



132nd MAINE LEGISLATURE

FIRST SPECIAL SESSION-2025

Legislative Document

No. 1224

H.P. 799

House of Representatives, March 25, 2025

An Act to Comprehensively Protect Consumer Privacy

Reference to the Committee on Judiciary suggested and ordered printed.

A handwritten signature in cursive script that reads "R B. Hunt".

ROBERT B. HUNT
Clerk

Presented by Representative ROBERTS of South Berwick.
Cosponsored by Senator BALDACCI of Penobscot and
Representatives: BRIDGEO of Augusta, COLLAMORE of Pittsfield, CROCKETT of
Portland, DILL of Old Town, HENDERSON of Rumford, STOVER of Boothbay, Senators:
GUERIN of Penobscot, MOORE of Washington.

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 PRIVACY ACT**

5 **§9601. Short title**

6 This chapter may be known and cited as "the Maine Consumer 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 used to identify a specific individual.
16 "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, or any other unambiguous affirmative act. "Consent" does not include:

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

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

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

36 **6. Consumer.** "Consumer" means an individual who is a resident of this State.
37 "Consumer" does not include an individual acting in a commercial or employment context

1 or as an employee, owner, director, officer or contractor of a company, partnership, sole
2 proprietorship, nonprofit organization or government agency whose communications or
3 transactions with the controller occur solely within the context of that individual's role with
4 the company, partnership, sole proprietorship, nonprofit organization or government
5 agency.

6 **7. Control.** "Control" means:

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

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

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

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

14 **9. COPPA.** "COPPA" means the federal Children's Online Privacy Protection Act of
15 1998, 15 United States Code, Section 6501 et seq. and the regulations, rules, guidance and
16 exemptions adopted pursuant to that Act, as that Act and such regulations, rules, guidance
17 and exemptions may be amended from time to time.

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

7 **16. Personal data.** "Personal data" means information that is linked or reasonably
8 linkable to an identified or identifiable individual. "Personal data" does not include de-
9 identified data or publicly available information.

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

15 A. The content of communications; or

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

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

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

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

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

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

36 **23. Publicly available information.** "Publicly available information" means
37 information that:

38 A. Is lawfully made available to the general public through federal, state or local
39 government records; or

40 B. Is lawfully made available to the general public through widely distributed media.

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

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

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

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

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

11 E. The disclosure of personal data that the consumer:

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

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

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

19 **25. Sensitive data.** "Sensitive data" means personal data that includes:

20 A. Data revealing racial or ethnic origins, religious beliefs, medical history, mental or
21 physical health conditions or diagnoses made by a medical professional, sexual
22 orientation or citizenship or immigration status;

23 B. The processing of genetic or biometric data for purposes of uniquely identifying an
24 individual;

25 C. Personal data collected from a consumer known to be a child;

26 D. Precise geolocation data; or

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

30 **26. Targeted advertising.** "Targeted advertising" means displaying an advertisement
31 to a consumer when the advertisement is selected based on personal data obtained or
32 inferred from that consumer's activities over time and across nonaffiliated publicly
33 accessible websites or online applications to predict that consumer's preferences or
34 interests. "Targeted advertising" does not include:

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

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

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

1 D. Processing personal data solely to measure or report advertising frequency,
2 performance or reach.

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

5 **§9603. Scope**

6 **1. Applicability; July 1, 2026 to December 31, 2027.** From July 1, 2026 to December
7 31, 2027, the provisions of this chapter apply to persons that conduct business in this State
8 or persons that produce products or services that are targeted to residents of this State and
9 that during the preceding calendar year:

10 A. Controlled or processed the personal data of not less than 100,000 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 **2. Applicability; beginning January 1, 2028.** Beginning January 1, 2028, the
16 provisions of this chapter apply to persons that conduct business in this State or persons
17 that produce products or services that are targeted to residents of this State and that during
18 the preceding calendar year:

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

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

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

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

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

29 C. A financial institution or affiliate of a financial institution, including a service
30 corporation, that is subject to Title V of the federal Gramm-Leach-Bliley Act, 15
31 United States Code, Section 6801 et seq. (1999), as amended;

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

35 E. A nonprofit organization that is established to detect and prevent fraudulent acts in
36 connection with insurance.

