



132nd MAINE LEGISLATURE

FIRST SPECIAL SESSION-2025

Legislative Document

No. 1822

H.P. 1220

House of Representatives, April 29, 2025

An Act to Enact the Maine Online Data Privacy Act

Reference to the Committee on Judiciary suggested and ordered printed.

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

ROBERT B. HUNT
Clerk

Presented by Representative KUHN of Falmouth.
Cosponsored by Senator CARNEY of Cumberland and
Representatives: Speaker FECTEAU of Biddeford, LEE of Auburn, MOONEN of Portland,
SATO of Gorham, SINCLAIR of Bath.

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 ONLINE DATA PRIVACY ACT**

5 **§9601. Short title**

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

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

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

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

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

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

24 **3. Biometric data.** "Biometric data":

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

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

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

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

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

36 **7. Consent.** "Consent":

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

5 B. Does not include:

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

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

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

11 **8. Consumer. "Consumer":**

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

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

19 **9. Consumer health data.** "Consumer health data" means personal data that a
20 controller uses to identify a consumer's physical or mental health status, and includes, but
21 is not limited to, data related to gender-affirming health care services and reproductive
22 health care services.

23 **10. Control. "Control" means:**

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

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

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

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

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

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

36 **14. De-identified data. "De-identified data" means data that cannot reasonably be used**
37 to infer information about or otherwise be linked to an identified or identifiable consumer,
38 or a device that may be linked to an identified or identifiable consumer, if the controller
39 that possesses the data:

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

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

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

5 **15. Decisions that produce legal or similarly significant effects concerning the**
6 **consumer.** "Decisions that produce legal or similarly significant effects concerning the
7 consumer" means decisions that result in the provision or denial to the consumer of
8 financial or lending services; housing; insurance; education enrollment or opportunity;
9 criminal justice; employment opportunities; health care services; or access to essential
10 goods or services.

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

13 **17. Gender identity.** "Gender identity" has the same meaning as in Title 5, section
14 4553, subsection 5-C.

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

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

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

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

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

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

34 **21. HIPAA.** "HIPAA" means the federal Health Insurance Portability and
35 Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and
36 the regulations, rules, guidance and exemptions adopted pursuant to that Act.

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

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

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

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

8 **26. Precise geolocation data.** "Precise geolocation data":

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

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

16 **27. Process.** "Process" means any operation or set of operations performed on personal
17 data or on sets of personal data by manual or automated means, including the use, storage,
18 disclosure, analysis, deletion or modification of personal data.

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

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

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

27 **31. Publicly available information.** "Publicly available information":

28 A. Means information about a consumer that a person:

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

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

32 (3) Obtains from a person to whom the consumer disclosed the information unless
33 the consumer has restricted the information to a specific audience; and

34 B. Does not include:

35 (1) Any obscene visual depiction as described in 18 United States Code, Section
36 1460;

37 (2) Biometric data;

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

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

3 (5) Intimate images a controller or processor knows have been created or shared
4 without consent of the consumer depicted in the images. For purposes of this
5 subparagraph, "intimate image" means a photograph, videotape, film or digital
6 recording of a consumer in a state of nudity or engaged in a sexual act or engaged
7 in sexual contact for which there is no public or newsworthy purpose.

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

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

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

13 B. Does not include:

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

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

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

20 (4) The disclosure of personal data when the consumer directs the controller to
21 disclose the personal data or intentionally uses the controller to interact with a 3rd
22 party;

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

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

25 (b) Did not restrict to a specific audience; or

26 (6) The disclosure of personal data to a 3rd party as an asset that is part of an actual
27 or proposed merger, acquisition, bankruptcy or other transaction in which the 3rd
28 party assumes control of all or part of the controller's assets.

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

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

33 B. Genetic data or biometric data;

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

35 D. Precise geolocation data;

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

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

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

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

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

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

8 **37. Targeted advertising.** "Targeted advertising":

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

14 B. Does not include:

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

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

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

21 (4) Processing personal data solely to measure or report advertising frequency,
22 performance or reach.

