"Redline" of LD 1973 - From Senator Keim (12/19/23)

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

# An Act to Enact the Maine Consumer Privacy Act

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

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

## CHAPTER 1057

## MAINE CONSUMER PRIVACY ACT

### §9601. 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. Business associate.** "Business associate" has the same meaning as in 45 Code of Federal Regulations, Section 160.103.

Biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a physical or digital photograph, a video or audio recording or data generated therefrom unless such data is generated to identify a specific individual, or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Section 1320d et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act.

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

**4. Consent.** "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means. "Consent" does not include:

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

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

C. Agreements obtained through the use of a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decision making or choice.

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

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

# "Redline" of LD 1973 - From Senator Keim (12/19/23)



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

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

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

**7. Controller.** "Controller" means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

**8. Covered entity.** "Covered entity" has the same meaning as in the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Section 1320d et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act.

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

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

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

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

~~**10. Institution of higher education.** "Institution of higher education" means a person that is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.~~

~~**11. Nonprofit organization.** "Nonprofit organization" means an organization that is exempt from taxation under Section 501(c)(3), Section 501(c)(4), Section 501(c)(6) or Section 501(c)(12) of the United States Internal Revenue Code of 1986, as amended.~~

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

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

A. The content of communications; or

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

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

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

**16. Protected health information.** "Protected health information" has the same meaning as in the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Section 1320d et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act.

# "Redline" of LD 1973 - From Senator Keim (12/19/23)

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

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

**18. Publicly available information.** (1) "Publicly available information" means information that is:

A. Lawfully made available through federal, state or municipal government records; ~~if the covered entity collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity.~~

B. ~~or W~~widely distributed media; ~~andor~~

C. A website or online service made available to all members of the public, for free or for a fee, can log in to the website or online service;

D. A disclosure that has been made to the general public as required by federal, state, or local law; or

E. The visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession.

(2) For purposes of this paragraph, information from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has restricted the information to a specific audience.

(3) The term "publicly available information" does not include:

A. Any obscene visual depiction, as defined in 18 U.S.C. section 1460;

~~B. Any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual.~~

B. Biometric information;

~~B. Publicly available information that has been combined with covered data.~~

C. Genetic information, unless otherwise made available by the individual to whom the information pertains; or

D. Intimate images known to have been created or shared without consent.

~~B. Information that a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.~~

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

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

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

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

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

E. The disclosure of personal data that the consumer:

**Commented [A1]:** This new definition has come from the OAG, with portions that were considered to have constitutional concerns stricken.

**Commented [A2]:** Would the word transfer and exchange have the same meaning here?

**Commented [A3]:** This language still poses a loophole and needs further consideration. A business can have any number of affiliates!
It is somewhat addressed in §9605, because it can be argued whether such sharing would violate consumer expectations.

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

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

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

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

**20. Sensitive data.** "Sensitive data" means personal data that includes:

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

B. The processing of genetic or biometric data for the purpose of uniquely identifying an individual;

C. Personal data collected from a known child; ~~or~~

D. Precise geolocation data; ~~.~~

E. The processing of a social security number, driver's license, state identification number, billing, financial, or payment method information.

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

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

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

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

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

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

**§9602. Scope**

**1. Applicability.** The provisions of this chapter apply to persons that conduct business in this State or persons that produce products or services that are targeted to residents of this State and that during the preceding calendar year:

A. Controlled or processed the personal data of ~~not less than 10050,000~~ consumers ~~any consumers~~, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or.

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

**2. Nonapplicability.** The provisions of this chapter do not apply to:

A. A body, authority, board, bureau, commission, district or agency of this State or of a political subdivision of this State;

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

**Commented [A4]:** Suggest different enforcement or implementation timeline for small businesses rather than exemption.

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

~~C. An institution of higher education;~~

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

E. A financial institution or data that is subject to the federal Gramm-Leach-Bliley Act, 15 United States Code, Section 6801 et seq. (1999);

F. A covered entity or business associate;

G. Protected health information under the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Section 1320d et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

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

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

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

K. The protection of human subjects in research under 21 Code of Federal Regulations, Parts 50 and 56, or personal data used or shared in research, as defined in 45 Code of Federal Regulations, Section 164.501, that is conducted in accordance with the standards set forth in paragraphs I and J, or other research conducted in accordance with applicable law;

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

M. Information derived from health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Section 1320d et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