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

38 A. Nonpublic personal information regulated under and collected, processed, sold or
39 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,
40 15 United States Code, Section 6801 et seq. (1999), as amended;

- 1 B. Health care information as defined in Title 22, section 1711-C, subsection 1,
2 paragraph E;
- 3 C. Protected health information under the federal Health Insurance Portability and
4 Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C,
5 and the regulations, rules, guidance and exemptions adopted pursuant to that Act;
- 6 D. Patient-identifying information as described in 42 United States Code, Section
7 290dd-2;
- 8 E. Identifiable private information for the protection of human subjects in research
9 under 45 Code of Federal Regulations, Part 46;
- 10 F. Identifiable private information that is otherwise information collected as part of
11 human subjects in research pursuant to the good clinical practice guidelines issued by
12 the International Council for Harmonisation of Technical Requirements for
13 Pharmaceuticals for Human Use or successor organization;
- 14 G. The protection of human subjects in research under 21 Code of Federal Regulations,
15 Parts 50 and 56, or personal data used or shared in research, as defined in 45 Code of
16 Federal Regulations, Section 164.501, that is conducted in accordance with the
17 standards set forth in paragraphs E and F, or other research conducted in accordance
18 with applicable law;
- 19 H. Information and documents created for purposes of the federal Health Care Quality
20 Improvement Act of 1986, 42 United States Code, Section 11101 et seq;
- 21 I. Information derived from health care-related information listed in this subsection
22 that is de-identified in accordance with the requirements for de-identification pursuant
23 to the federal Health Insurance Portability and Accountability Act of 1996, 42 United
24 States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and
25 exemptions adopted pursuant to that Act;
- 26 J. Information that originates from information described in paragraphs C to I, or
27 information that is intermingled so as to be indistinguishable from information
28 described in paragraphs C to I, that a covered entity, business associate or program or
29 activity relating to substance use disorder as described in 42 United States Code,
30 Section 290dd-2, creates, processes or maintains in the same manner as is required
31 under the applicable laws and regulations cited in paragraphs C to I;
- 32 K. Information used for public health activities and purposes as authorized by the
33 federal Health Insurance Portability and Accountability Act of 1996, 42 United States
34 Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and
35 exemptions adopted pursuant to that Act;
- 36 L. The collection, maintenance, disclosure, sale, communication or use of personal
37 information bearing on a consumer's creditworthiness, credit standing, credit capacity,
38 character, general reputation, personal characteristics or mode of living by a consumer
39 reporting agency, furnisher or user that provides information for use in a consumer
40 report, and by a user of a consumer report, but only to the extent that such activity is
41 regulated by and authorized under the federal Fair Credit Reporting Act, 15 United
42 States Code, Section 1681 et seq.;

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

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

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

7 P. Data processed or maintained:

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

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

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

16 Q. Personal data collected, processed, sold or disclosed in relation to price, route or
17 service, as such terms are used in the federal Airline Deregulation Act of 1978, 49
18 United States Code, Section 40101 et seq., by an air carrier subject to that Act, to the
19 extent this chapter is preempted by the federal Airline Deregulation Act of 1978, 49
20 United States Code, Section 41713.

21 **5. Compliance with COPPA.** Controllers and processors that comply with the
22 verifiable parental consent requirements of COPPA are deemed to be compliant with an
23 obligation to obtain parental consent pursuant to this chapter.

