

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

Date: (Filing No. S- )

**JUDICIARY**

Reproduced and distributed under the direction of the Secretary of the Senate.

**STATE OF MAINE  
SENATE  
131ST LEGISLATURE  
SECOND REGULAR SESSION**

COMMITTEE AMENDMENT “ ” to S.P. 807, L.D. 1973, “An Act to Enact the Maine Consumer Privacy Act”

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

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

**CHAPTER 1057**

**MAINE CONSUMER PRIVACY ACT**

**§9601. Short title**

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

**§9602. Definitions**

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

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

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

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

**COMMITTEE AMENDMENT**

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

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

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

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

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

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

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

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

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

27 **8. Control.** "Control" means:

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

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

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

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

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

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

1           **12. Decisions that produce legal or similarly significant effects concerning the**  
2 **consumer.** "Decisions that produce legal or similarly significant effects concerning the  
3 consumer" means decisions that result in the provision or denial to the consumer of  
4 financial or lending services, housing, insurance, education enrollment or opportunity,  
5 criminal justice, employment opportunities, health care services or access to essential  
6 goods or services.

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

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

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

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

16           **14. Federally recognized Indian tribe in this State.** "Federally recognized Indian  
17 tribe in this State" means the Houlton Band of Maliseet Indians, the Mi'kmaq Nation, the  
18 Passamaquoddy Tribe or the Penobscot Nation when the band, nation or tribe is acting in  
19 a governmental capacity and not in a business capacity. "Federal recognized Indian tribe  
20 in this State" does not include a business entity, including any federally chartered tribal  
21 corporation or other business entity owned or partly owned by the Houlton Band of  
22 Maliseet Indians, the Mi'kmaq Nation, the Passamaquoddy Tribe or the Penobscot Nation.

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

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

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

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

38           A. The content of communications; or

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

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

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

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

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

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

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

17           A. Means information that is:

18                   (1) Lawfully made available to the general public through federal, state or local  
19 government records;

20                   (2) Made available to the general public through widely distributed media;

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

27                   (4) Disclosed to the general public as required by federal, state or local law; or

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

31           B. Does not include:

32                   (1) Any obscene visual depiction as described in 18 United States Code, Section  
33 1460;

34                   (2) Biometric data;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24 B. Genetic or biometric data;

25 C. Consumer health data;

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

27 E. Precise geolocation data;

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

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

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

37 **27. Targeted advertising.** "Targeted advertising" means displaying an advertisement  
38 to a consumer when the advertisement is selected based on personal data obtained or  
39 inferred from that consumer's activities over time and across nonaffiliated publicly

1 accessible websites or online applications to predict that consumer's preferences or  
2 interests. "Targeted advertising" does not include:

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

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

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

9 D. Processing personal data solely to measure or report advertising frequency,  
10 performance or reach.

11 **28. Trade secret.** "Trade secret" has the same meaning as in Title 10, section 1542,  
12 subsection 4.

13 **§9603. Scope**

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

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

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

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

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

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

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

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

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

37 C. A financial institution or affiliate of a financial institution, including a service  
38 corporation, that is subject to the federal Gramm-Leach-Bliley Act, 15 United States  
39 Code, Section 6801 et seq. (1999) only if that institution or affiliate is directly and  
40 solely engaged in financial activities as described in 12 United States Code, Section

1 1843(k) (2023). For purposes of this paragraph, "service corporation" has the same  
2 meaning as in Title 9-B, section 131, subsection 37;

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

6 E. A person or entity that is subject to Title 35-A, section 9301 as a provider of  
7 broadband Internet access service that provides broadband Internet access service on  
8 its own or as part of a bundle.

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

10 A. Nonpublic personal information regulated under and collected, processed, sold or  
11 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,  
12 15 United States Code, Section 6801 et seq. (1999);

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

16 C. Patient-identifying information as described in 42 United States Code, Section  
17 290dd-2;

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

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

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

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

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

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

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

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

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

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

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

18 O. Data processed or maintained:

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

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

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

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

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

38 **§9604. Consumer rights**

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

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



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

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

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

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

10 (1) Targeted advertising;

11 (2) The sale of personal data; or

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

14 **2. Exercise of consumer rights.** A consumer may communicate and access the  
15 information necessary to exercise rights under this section by a secure and reliable means  
16 established by the controller and described to the consumer in the controller's privacy  
17 notice. A consumer may designate an authorized agent in accordance with section 9605 to  
18 exercise the rights of the consumer to opt out of the processing of the consumer's personal  
19 data as specified in subsection 1, paragraph E. In the case of processing personal data of a  
20 consumer known to be a child, the parent or legal guardian may exercise consumer rights  
21 on the child's behalf. In the case of processing personal data concerning a consumer subject  
22 to a guardianship, conservatorship or other protective arrangement, the guardian or the  
23 conservator of the consumer may exercise rights on the consumer's behalf.

