residents
13 of this State, referred to in the Act as a "controller." Under the Act, a controller must limit
14 the collection of personal data to what is adequate, relevant and reasonably necessary in
15 relation to the purposes for which the controller processes that data, as disclosed in a
16 privacy notice specifying the categories of personal data processed by the controller, the
17 purposes for processing the personal data, the categories of personal data transferred to 3rd
18 parties and the categories of 3rd parties to whom personal data is shared. The Act also
19 requires a controller to process the minimum amount of personal data reasonably necessary,
20 adequate or relevant for each disclosed processing purpose.

21 A consumer has the right, under the Act, to confirm whether a controller is processing
22 the consumer's personal data; to require the controller to correct inaccuracies in or delete
23 the consumer's personal data; to obtain a copy of the consumer's personal data; and to opt
24 out of the processing of the consumer's personal data for purposes of targeted advertising,
25 sale or profiling in furtherance of decisions about the consumer's access to financial or
26 lending services, housing, insurance, education, criminal justice, employment
27 opportunities, health care services and essential goods and services. The privacy notice
28 must describe how a consumer may exercise these rights. The controller must obtain the
29 affirmative, informed consent of a consumer before processing the consumer's sensitive
30 data, including data revealing the consumer's race or ethnic origins, religious beliefs,
31 mental or physical health conditions or diagnoses, sexual orientation or citizenship or
32 immigration status; genetic or biometric data; precise geolocation data; complete social
33 security, driver's license or nondriver identification card number; specific financial or
34 account access information; data of a known child who has not attained 13 years of age; or
35 data concerning the consumer's status as the victim of a crime. If the controller knows that
36 the consumer has not attained 13 years of age, the controller may not process the consumer's
37 data for any purpose without parental consent. If the controller knows or willfully
38 disregards that the consumer is at least 13 years of age but has not attained 16 years of age,
39 the controller may not process the consumer's data for targeted advertising and must obtain
40 the consumer's consent before processing the consumer's data for sale.

41 The Act prohibits a controller from processing data in a manner that discriminates
42 against a person in violation of state or federal law. A controller is also prohibited from
43 retaliating against a consumer for exercising the consumer's rights under the Act, except
44 that a controller may offer different prices or selection of goods in connection with a

1 consumer's voluntary participation in a bona fide loyalty or discount program. A controller
2 must establish, implement and maintain reasonable data security practices and a retention
3 schedule that requires the deletion or de-identification of personal data when retention of
4 the data is no longer reasonably necessary and relevant to the purposes for which data is
5 processed or when deletion of the data is required by law. Beginning July 1, 2026, if a
6 controller engages in a data processing activity that presents a heightened risk of harm to a
7 consumer, including processing any data for targeted advertising, sale or profiling or any
8 processing of sensitive data, the controller must conduct and document a data protection
9 assessment to identify and weigh the benefits and potential risks of the processing activity.
10 The controller may be required to disclose the data protection assessment to the Attorney
11 General, who must keep it confidential, when the assessment is relevant to an investigation
12 conducted by the Attorney General. The Act further prohibits any person from establishing
13 a geofence within 1,750 feet of any in-person health care facility in the State, other than
14 the operator of the facility, for the purpose of identifying, tracking, collecting data from or
15 sending a notification regarding consumer health data to consumers who enter that area.

16 The provisions of the Act do not apply to specifically enumerated persons, including
17 the State, political subdivisions of the State and federally recognized Indian tribes in the
18 State; financial institutions or their affiliates subject to the federal Gramm-Leach-Bliley
19 Act that are directly and solely engaged in financial activities; state-licensed and authorized
20 insurers that are in compliance with applicable Maine laws governing insurer data security
21 and data privacy; and persons that both processed the personal data of fewer than 25,000
22 consumers in the preceding calendar year and derived no more than 25% of gross revenue
23 from the sale of personal data. The Act also does not apply to persons that controlled or
24 processed the personal data for purposes other than completing payment transactions of
25 fewer than 100,000 consumers in the preceding calendar year, except that, beginning
26 January 1, 2028, this exception applies only to persons that controlled or processed the
27 personal data for purposes other than completing payment transactions of fewer than
28 50,000 consumers in the preceding calendar year.

29 In addition, the provisions of the Act do not apply to specifically enumerated types of
30 data, including: nonpublic personal information regulated under the federal Gramm-Leach-
31 Bliley Act; protected health information under the federal Health Insurance Portability and
32 Accountability Act of 1996; personal data regulated by the Family Educational Rights and
33 Privacy Act of 1974; data processed and maintained by the controller regarding an
34 applicant for employment or employee to the extent the data is collected and used within
35 the context of that role; and data necessary for the controller to administer benefits. The
36 Maine Consumer Data Privacy Act also does not prohibit controllers from engaging in
37 specifically enumerated activities, including complying with Maine or federal law;
38 complying with investigations or subpoenas from governmental authorities including the
39 Federal Government and the government of the State or a federally recognized Indian tribe
40 in the State; cooperating with federal, Maine or tribal law enforcement agencies; providing
41 a product or service specifically requested by the consumer; protecting life and physical
42 safety of consumers and preventing or responding to security incidents; and conducting
43 internal product research, effectuating a product recall or performing other internal
44 operations aligned with the expectations of a consumer.

45 Violations of the Act may be enforced exclusively by the Attorney General under the
46 Maine Unfair Trade Practices Act. Absent a showing of immediate irreparable harm, the

1 Attorney General is required to provide a potential defendant with at least 30 days' notice
2 prior to initiating an enforcement action, during which time the potential defendant may
3 confer with the Attorney General to avoid the action. Any civil penalties, attorney's fees
4 or costs awarded to the State for a violation of the Act must be deposited in the Maine
5 Privacy Fund, which is established to provide funding for the enforcement staff and
6 activities of the Department of the Attorney General. The Act further requires the Attorney
7 General to submit a report by January 1, 2028 to the joint standing committee of the
8 Legislature having jurisdiction over judiciary matters regarding the operation and
9 implementation of the Act. The committee may report out legislation related to the report
10 to the Second Regular Session of the 133rd Legislature.

11 The bill also repeals the current law governing the privacy of broadband Internet access
12 service customer personal information because broadband Internet access service providers
13 are subject to the provisions of the Act.