24 **§9604. Consumer rights**

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

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

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

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

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

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

38 (1) Targeted advertising;

39 (2) The sale of personal data; or

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

3 **2. Exercise of consumer rights.** A consumer may communicate and access the
4 information necessary to exercise rights under this section by a secure and reliable means
5 established by the controller and described to the consumer in the controller's privacy
6 notice. A consumer may designate an authorized agent in accordance with section 9605 to
7 exercise the rights of the consumer to opt out of the processing of the consumer's personal
8 data as specified in subsection 1, paragraph E, subparagraphs (1) and (2). In the case of
9 processing personal data of a consumer known to be a child, the parent or legal guardian
10 may exercise consumer rights on the child's behalf. In the case of processing personal data
11 concerning a consumer subject to a guardianship, conservatorship or other protective
12 arrangement, the guardian or the conservator of the consumer may exercise rights on the
13 consumer's behalf.

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

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

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

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

32 D. If a controller is unable to authenticate a request to exercise a right afforded under
33 subsection 1, using commercially reasonable efforts, the controller is not required to
34 comply with a request to initiate an action pursuant to this section and shall provide
35 notice to the consumer that the controller is unable to authenticate the request to
36 exercise the right until the consumer provides additional information reasonably
37 necessary to authenticate the consumer and the consumer's request to exercise the right.

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

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

1 (2) Opting the consumer out of the processing of the personal data for any purpose
2 other than the purposes exempted from the provisions of this chapter.

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

12 **§9605. Authorized agent**

13 A consumer may designate another person to serve as the consumer's authorized agent,
14 and act on the consumer's behalf, to opt out of the processing of the consumer's personal
15 data for the purposes specified in section 9604, subsection 1, paragraph E, subparagraphs
16 (1) and (2). The consumer may designate an authorized agent by way of, among other
17 methods, technology, including, but not limited to, an Internet link or a browser setting,
18 browser extension or global device setting, indicating the consumer's intent to opt out of
19 such processing. A controller shall comply with an opt-out request received from an
20 authorized agent if the controller is able to verify, using commercially reasonable efforts,
21 the identity of the consumer and the authorized agent's authority to act on the consumer's
22 behalf.

23 **§9606. Actions of controllers**

24 **1. Data minimization.** A controller must comply with the requirements of this
25 subsection.

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

29 B. Except as otherwise provided in this chapter, a controller may not process personal
30 data for purposes that are neither reasonably necessary for, nor compatible with, the
31 disclosed purposes for which the data is processed, as disclosed to the consumer, unless
32 the controller obtains the consumer's consent.

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

34 A. Establish, implement and maintain reasonable administrative, technical and physical
35 data security practices to protect the confidentiality, integrity and accessibility of
36 personal data appropriate to the volume and nature of the personal data;

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

41 C. Provide an effective mechanism for a consumer to revoke the consumer's consent
42 under this section that is at least as easy as the mechanism by which the consumer

1 provided the consumer's consent and, upon revocation of the consent, cease to process
2 the data as soon as practicable, but not later than 15 days after the receipt of the request.

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

4 A. Process sensitive data concerning a consumer unless the controller obtains the
5 consumer's consent;

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

8 C. When the controller, under the circumstances, has actual knowledge or willfully
9 disregards that the consumer is at least 13 years of age but has not attained 16 years of
10 age;

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

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

14 D. Retaliate against a consumer for exercising a consumer right in this chapter or for
15 not agreeing to the collection or processing of personal data for a separate product or
16 service, including by denying goods or services, charging different prices or rates for
17 goods or services or providing a different level of quality of goods or services to the
18 consumer.

19 **4. Loyalty and rewards programs.** Subsection 3 may not be construed to require a
20 controller to provide a product or service that requires the personal data of a consumer that
21 the controller does not collect or maintain or prohibit a controller from offering a different
22 rate, level, quality or selection of goods or services to a consumer, including offering goods
23 or services for no fee, if the offering is in connection with a consumer's voluntary
24 participation in a bona fide loyalty, rewards, premium features, discounts or club card
25 program.