N. Information originating from and intermingled to be indistinguishable with information described in this subsection that is maintained by a covered entity or business associate, program or qualified service organization, as specified in 42 United States Code, Section 290dd-2 et seq.;

O. Information used for public health activities and purposes as authorized by the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Section 1320d et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

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

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

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

**Commented [A5]:** GLBA applies quite broadly. While we likely agree that our local banks and credit unions are not the target of this bill, GLBA institutions could include payday lenders, mortgage brokers, tax preparers and check-cashers -- all subject to GLBA and would be exempted.
GLBA itself is not a particularly strong privacy law – it requires notice and security regulations, but the federal GLBA does not have, for example, an opt-out provision. (California does.)

Perhaps we could add a provision, as in California, that would also require some data control by consumers. I don't have this language but we can look at this further.

**Commented [A6]:** Too broad?

**Commented [A7]:** Too broad?

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

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

T. Data processed or maintained:

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

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

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

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

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

**§9603. Consumer rights**

**1. Consumer rights.** A consumer is entitled to:

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

B. 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;

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

D. 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 without hindrance, when the processing is carried out by automated means, as long as the controller is not required to reveal a trade secret.

**2. Opt-~~in~~out.**

**(A)** A controller may not process the personal data of a consumer for the purposes of targeted advertising, the sale of personal data or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer ~~unless~~ if the consumer opts ~~in~~ out ~~to~~ of ~~the~~ such processing.

**(B)** A controller that processes personal data as described in subsection (A) of this paragraph shall:

(i) Provide a clear and conspicuous link on the controller's internet homepage(s) titled "Do Not Sell My Personal Data," that directs the consumer, or a person authorized by the consumer, to an internet web page ~~that~~which enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal data;

**Commented [A8]:** Too broad?

**Commented [A9]:** It was suggested that since federal law preempts state law this exemption is unnecessary for us to include, and should be removed federally.

**Commented [A10]:** Looking for tighter language for this section.

**Commented [A11]:** What could this mean?

**Commented [A12]:** What could this mean?

**Commented [A13]:** The goal of this change is to provide to Mainers the same type of obvious banner that CA residents have- so that people have the ability to opt out in an obvious way. This will prevent consent fatigue, and help Mainers know and consider exercising their right to privacy. This provide a learning opportunity- know your rights…

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

(ii) Provide a clear and conspicuous link on the controller's internet homepage(s) titled "Opt Me Out of Targeted Advertising," that directs the consumer, or a person authorized by the consumer, to an internet web page ~~that~~which enables a consumer, or a person authorized by the consumer, to opt-out of the processing of personal data for the purposes of targeted advertising; or

(iii) At the controller's discretion, provide a single, clearly-labeled link on the controller's internet homepage(s) ~~,~~ in lieu of the separate links described in (i) and (ii),if such a link easily allows a consumer to opt out of the processing of both the sale of the consumer's personal data and the processing of personal data for the purpose of targeted advertising.

(iv) If a controller maintains a privacy-specific section of its internet website that provides the above-mentioned consumer controls as well as additional privacy controls, the controller may satisfy the requirements of this section by providing a clear and conspicuous link titled "Your Privacy Choices" or substantially similar language that directs the consumer to such privacy-specific section of its internet website.

**3. Exercise of consumer rights.** A consumer may communicate and access the information necessary to exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 9604 to exercise the rights of the consumer to opt ~~in to~~out of the processing of the consumer's personal data for purposes of subsection 2 on behalf of the consumer. In the case of processing personal data of a child, the parent or legal guardian may exercise consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise rights on the consumer's behalf.

**Commented [A14]:** Consider allowing an authorized agent to complete requests to know, correct, and delete data- not just out-out of processing.

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

A. A controller shall respond to the consumer without undue delay, but not later than the 45th day after receipt of the request.

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

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

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

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

that the consumer's personal data remains deleted from the controller's records and not using the retained data for any other purpose pursuant to the provisions of this chapter.

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

**§9604. Authorized agent**

A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to opt ~~in to~~ out of t~~t~~he processing of the consumer's personal data for the purposes specified in section 9603, subsection 2. A controller shall comply with an opt-~~in~~ out request received from an authorized agent if the controller is able to verify, using commercially reasonable efforts, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

**§9605. Actions of controllers**

**1. Duties.** A controller shall:

A. Limit the collection of personal data to what is adequate, relevant and reasonably necessary to provide the service requested by the ~~in relation to the purposes for which the data is processed, as disclosed to the~~ consumer;

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

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

D. Provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of the consent, cease to process the data as soon as practicable, but not later than 45 days after the receipt of the request.