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

25 **39. Trade secret.** "Trade secret" has the same meaning as in section 1542, subsection
26 4.

27 **§9603. Applicability**

28 **1. Effective date.** The requirements of this chapter take effect on July 1, 2026.

29 **2. Persons affected.** The provisions of this chapter apply to persons that conduct
30 business in this State or persons that produce products or services that are targeted to
31 residents of this State and that during the preceding calendar year:

32 A. Controlled or processed the personal data of not less than 35,000 consumers,
33 excluding personal data controlled or processed solely for the purpose of completing a
34 payment transaction; or

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

37 **§9604. Exceptions**

38 **1. Exempt entities.** The provisions of this chapter do not apply to:

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

1 B. An organization that is exempt from taxation under Section 501(c)(3), Section
2 501(c)(4), Section 501(c)(6) or Section 501(c)(12) of the United States Internal
3 Revenue Code of 1986, as amended;

4 C. An institution of higher education;

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

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

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

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

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

23 **2. Exempt data.** The provisions of this chapter do not apply to:

24 A. Nonpublic personal information regulated under and collected, processed, sold or
25 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,
26 15 United States Code, Section 6801 et seq. (1999);

27 B. Protected health information;

28 C. Patient-identifying information as described in 42 United States Code, Section
29 290dd-2;

30 D. Identifiable private information used for the purposes of the federal policy for the
31 protection of human subjects in research under 45 Code of Federal Regulations, Part
32 46;

33 E. Identifiable private information to the extent that it is collected as part of human
34 subjects in research pursuant to the good clinical practice guidelines issued by the
35 International Council for Harmonisation of Technical Requirements for
36 Pharmaceuticals for Human Use or successor organization or in accordance with the
37 standards for the protection of human subjects in research under 21 Code of Federal
38 Regulations, Parts 50 and 56;

39 F. Personal data used or shared in research, as defined in 45 Code of Federal
40 Regulations, Section 164.501, that is conducted in accordance with the standards set
41 forth in paragraphs D and E, or other research conducted in accordance with applicable
42 law;

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

3 H. Information derived from health care-related information listed in this subsection
4 that is de-identified in accordance with the requirements for de-identification pursuant
5 to HIPAA;

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

12 J. Information used for public health activities and purposes as authorized by HIPAA;

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

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

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

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

26 O. Data processed or maintained:

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

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

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

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

40 **3. Compliance with COPPA.** Controllers and processors that comply with the
41 verifiable parental consent requirements of the federal Children's Online Privacy Protection
42 Act of 1998, 15 United States Code, Section 6501 et seq., and the regulations, rules,

guidance and exemptions adopted pursuant to that Act are compliant with an obligation to obtain parental consent pursuant to this chapter.

§9605. Consumer health data

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

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

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

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

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

§9606. Consumer rights

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

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

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

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

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

E. When processing of personal data is done by automatic means, obtain a copy of the consumer's personal data processed by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller easily and without hindrance;

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

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

(1) Targeted advertising;

(2) The sale of personal data; or

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

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

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

5 A. A controller shall establish a secure and reliable method for a consumer to exercise
6 a consumer right under this section.

7 B. A consumer may exercise a consumer right under this section using the method
8 established by the controller under paragraph A.

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

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

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

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

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

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

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

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

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

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

33 (2) Instructions for how to appeal the decision.

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

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

40 (2) Decline to act on the request.

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

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

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

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

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

14 F. A controller that has obtained personal data about a consumer from a source other
15 than the consumer is in compliance with a request to delete that data pursuant to
16 subsection 1, paragraph D by retaining a record of the deletion request and the
17 minimum data necessary for the purpose of ensuring that the consumer's personal data:

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

19 (2) Is not used for any other purpose.