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

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

30 B. The purpose for processing personal data;

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

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

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

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

38 **6. Consumer rights request mechanism.** A controller shall establish, and shall
39 describe in a privacy notice, one or more secure and reliable means for consumers to submit
40 a request to exercise a consumer right pursuant to this chapter. The design of the secure
41 and reliable means must take into account the ways in which consumers normally interact

1 with the controller, the need for secure and reliable communication of requests and the
2 ability of the controller to verify the identity of the consumer making the request. A
3 controller may not require a consumer to create a new account in order to exercise a
4 consumer right, but may require a consumer to use an existing account.

5 **7. Notice of sale and targeted advertising.** If a controller sells personal data to a 3rd
6 party or processes personal data for targeted advertising, the controller shall clearly and
7 conspicuously disclose such processing, as well as the manner in which a consumer may
8 exercise the right to opt out of such processing.

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

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

16 B. May not unfairly disadvantage another controller;

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

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

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

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

27 **§9607. Responsibilities of processors and controllers**

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

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

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

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

41 **2. Contractual requirements.** A contract between a controller and a processor must
42 govern the processor's data processing procedures with respect to processing performed on

1 behalf of the controller. The contract must clearly set forth instructions for processing data,
2 the nature and purpose of processing, the type of data subject to processing, the duration of
3 processing and the rights and obligations of both parties. The contract must require that the
4 processor:

5 A. Ensure that each person processing personal data is subject to a duty of
6 confidentiality with respect to the data;

7 B. At the controller's direction, delete or return all personal data to the controller as
8 requested at the end of the provision of services, unless retention of the personal data
9 is required by law;

10 C. On the reasonable request of the controller, make available to the controller all
11 information in the processor's possession necessary to demonstrate the processor's
12 compliance with the obligations in this chapter;

13 D. Allow and cooperate with reasonable assessments by the controller or the
14 controller's designated assessor or arrange for a qualified and independent assessor to
15 conduct an assessment of the processor's policies and technical and organizational
16 measures in support of the obligations in this chapter, using an appropriate and
17 accepted control standard or framework and assessment procedure for the assessment.
18 The processor shall provide a report of the assessment to the controller upon request;
19 and

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

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

26 **4. Fact-based determination.** Determining whether a person is acting as a controller
27 or processor with respect to a specific processing of data is a fact-based determination that
28 depends upon the context in which personal data is to be processed. A person who is not
29 limited in the person's processing of personal data pursuant to a controller's instructions, or
30 who fails to adhere to the instructions, is a controller and not a processor with respect to a
31 specific processing of data. A processor that continues to adhere to a controller's
32 instructions with respect to a specific processing of personal data remains a processor. If a
33 processor begins, alone or jointly with other persons, determining the purposes and means
34 of the processing of personal data, the processor acts as a controller with respect to the
35 processing and may be subject to an enforcement action under section 9611.

36 **§9608. Data protection assessments**

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

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

42 B. The sale of personal data;

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

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

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

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

8 (4) Other substantial injury to consumers; and

9 D. The processing of sensitive data.

10 **2. Required elements.** Data protection assessments conducted pursuant to subsection
11 1 must identify and weigh the benefits that may flow, directly and indirectly, from the
12 processing to the controller, the consumer, other stakeholders and the public against the
13 potential risks to the rights of the consumer associated with the processing, as mitigated by
14 safeguards that can be employed by the controller to reduce the risks. The controller shall
15 factor into the data protection assessment the use of de-identified data and the reasonable
16 expectations of consumers, as well as the context of the processing and the relationship
17 between the controller and the consumer whose personal data will be processed.