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

A. Process sensitive data concerning a consumer without obtaining the consumer's consent;

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

C. Process the personal data of a consumer for purposes of targeted advertising or sell the consumer's personal data without the consumer's consent under circumstances when a controller has actual knowledge and willfully disregards that the consumer is at least 13 years of age but has not attained 16 years of age;

D. Discriminate against a consumer for exercising a consumer right in this chapter, including by denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer; or

**Commented [A15]:** AG office suggested moving this to 18, but that seems incongruous with the other legal rights of 16 year old.

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

E. Except as otherwise provided in this chapter, process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

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

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

**4. Transparency.** A controller shall provide consumers with an accessible, clear and meaningful privacy notice that includes:

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

B. The purpose for processing personal data;

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

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

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

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

**5. Sale and targeted advertising transparency.** A controller may not sell personal data to 3rd parties or process personal data for targeted advertising unless the individual to whom the personal data pertains opts in to the sale.

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

**7. ~~Deletion~~Universal Opt-Out Mechanism.** No later than July 1, 2025, a controller shall ~~delete a consumer's~~allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or sale of the personal data~~ through an opt-out preference signal sent, with such consumer's consent, by a platform, technology, or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale~~if the consumer has not opted in to the targeted advertising or sale~~. The platform, technology or mechanism for opting ~~in~~ out may not unfairly disadvantage another controller or make use of a default setting but rather require the consumer to make an affirmative, freely given and unambiguous choice to opt ~~in~~ out of~~to~~ processing of the consumer's personal data pursuant to this chapter. The platform, technology or mechanism must:

A. Be consumer-friendly and easy to use by the average consumer;

B. Be as consistent as possible with another similar platform, technology or mechanism required by federal or state law; and

**Commented [A16]:** This part of the bill was not well-worded originally and needed change. There is a right to delete **§9603**

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

C. Enable the controller to reasonably~~accurately~~ determine whether the consumer is a resident of this State and whether the consumer has made a legitimate request to opt ~~in to~~out of the sale of the consumer's personal data or targeted advertising.

**8. Opt-~~in~~ out preference signal.** A controller that recognizes an opt-~~in~~ out preference signal that has been approved by the laws of other states is in compliance with this subsection.

**§9606. Responsibilities of processors and controllers**

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

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

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

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

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

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

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

C. 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;

D. Allow and cooperate with reasonable assessments by the controller or the controller's designated assessor, ~~.~~ or t~~T~~he processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations in this chapter, using an appropriate and accepted control standard or framework and assessment procedure for the assessment. The processor shall provide a report of the assessment to the controller upon request; and

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

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

**Commented [A17]:** "accurate" location may allow a business to require onerous proof of residency- and more disclosure of data. This language change is meant to address that concern.

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

**4. Fact-based determination.** Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in the person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor acts as a controller with respect to the processing and may be subject to an enforcement action under section 9610.

**§9607. Data protection assessments**

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

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

B. The sale of personal data;

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

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

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

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

(4) Other substantial injury to consumers; and

D. The processing of sensitive data.

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

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

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

**5. Reciprocity.** If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment satisfies the requirements established

in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

**§9608. De-identified and pseudonymous data**

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

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

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

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

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

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

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

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

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

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

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

**4. Pseudonymous data requirements.** The rights afforded under section 9603, subsection 1 do not apply to pseudonymous data in cases when the controller is able to demonstrate that information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

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

**§9609. Limitations**

**1. Limitations on use.** Nothing in this chapter may be construed to restrict a controller's or processor's ability to:

A. Comply with federal, Maine state ~~or municipal~~ ordinances or regulations;

B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, Maine state, ~~municipal~~ or other governmental authorities;

C. Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or municipal ordinances or regulations

**Commented [A18]:** OAG suggest limit to Maine

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Effectuate a product recall;

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

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

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

# "Redline" of LD 1973 - From Senator Keim (12/19/23)

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

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

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

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

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

(2) Under Title 16, section 61; or

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

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

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

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

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

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

**§9610. Enforcement**

**1. Exclusive Attorney General enforcement.** The Attorney General has the exclusive authority to enforce violations of this chapter. The provisions of Title 5, section 207, subsection 2 do not apply to this chapter. Nothing in this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of this or any other law.