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

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

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

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

34 **§9607. Authorized agent**

35 **1. Authority to designate agent to opt out of processing.** A consumer may designate
36 another person to serve as the consumer's authorized agent, and act on the consumer's
37 behalf, to exercise the consumer's right under section 9606, subsection 1, paragraph G to
38 opt out of the processing of personal data.

39 **2. Method of designating agent.** The consumer may designate an authorized agent
40 by way of, among other methods, a technology, including, but not limited to, an Internet
41 link or a browser setting, browser extension or global device setting, indicating the
42 consumer's intent to opt out of certain processing of the consumer's data.

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

5 A. The identity of the consumer; and

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

7 **§9608. Actions of controllers**

8 **1. Prohibitions.** A controller may not:

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

12 B. Sell sensitive data;

13 C. Process personal data in violation of state or federal laws that prohibit unlawful
14 discrimination;

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

16 (1) Process personal data of the consumer for the purpose of targeted advertising;

17 or

18 (2) Sell the personal data of the consumer;

19 E. Retaliate against a consumer for exercising a consumer right granted in this chapter,
20 including by denying goods or services, charging different prices or rates for goods or
21 services or providing a different level of quality of goods or services to the consumer;

22 F. Collect, process or disclose personal data or publicly available information in a
23 manner that unlawfully discriminates in or otherwise unlawfully makes unavailable the
24 equal enjoyment of goods or services on the basis of an individual's actual or perceived
25 race, color, sex, sexual orientation or gender identity, physical or mental disability,
26 religion, ancestry, national origin, age or familial status. This paragraph does not apply
27 to the collection, processing or disclosure of personal data for:

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

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

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

31 or

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

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

36 A. Limit the collection of personal data to what is reasonably necessary and
37 proportionate to provide or maintain a specific product or service requested by the
38 consumer to whom the data pertains;

39 B. Establish, implement and maintain reasonable administrative, technical and physical
40 data security practices to protect the confidentiality, integrity and accessibility of

1 personal data appropriate to the volume and nature of the personal data at issue. These
2 processes must include the disposal of personal data in accordance with a retention
3 schedule that requires the disposal of personal data by the controller when the data is
4 required to be deleted by law or when the data is no longer necessary for the purpose
5 for which the data was processed unless the consumer has consented to the retention
6 of the data for a longer period of time or retention of the data is required by law. For
7 purposes of this paragraph, "disposal of personal data" means the destruction or
8 permanent deletion of the data or other modification of the data to make the data
9 unreadable and unrecoverable; and

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

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

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

18 B. Prohibit a controller from offering a different price, rate, level, quality or selection
19 of goods or services to a consumer, including offering goods or services for no fee, if
20 the offering is in connection with a consumer's voluntary participation in a bona fide
21 loyalty, rewards, premium features, discounts or club card program, as long as the sale
22 of personal data is not a condition of participation in the program.

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

25 A. The categories of personal data, including sensitive data, processed by the
26 controller;

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

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

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

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

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

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

41 **5. Notice of sale of personal data, targeted advertising or profiling; opt-out**
42 **mechanism.** If a controller sells personal data to 3rd parties, processes personal data for

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

8 **6. Method for exercising consumer rights.** A controller shall establish, and shall
9 describe in the privacy notice as required by subsection 4, paragraph C, one or more secure
10 and reliable mechanisms for a consumer to submit a request to exercise each consumer
11 right under this chapter.

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

- 14 (1) The ways in which consumers normally interact with the controller;
15 (2) The need for secure and reliable communication of consumer requests; and
16 (3) The ability of the controller to verify the identity of a consumer making the
17 request.