18 **3. Attorney General disclosure; exemption from public records.** The Attorney
19 General may require that a controller disclose a data protection assessment that is relevant
20 to an investigation conducted by the Attorney General, and the controller shall make the
21 data protection assessment available to the Attorney General. The Attorney General may
22 evaluate the data protection assessment for compliance with the responsibilities set forth in
23 this chapter. A data protection assessment is confidential and exempt from disclosure under
24 Title 1, chapter 13. To the extent information contained in a data protection assessment
25 disclosed to the Attorney General includes information subject to attorney-client privilege
26 or work product protection, the disclosure does not constitute a waiver of that privilege or
27 protection.

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

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

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

37 **§9609. De-identified and pseudonymous data**

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

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

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

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

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

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

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

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

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

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

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

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

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

31 **§9610. Controller and processor; duties and obligations**

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

34 A. Comply with federal laws or regulations or the laws or rules of a state;

35 B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or
36 summons by federal or state governmental authorities or governmental authorities of a
37 federally recognized Indian tribe in this State;

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

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

- 1 E. Provide a product or service specifically requested by a consumer;
- 2 F. Perform under a contract to which a consumer is a party, including fulfilling the
3 terms of a written warranty;
- 4 G. Take steps at the request of a consumer prior to entering into a contract;
- 5 H. Take immediate steps to protect an interest that is essential for the life or physical
6 safety of the consumer or another individual and when the processing cannot be
7 manifestly based on another legal basis;
- 8 I. Prevent, detect, protect against or respond to security incidents, identity theft, fraud,
9 harassment, malicious or deceptive activities or illegal activity or preserve the integrity
10 or security of systems or investigate, report or prosecute those responsible for an action
11 described in this paragraph;
- 12 J. Engage in public or peer-reviewed scientific or statistical research in the public
13 interest that adheres to all other applicable ethics and privacy laws and is approved,
14 monitored and governed by an institutional review board that determines, or similar
15 independent oversight entities that determine:
- 16 (1) Whether the deletion of the information is likely to provide substantial benefits
17 that do not exclusively accrue to the controller;
- 18 (2) Whether the expected benefits of the research outweigh the privacy risks; and
- 19 (3) Whether the controller has implemented reasonable safeguards to mitigate
20 privacy risks associated with research, including risks associated with re-
21 identification;
- 22 K. Assist another controller, processor or 3rd party with obligations under this chapter;
23 or
- 24 L. Process personal data for reasons of public interest in the area of public health, but
25 solely to the extent that the processing is:
- 26 (1) Subject to suitable and specific measures to safeguard the rights of the
27 consumer whose personal data is being processed; and
- 28 (2) Under the responsibility of a professional subject to confidentiality obligations
29 under federal or state laws or local ordinances.
- 30 **2. Internal use.** The obligations imposed on controllers or processors under this
31 chapter do not restrict a controller's or processor's ability to collect, use or retain data for
32 internal use to:
- 33 A. Conduct internal research to develop, improve or repair products, services or
34 technology;
- 35 B. Effectuate a product recall;
- 36 C. Identify and repair technical errors that impair existing or intended functionality;
37 or
- 38 D. Perform internal operations that are reasonably aligned with the expectations of the
39 consumer or reasonably anticipated based on the consumer's existing relationship with
40 the controller, or are otherwise compatible with processing data in furtherance of the

1 provision of a product or service specifically requested by a consumer or the
2 performance of a contract to which the consumer is a party.

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

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

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

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

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

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

25 B. Apply to a person's processing of personal data in the course of the person's purely
26 personal or household activities.

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

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

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

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

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

1 **§9611. Enforcement**

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

8 **2. Notice.** Notwithstanding any provision of Title 5, section 209 to the contrary, at
9 least 30 days prior to commencement of any action under the Maine Unfair Trade Practices
10 Act to enforce this chapter, the Attorney General shall notify the person against whom an
11 action may be brought of the intended action and give the person an opportunity to cure the
12 alleged violation or violations. The Attorney General may bring an action pursuant to this
13 section only if the controller fails to cure one or more of the alleged violations described in
14 the notice within 30 days of receiving the notice.