**2. Right to cure.**

(A) During the period beginning on July 1, 2025~~6~~ and ending on December 31, 2027, the Attorney General shall, b~~B~~efore initiating an action for a violation of a provision of this chapter, ~~the Attorney General~~ shall issue a notice of violation to the controller identifying the specific provisions of this chapter the Attorney General alleges have been or are being violated, if the Attorney General determines that a cure is possible. If the controller or processor cures the violation before the 30th day after the date of the notice and provides the Attorney General an express written statement that the alleged violations have been cured and that no such

**Commented [A19]:** Enforcement has so many options. The proposed language is one, though it does not accurately capture my thoughts.

The purpose of enforcement at the early stages of this complex law should be to reverse unintentional mistakes during the learning curve. This could be done with a 30 day right to cure that is limited to a specific timeframe (one year?) with an option for AG enforcement if the issue is one of blatantly ignoring the law and/or causing a high level of harm.

The bill should include language for a report back by the AG to JUD that updates the legislature on the law, and authorizes JUD to report out a bill with changes that are needed. We are way behind in this and the landscape is constantly evolving- forcing ourselves to stay current with privacy would be good policy.

It may also be helpful to establish a right to cure portal that consumers can utilize themselves, to reduce the burden on the AG. (Small fiscal note?)

Civil violation/ PRA of a limited amount, should be saved for future considerations when the AG reports back on the law and its utilization.

However, intentional and consistent violations should always be able to be prosecuted at the AGs discretion.

A PRA will make Maine businesses a target for those seeking to earn a buck through lawsuits. We cannot allow our law to be used to unfairly go after business caught in legitimate mistake.

131st Maine Legislature
An Act to Enact the Maine Consumer Privacy Act
L.D.

further violations will occur, the Attorney General may not initiate an action against the controller or processor for the violation listed in the notice.

(C~~B~~) Not later than February 1, 2027, the Attorney General shall submit a report to the Joint Committee on the Judiciary disclosing: (1) the number of notices of violation the Attorney General has issued; (2) the nature of such violation; (3) the number of violations that were cured during the thirty-day cure period; and (4) any other matter the Attorney General deems relevant for the purposes of such report.

(~~C~~D) Beginning on January 1, 2028, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (B), consider: (1) The number of violations; (2) the size and complexity of the controller or processor; (3) the nature and extent of the controller's or processor's processing activities; (4) the substantial likelihood of injury to the public; (5) the safety or persons or property; (6) whether such alleged violation was likely caused by human or technical error.

**3. Violation of statute.** A violation of this chapter constitutes an unfair trade practice under Title 5, chapter 10 and may be enforced solely by the Attorney General. The provisions of Title 5, section 213 do not apply to a violation of this chapter.

**§9611. Effective Date**

**1. Effective Date**. This act shall take effect on July 1, 2025.

**Commented [A20]:** Suggest having a delayed effective date for small business as way to allow them more time to prepare and take advantage of the large business setting up structure of compliance that may make it easier for them to copy.

**Sec. 2. 35-A MRSA §9301,** as enacted by PL 2019, c. 216, §1 and affected by §2, is repealed.

**SUMMARY**

This bill enacts the Maine Consumer Privacy Act to entitle consumers to certain rights concerning the use of personal data.

"Redline" of LD 1977 - From Rep. O'Neil (12/19/23)

## An Act to Create the Data Privacy and Protection Act

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

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

**CHAPTER 1057**

**DATA PRIVACY AND PROTECTION ACT**

**§9601. Definitions.**

As used in this chapter, unless the context otherwise requires:

(1) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by or is under common control with another legal entity. For the purposes of this subdivision, "control" and "controlled" mean (A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company, (B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions, or (C) the power to exercise controlling influence over the management of a company.