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

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

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

29 (2) No later than July 1, 2026, allowing a consumer to opt out of any processing of
30 the consumer's personal data for the purposes of targeted advertising or profiling
31 or any sale of personal data through an opt-out preference signal sent, with the
32 consumer's consent, by a platform, technology or mechanism to the controller
33 indicating the consumer's intent to opt out of the processing or sale. The platform,
34 technology or mechanism:

- 35 (a) Must be consumer-friendly and easy to use by the average consumer;
36 (b) Must use clear, easy to understand and unambiguous language;
37 (c) Must be as consistent as possible with any other similar platform,
38 technology or mechanism required by federal or state law, rule or regulation;
39 (d) Must enable the controller to reasonably determine whether the consumer
40 is a resident of the State, which reasonable determination may be based on the
41 location associated with the consumer's Internet protocol address, and whether

1 the consumer has made a legitimate request to opt out of any such processing
2 or sale of the consumer's personal data;

3 (e) May not unfairly disadvantage another controller; and

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

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

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

17 **§9609. Responsibilities of processors and controllers**

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

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

- 23 (1) Instructions for processing personal data;
24 (2) The nature and purpose of the processing;
25 (3) The type of personal data subject to processing;
26 (4) The duration of the processing; and
27 (5) The rights and obligations of the processor and the controller.

28 B. The contract must require that the processor:

- 29 (1) Ensure that each person processing personal data is subject to a duty of
30 confidentiality with respect to the data;
31 (2) Establish, implement and maintain reasonable administrative, technical and
32 physical data security practices to protect the confidentiality, integrity and
33 accessibility of personal data, considering the volume and nature of the personal
34 data;
35 (3) Stop processing personal data on request by the controller made in accordance
36 with a consumer's authenticated request;
37 (4) At the controller's direction, delete or return all personal data to the controller
38 as requested at the end of the provision of service, unless retention of the personal
39 data is required by law;

(5) On the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

(6) After providing the controller an opportunity to object, engage a subcontractor to assist with processing personal data on the controller's behalf only in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data under the processor's contract with the controller;

(7) Allow and cooperate with reasonable assessments by the controller, the controller's designated assessor or a qualified and independent assessor arranged for by the processor to assess the processor's policies and technical and organizational measures in support of the obligations under this chapter. An assessment conducted under this subparagraph must be conducted using an appropriate and accepted control standard framework and assessment procedure; and

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

2. Processor responsibilities. A processor shall:

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

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

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

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

C. Provide necessary information to enable the controller to conduct and document data protection assessments as required by section 9611.

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

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

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

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

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

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

C. If a processor or 3rd party begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under section 9614.

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

§9610. Third-party responsibilities

1. Notice required. If a 3rd party intends to use or share a consumer's personal data in a manner inconsistent with the disclosures made to the consumer at the time that the personal data was collected, the 3rd party shall provide an affected consumer with notice of the new or changed use or sharing of personal data before implementing the new or changed use or sharing.

2. Method of notification. The 3rd party shall provide the notice required by subsection 1 in a manner and at a time reasonably calculated to allow a consumer to exercise the consumer's rights under this chapter.

§9611. Data protection assessments

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

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

B. The sale of personal data;

C. The processing of sensitive data; and

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

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

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

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

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

(5) Other substantial injury to a consumer.

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

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

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

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

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

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

12 (1) The use of de-identified data;

13 (2) The reasonable expectations of consumers;

14 (3) The context of the processing; and

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

17 **4. Disclosure to Attorney General.** The Attorney General may require that a
18 controller disclose to the Attorney General a data protection assessment that is relevant to
19 an investigation conducted by the Attorney General. The Attorney General may evaluate
20 the data protection assessment for compliance with the responsibilities set forth in this
21 chapter.