15 **3. No private right of action.** Notwithstanding Title 5, section 213, this chapter may
16 not be construed as creating a private right of action under this chapter or any other
17 provision of law against any person based on a violation of any provision of this chapter or
18 any other law.

19 **4. Preemption.** This chapter supersedes and preempts any ordinance, resolution, rule
20 or other regulation adopted by a political subdivision of the State regarding the processing
21 of personal data by a controller or processor.

22 **§9612. Maine Privacy Fund established**

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

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

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

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

35 C. Interest earned on fund balances; and

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

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

1 1. The number of notices the Attorney General has issued under Title 10, section 9611,
2 subsection 2 and the nature of the violations alleged in the notices;

3 2. The number of persons sent a notice described in subsection 1 that conferred with
4 the Attorney General during the notice period described in Title 10, section 9611,
5 subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair
6 Trade Practices Act;

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

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

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

13 **Sec. 3. Effective date.** This Act takes effect July 1, 2026.

14 SUMMARY

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

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

1 The Act prohibits a controller from processing data in a manner that discriminates
2 against a person in violation of state or federal law. A controller is also prohibited from
3 retaliating against a consumer for exercising the consumer's rights under the Act, except
4 that a controller may offer different prices or selection of goods in connection with a
5 consumer's voluntary participation in a bona fide loyalty or discount program. A controller
6 must establish, implement and maintain reasonable data security practices. Beginning July
7 1, 2026, if a controller engages in a data processing activity that presents a heightened risk
8 of harm to a consumer, including processing any data for targeted advertising, sale or
9 profiling or any processing of sensitive data, the controller must conduct and document a
10 data protection assessment to identify and weigh the benefits and potential risks of the
11 processing activity. The controller may be required to disclose the data protection
12 assessment to the Attorney General, who must keep it confidential, when the assessment is
13 relevant to an investigation conducted by the Attorney General.

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

27 In addition, the provisions of the Act do not apply to specifically enumerated types of
28 data, including: nonpublic personal information regulated under the federal Gramm-Leach-
29 Bliley Act; health care information protected under the Maine Revised Statutes, Title 22,
30 section 1711-C; protected health information under the federal Health Insurance Portability
31 and Accountability Act of 1996; personal data regulated by the Family Educational Rights
32 and Privacy Act of 1974; data processed and maintained by the controller regarding an
33 applicant for employment or employee to the extent the data is collected and used within
34 the context of that role; and data necessary for the controller to administer benefits. The
35 Maine Consumer Privacy Act also does not prohibit controllers from engaging in
36 specifically enumerated activities, including complying with state or federal law;
37 complying with investigations or subpoenas from governmental authorities including the
38 Federal Government and the government of a state or a federally recognized Indian tribe
39 in the State; cooperating with federal, state or tribal law enforcement agencies; providing
40 a product or service specifically requested by the consumer; protecting life and physical
41 safety of consumers and preventing or responding to security incidents; and conducting
42 internal product research, effectuating a product recall or performing other internal
43 operations aligned with the expectations of a consumer.

44 Violations of the Act may be enforced exclusively by the Attorney General under the
45 Maine Unfair Trade Practices Act. Absent a showing of immediate irreparable harm, the
46 Attorney General is required to provide a potential defendant with at least 30 days' notice

1 prior to initiating an enforcement action, during which time the potential defendant may
2 cure any violation alleged in the notice. Any civil penalties, attorney's fees or costs
3 awarded to the State for a violation of the Act must be deposited in the Maine Privacy Fund,
4 which is established to provide funding for the enforcement staff and activities of the
5 Department of the Attorney General. The Act further requires the Attorney General to
6 submit a report by February 1, 2027 to the joint standing committee of the Legislature
7 having jurisdiction over judiciary matters regarding the operation and implementation of
8 the Act. The committee may report out legislation related to the report to the 133rd
9 Legislature in 2027.