(2) "Affirmative Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a controller, provided:~~agreement to allow the processing of personal data relating to the consumer~~

(A) The request is provided to the consumer in a clear and conspicuous stand-alone disclosure made through the primary medium used to offer the controllers' product or service, or, if the product or service is not offered in a medium that permits the making of the request under this paragraph, another medium regularly used in conjunction with the controller's product or service;

Formatted: No underline

(B) The request includes a description of the processing purpose for which the consumer's consent is sought and:

Formatted: No underline

(1) Clearly states the specific categories of personal data that the controller intends to collect, process or transfer necessary to achieve the processing purpose; and

Formatted: No underline

(2) Includes a prominent heading and is written in language that would enable a reasonable consumer to identify and understand the processing purpose for which consent is sought and the personal data to be collected, processed or transferred by the controller for the processing purpose;

(C) The request clearly explains the consumer's rights related to consent;

(D) The request is made in a manner reasonably accessible to and usable by consumers with disabilities;

(E) The request is made available to the consumer in each language in which the controller provides a product or service for which authorization is sought;

(F) The option to refuse to give consent is at least as prominent as the option to give consent and the option to refuse to give consent takes the same number of steps or fewer as the option to give consent; and

(G) Affirmative consent to an act or practice is not inferred from the inaction of the consumer or the consumer's continued use of a service or product provided by the controller.

"Affirmative Consent" does not include:

(A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information,

(B) hovering over, muting, pausing or closing a given piece of content,

(C) The use of a false, fraudulent, or materially misleading statement or representation, or

(~~C~~D) agreement obtained through the use of dark patterns.

(3) "Algorithm" means a computational process that uses machine learning, natural language processing, artificial intelligence techniques or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision-making with respect to personal data, including to determine

Formatted: No underline

Formatted: Indent: Left: 0.5", Line spacing: Multiple 1.25 li

Formatted: No underline

Formatted: No underline

Formatted: No underline

Formatted: No underline

Formatted: No underline

Formatted: No underline

the provision of products or services or to rank, order, promote, recommend, amplify or similarly determine the delivery or display of information to a consumer.

(4) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded ~~under subdivisions (1) to (4), inclusive, of subsection (a) of section 4 of this act~~this chapter is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(5) "Biometric data" means data generated by ~~automatic measurements~~technological processing of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that ~~are~~ can be used to identify a specific individual. "Biometric data" does not include:

Commented [CMF1]: This is the term used in ADPPA and I think it works better.

(A) a digital or physical photograph,

(B) an audio or video recording, or

(C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(6) "Business associate" has the same meaning as provided in HIPAA.

(7) "Child" has the same meaning as provided in COPPA.

(8) "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

(9) "Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive or sexual health data;

(10) "Controller" means a person who, ~~or legal entity that,~~ alone or jointly with others determines the purpose and means of processing personal data.

(11) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

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

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

(14) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

(15) "De-identified data" means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data:

(A) takes ~~reasonable~~ technical measures to ensure that such data cannot be associated with an individual or be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual,

(B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and

(C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(16) "Gender-affirming health care services" means all medical care relating to the treatment of gender dysphoria as set forth in the most recent edition of the American Psychiatric Association's "Diagnostic and Statistical Manual of Mental Disorders" and gender incongruence, as defined in the most recent revision of the "International Statistical Classification of Diseases and Related Health Problems."

(17) "Gender-affirming health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

(18) "Geofence" means any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data or any other form of location detection, or any combination of such coordinates, connectivity, data, identification or other form of location detection, to establish a virtual boundary.

(19) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

(20) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

~~(20) "Institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.~~

(21) "Mental health facility" means any health care facility in which at least seventy per cent of the health care services provided in such facility are mental health services.

~~(17) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.~~

(22) "Minor" means any consumer who is younger than 18 years of age;

(23) "Person" means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

(24) "Personal data" means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or a device that identifies or is linked or reasonably linkable to an individual. "Personal data" does not include de-identified data or publicly available information.

(25) "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals~~directly identifies the specific location of an individual~~ with precision and accuracy within a radius of one thousand seven hundred fifty feet. "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility

(26) "Process" and "processing" mean any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

(27) "Processor" means a person who processes personal data on behalf of a controller.

(28) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual, including an individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

(29) "Protected health information" has the same meaning as provided in HIPAA.

~~(24) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.~~

(30) "Publicly available information" means information that has been

~~(A) is~~ lawfully made available to the general public from:

~~through~~ (A) federal, state or municipal government records, if the person collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

~~or~~ (B) widely distributed media~~,~~;

**Commented [CMF2]:** This is the definition suggested by the AG's office to the Committee

(C) A website or online service made available to all members of the public, for free or for a fee, including where all members of the public, for free or for a fee, can log in to the website or online service;

(D) A disclosure that has been made to the general public as required by federal, state, or local law; or

(E) The visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession.~~and~~

Formatted: Indent: First line: 0.5"

For purposes of this paragraph, information from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has restricted the information to a specific audience.