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

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

33 **7. Deadlines for performing data protection assessments.** A controller shall conduct
34 and document a data protection assessment as required by this section:

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

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

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

41 **§9612. De-identified data**

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

3 A. Re-identify de-identified data;

4 B. Maintain data in an identifiable form; or

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

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

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

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

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

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

25 **§9613. Exemptions**

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

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

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

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

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

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

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

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

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

4 I. Prevent, detect, protect against, investigate, prosecute those responsible for or
5 respond to security incidents, identity theft, fraud, harassment, malicious or deceptive
6 activities or any other type of illegal activity;

7 J. Preserve the integrity or security of systems; or

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

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

13 A. Effectuate a product recall;

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

15 C. Perform internal operations that:

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

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

22 **3. Evidentiary privilege.** The obligations imposed on controllers or processors under
23 this chapter do not apply when compliance with this chapter by the controller or processor
24 would violate an evidentiary privilege under state law. This chapter may not be construed
25 to prevent a controller or processor from providing personal data concerning a consumer
26 to a person covered by an evidentiary privilege under state law as part of a privileged
27 communication.

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

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

33 (1) At the time the disclosing controller or processor disclosed the personal data,
34 the disclosing controller or processor did not have actual knowledge that the
35 receiving processor or 3rd-party controller would violate this chapter; and

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

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

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

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

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

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

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

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

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

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

21 **8. Processing personal data pursuant to an exemption.** A person that processes
22 personal data pursuant to an exemption in this section may not be considered a controller
23 solely based on that processing of personal data.

24 **§9614. Enforcement**

25 **1. Violation as unfair trade practice; exclusive Attorney General enforcement.** A
26 violation of this chapter constitutes an unfair trade practice under the Maine Unfair Trade
27 Practices Act, except that the provisions of Title 5, section 213 do not apply to this chapter
28 and except as provided in subsection 2. The Attorney General has the exclusive authority
29 to enforce violations of this chapter under the Maine Unfair Trade Practices Act.

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

40 A. The number of alleged violations;

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

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

D. The likelihood of injury to the public;

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

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

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

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

1. The number of notices the Attorney General has issued under Title 10, section 9614, subsection 2 and the nature of the violations alleged in the notices;

2. The number of persons sent a notice described in subsection 1 that conferred with the Attorney General during the notice period described in Title 10, section 9614, subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair Trade Practices Act;

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

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

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

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

SUMMARY

This bill enacts the Maine Online Data Privacy Act, which takes effect July 1, 2026. The Act regulates the collection, use, processing, disclosure, sale and deletion of nonpublicly available personal data by a person that conducts business in this State or that produces products or services targeted to residents of this State, referred to in the Act as a "controller," if the personal data is linked or can be reasonably linked to an identified or identifiable individual who is a resident of this State, referred to in the Act as a "consumer," or is linked or reasonably can be linked to a device that is linked or reasonably can be linked to an identified or identifiable consumer. Under the Act, a controller must limit the collection and processing of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer, except that the controller must limit the collection and processing of certain sensitive data to what is strictly necessary to provide or maintain a specific product or service requested by the consumer. Under the Act, "sensitive data" includes data revealing a consumer's race or ethnic origins, religious beliefs, mental or physical health conditions or diagnoses, sexual orientation, gender identity, citizenship or immigration status; genetic or biometric data; precise geolocation data; social security, driver's license or nondriver identification card numbers; specific financial or account access information; data of a minor under 18 years of age; or data concerning the consumer's status as the victim of a crime.

1 The Act establishes that consumers have the right to confirm whether a controller is
2 processing their data; correct inaccuracies in their personal data; require the controller to
3 delete any portion of their personal data that the controller is not required to maintain by
4 law; obtain a copy of their personal data in a format that can be readily transferred to
5 another controller; obtain a list of the 3rd parties to which the controller has sold personal
6 data; and opt out of the processing of their personal data for purposes of targeted
7 advertising, sale or consumer profiling. The Act also prohibits a controller from selling
8 any sensitive data; processing the personal data of a minor for purposes of targeted
9 advertising or sale; processing personal data in a manner that discriminates against a person
10 in violation of state or federal law; and retaliating against a consumer for exercising a
11 consumer's rights under the Act, except that a controller may offer different prices or
12 selection of goods in connection with a consumer's voluntary participation in a bona fide
13 loyalty or discount program.