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

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

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

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

42 D. If a controller is unable to authenticate a request to exercise a right afforded under  
43 subsection 1, using commercially reasonable efforts, the controller is not required to

1 comply with a request to initiate an action pursuant to this section and shall provide  
2 notice to the consumer that the controller is unable to authenticate the request to  
3 exercise the right until the consumer provides additional information reasonably  
4 necessary to authenticate the consumer and the consumer's request to exercise the right.

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

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

20 **§9605. Authorized agent**

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

31 **§9606. Actions of controllers**

32 **1. Data minimization.** A controller must comply with the requirements of this  
33 subsection.

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

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

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

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

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

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

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

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

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

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

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

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

29 (1) The controller's identity;

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

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

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

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

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

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

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

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

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

9 D. Retaliate against a consumer for exercising a consumer right in this chapter or for  
10 not agreeing to the collection or processing of personal data for a separate product or  
11 service, including by denying goods or services, charging different prices or rates for  
12 goods or services or providing a different level of quality of goods or services to the  
13 consumer.

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

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

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

22 B. The purpose for processing personal data;

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

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

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

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

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

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

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

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

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

23           **8. Universal opt-out mechanism.** No later than December 1, 2026, a controller shall  
24           allow a consumer to opt out of any processing of the consumer's personal data for the  
25           purposes of targeted advertising or any sale of personal data through an opt-out preference  
26           signal sent, with the consumer's consent, by a platform, technology or mechanism to the  
27           controller indicating the consumer's intent to opt out of any such processing or sale. The  
28           platform, technology or mechanism:

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

30           B. May not unfairly disadvantage another controller;

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

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

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

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

41           **§9607. Responsibilities of processors and controllers**

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

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

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

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

14           **2. Contractual requirements.** A contract between a controller and a processor must  
15 govern the processor's data processing procedures with respect to processing performed on  
16 behalf of the controller. The contract must clearly set forth instructions for processing data,  
17 the nature and purpose of processing, the type of data subject to processing, the duration of  
18 processing and the rights and obligations of both parties. The contract must require that the  
19 processor:

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

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

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

28           D. Allow and cooperate with reasonable assessments by the controller or the  
29 controller's designated assessor or arrange for a qualified and independent assessor to  
30 conduct an assessment of the processor's policies and technical and organizational  
31 measures in support of the obligations in this chapter, using an appropriate and  
32 accepted control standard or framework and assessment procedure for the assessment.  
33 The processor shall provide a report of the assessment to the controller upon request;  
34 and

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

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

41           **4. Fact-based determination.** Determining whether a person is acting as a controller  
42 or processor with respect to a specific processing of data is a fact-based determination that  
43 depends upon the context in which personal data is to be processed. A person who is not

1 limited in the person's processing of personal data pursuant to a controller's instructions, or  
2 who fails to adhere to the instructions, is a controller and not a processor with respect to a  
3 specific processing of data. A processor that continues to adhere to a controller's  
4 instructions with respect to a specific processing of personal data remains a processor. If a  
5 processor begins, alone or jointly with other persons, determining the purposes and means  
6 of the processing of personal data, the processor acts as a controller with respect to the  
7 processing and may be subject to an enforcement action under section 9612.

8 **§9608. Data protection assessments**

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

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

14 B. The sale of personal data;

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

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

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

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

22 (4) Other substantial injury to consumers; and

23 D. The processing of sensitive data.

24 **2. Required elements.** Data protection assessments conducted pursuant to subsection  
25 1 must identify and weigh the benefits that may flow, directly and indirectly, from the  
26 processing to the controller, the consumer, other stakeholders and the public against the  
27 potential risks to the rights of the consumer associated with the processing, as mitigated by  
28 safeguards that can be employed by the controller to reduce the risks. The controller shall  
29 factor into the data protection assessment the use of de-identified data and the reasonable  
30 expectations of consumers, as well as the context of the processing and the relationship  
31 between the controller and the consumer whose personal data will be processed.

32 **3. Attorney General disclosure; exemption from public records.** The Attorney  
33 General may require that a controller disclose a data protection assessment that is relevant  
34 to an investigation conducted by the Attorney General, and the controller shall make the  
35 data protection assessment available to the Attorney General. The Attorney General may  
36 evaluate the data protection assessment for compliance with the responsibilities set forth in  
37 this chapter. A data protection assessment is confidential and exempt from disclosure under  
38 Title 1, chapter 13. To the extent information contained in a data protection assessment  
39 disclosed to the Attorney General includes information subject to attorney-client privilege or  
40 work product protection, the disclosure does not constitute a waiver of that privilege or  
41 protection.