14 The Act also requires a controller to provide consumers with a privacy notice
15 specifying how a consumer may exercise the consumer's rights under the Act; the
16 categories of personal data processed by the controller; the purposes for processing the
17 personal data; the categories of personal data transferred to 3rd parties; and the categories
18 of 3rd parties to whom personal data is shared. The controller must establish, implement
19 and maintain reasonable data security practices and a retention schedule that requires the
20 disposal of personal data by the controller either when deletion is required by law or when
21 the data is no longer necessary for the purpose for which it was processed and retention of
22 the data is not required by law. The controller must also require, by contract, that any
23 person who processes a consumer's personal data on behalf of the controller treats the
24 personal data confidentially and deletes or returns all personal data to the controller at the
25 end of the processing, unless retention of the data is required by law. If a controller engages
26 in a data processing activity that presents a heightened risk of harm to a consumer,
27 including processing any data for targeted advertising, sale or profiling or any processing
28 of sensitive data, the controller must conduct and document a data protection assessment
29 identifying and weighing the benefits and potential risks of the processing activity. The
30 controller may be required to disclose the data protection assessment to the Attorney
31 General, who must keep it confidential, when the assessment is relevant to an investigation
32 conducted by the Attorney General.

33 The Act further prohibits any person from establishing a geofence within 1,750 feet of
34 any in-person health care facility in the State, other than the operator of the facility, for the
35 purpose of identifying, tracking, collecting data from or sending a notification regarding
36 consumer health data to consumers who enter that area.

37 The provisions of the Act do not apply to specifically enumerated persons, including
38 the State, political subdivisions of the State and federally recognized Indian tribes in the
39 State; nonprofit organizations; institutions of higher education; federally registered national
40 securities associations; supervised financial organizations and service corporations; health
41 care facilities and health care practitioners as well as their affiliates that both qualify as
42 business associates and provide services only to covered entities; state-licensed and
43 authorized insurers that are in compliance with applicable Maine laws governing insurer
44 data security and data privacy; and broadband Internet service providers to the extent those
45 providers are subject to the data privacy requirements of the Maine Revised Statutes, Title
46 35-A, section 9301. In addition, the provisions of the Act do not apply to specifically

1 enumerated types of data, including, for example: nonpublic personal information
2 regulated under the federal Gramm-Leach-Bliley Act; protected health information under
3 the federal Health Insurance Portability and Accountability Act of 1996; personal data
4 regulated by the Family Educational Rights and Privacy Act of 1974; data processed and
5 maintained by the controller regarding an applicant for employment or employee to the
6 extent the data is collected and used within the context of that role; and data necessary for
7 the controller to administer benefits.

8 The Act also does not prohibit controllers from engaging in specifically enumerated
9 activities, including, for example: complying with state or federal law; complying with
10 investigations or subpoenas from federal, state or tribal governmental authorities;
11 cooperating with federal, tribal or Maine law enforcement agencies; providing a product or
12 service specifically requested by the consumer; protecting life and physical safety of
13 consumers; and preventing or responding to security incidents. The Act also does not
14 prohibit a controller from using personal data collected in a lawful manner to effectuate a
15 product recall, identify and repair technical errors and perform internal operations that are
16 reasonably aligned with a consumer's expectations or otherwise compatible with providing
17 the product or service specifically requested by the consumer.

18 Violations of the Act may be enforced exclusively by the Attorney General under the
19 Maine Unfair Trade Practices Act. If the violation occurs on or before April 1, 2027, the
20 Attorney General may provide a potential defendant with a notice of violation at least 60
21 days prior to initiating an enforcement action, during which time the potential defendant
22 may cure the violation to avoid the enforcement action. The Act further requires the
23 Attorney General to submit a report by February 1, 2027 to the joint standing committee of
24 the Legislature having jurisdiction over judiciary matters regarding the implementation and
25 operation of the Act. The committee may report out legislation related to the report to the
26 133rd Legislature in 2027.