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

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

8           **6. Application.** A controller is not required to conduct a data protection assessment  
9 under this section for any processing activity created or initiated before July 1, 2025.

10 **§9609. De-identified and pseudonymous data**

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

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

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

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

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

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

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

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

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

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

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

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



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

5           **§9610. Geofence**

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

12           **§9611. Controller and processor; duties and obligations**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15                   A. Conduct internal research to develop, improve or repair products, services or  
16                   technology;

17                   B. Effectuate a product recall;

18                   C. Identify and repair technical errors that impair existing or intended functionality;  
19                   or

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

25                   **3. Evidentiary privilege.** The obligations imposed on controllers or processors under  
26                   this chapter do not apply when compliance with this chapter by the controller or processor  
27                   would violate an evidentiary privilege under the laws of this State. Nothing in this chapter  
28                   may be construed to prevent a controller or processor from providing personal data  
29                   concerning a consumer to a person covered by an evidentiary privilege under the laws of  
30                   this State as part of a privileged communication.

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

41                   **5. Exemptions.** Nothing in this chapter may be construed to:

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

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

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

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

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

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

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

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

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

24 **§9612. 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 207, subsection 2 do not apply  
28 to this chapter and except as provided in subsections 2 and 3. The Attorney General has the  
29 exclusive authority to enforce violations of this chapter under the Maine Unfair Trade  
30 Practices Act.

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

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

1 **§9613. Maine Privacy Fund established**

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

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

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

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

14 C. Interest earned on fund balances; and

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

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

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

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

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

29 4. Any recommendations the Attorney General has for improving the operation of Title  
30 10, chapter 1057.

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

33 **Sec. 3. Appropriations and allocations.** The following appropriations and  
34 allocations are made.

35 **ATTORNEY GENERAL, DEPARTMENT OF THE**

36 **Administration - Attorney General 0310**

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

|                                  |                |                |
|----------------------------------|----------------|----------------|
| 39 <b>GENERAL FUND</b>           | <b>2023-24</b> | <b>2024-25</b> |
| 40 POSITIONS - LEGISLATIVE COUNT | 0.000          | 4.000          |
| 41 Personal Services             | \$0            | \$224,428      |



1 that a controller may offer different prices or selection of goods in connection with a  
2 consumer's voluntary participation in a bona fide loyalty or discount program. A controller  
3 must establish, implement and maintain reasonable data security practices and a retention  
4 schedule that requires the deletion or de-identification of personal data when retention of  
5 the data is no longer reasonably necessary and relevant to the purposes for which data is  
6 processed or when deletion of the data is required by law. Beginning July 1, 2025, if a  
7 controller engages in a data processing activity that presents a heightened risk of harm to a  
8 consumer, including processing any data for targeted advertising, sale or profiling or any  
9 processing of sensitive data, the controller must conduct and document a data protection  
10 assessment to identify and weigh the benefits and potential risks of the processing activity.  
11 The controller may be required to disclose the data protection assessment to the Attorney  
12 General, who must keep it confidential, when the assessment is relevant to an investigation  
13 conducted by the Attorney General. The Act further prohibits any person from establishing  
14 a geofence within 1,750 feet of any in-person health care facility in the State, other than  
15 the operator of the facility, for the purpose of identifying, tracking, collecting data from or  
16 sending a notification regarding consumer health data to consumers who enter that area.

17 The provisions of the Act do not apply to specifically enumerated persons, including  
18 the State, political subdivisions of the State and federally recognized Indian tribes in the  
19 State; financial institutions or their affiliates subject to the federal Gramm-Leach-Bliley  
20 Act that are directly and solely engaged in financial activities; state-licensed and authorized  
21 insurers that are in compliance with applicable Maine laws governing insurer data security  
22 and data privacy; broadband Internet access service providers subject to the data privacy  
23 requirements of the Maine Revised Statutes, Title 35-A, section 9301; and persons that  
24 both processed the personal data of fewer than 25,000 consumers in the preceding calendar  
25 year and derived no more than 25% of gross revenue from the sale of personal data. The  
26 Act also does not apply to persons that controlled or processed the personal data for  
27 purposes other than completing payment transactions of fewer than 100,000 consumers in  
28 the preceding calendar year, except that, beginning January 1, 2027, this exception applies  
29 only to persons that controlled or processed the personal data for purposes other than  
30 completing payment transactions of fewer than 50,000 consumers in the preceding calendar  
31 year.

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