(B) ~~a controller has a reasonable basis to believe a consumer has lawfully made available to the general public.~~"Publicly available information" does not include:

Formatted: Indent: Left: 0.5"

1. Any obscene visual depiction, as defined in section 1460 of title 18, United States Code;

2. any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive data with respect to an individual;

3. biometric information;

4. publicly available information that has been combined with personal data;

5. genetic information, unless otherwise made available by the individual to whom the information pertains; or

6. intimate images known to have been created or shared without consent.

(31) "Reproductive or sexual health care" means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including, but not limited to, any such service or product rendered or provided concerning (A) an individual health condition, status, disease, diagnosis,

diagnostic test or treatment, (B) a social, psychological, behavioral or medical intervention, (C) a surgery or procedure, including, but not limited to, an abortion, (D) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion, (E) a bodily function, vital sign or symptom, (F) a measurement of a bodily function, vital sign or symptom, or (G) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

(32) "Reproductive or sexual health data" means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

(33) "Reproductive or sexual health facility" means any health care facility in which at least seventy per cent of the health care-related services or products rendered or provided in such facility are reproductive or sexual health care.

(34) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party. "Sale of personal data" does not include:

(A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller,

~~(B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer,~~

(C) the disclosure or transfer of personal data to an affiliate of the controller,

(D) with the consumer's affirmative consent, the disclosure of personal data where the consumer affirmatively directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party,

(E) the disclosure of personal data that the consumer

(i) intentionally made available to the general public via a channel of mass media, and

(ii) did not restrict to a specific audience, or

**Commented [CMF3]:** Trying to think of a situation where a controller needs to *sell* personal data to provide a service.

~~(F) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the controller's assets.~~

**Commented [CMF4]:** Recommend deleting this here and putting it in the Sec. 9611 exemptions because you also need to exempt it from the data minimization provisions (if added)

(35) "Sensitive data" means personal data that includes

(A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, status as pregnant, sex life, sexual orientation, union membership, or citizenship or immigration status,

**Commented [CMF5]:** Delaware added this.

(B) consumer health data;

(C) ~~the processing of~~ genetic or biometric data ~~for the purpose of uniquely identifying an individual~~,

**Commented [CMF6]:** Do we need a definition of genetic?

(D) information about a consumer when the controller or processor has knowledge that the consumer is a minor~~personal data collected from a known child~~, ~~or~~

(E) data concerning an individual's status as a victim of crime,

(E) precise geolocation data,

**Formatted:** English (United States)

(F) a government-issued identifier, including a Social Security number, passport number or driver's license number, that is not required by law to be displayed in public;

(G) a financial account number, debit card number, credit card number or information that describes the income level or bank account balances of a consumer, except that "sensitive data" does not include the last 4 digits of a debit or credit card number;

(H) a consumer's private communications, including voicemails, e-mails, texts, direct messages or mail, or information identifying the parties to those communications, voice communications, video communications and information that pertains to the transmission of those communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration and location information of the parties to the call,

unless the controller or processor is the sender or an intended recipient of the communication. For purposes of this paragraph, communications are not private if those communications are made from or to a device provided by an employer to an employee and the employer provides conspicuous notice that the employer may access communications made on the device;

(I) account or device log-in credentials or security or access codes for an account or device;

(J) calendar information, address book information, phone or text logs, photos, audio recordings or videos maintained for private use by a consumer, regardless of whether that information is stored on the consumer's device or is accessible from that device and is backed up in a separate location. For purposes of this paragraph, information is not sensitive if the information is sent from or to a device provided by an employer to an employee and the employer provides conspicuous notice that the employer may access the information on the device;

(K) a photograph, film, video recording or other similar medium that shows the naked or undergarment-clad genitals of a consumer;

(L) information revealing the video content requested or selected by a consumer collected by a controller, not including personal data used solely for transfers for independent video measurement; or

(M) information identifying a consumer's online activities over time and across 3rd-party websites or online services.~~.~~

(36) "Targeted advertising" means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics or interests associated with the individual or a device identified by a unique identifier~~displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet web sites or online applications to predict such consumer's preferences or interests~~. "Targeted advertising" does not include

**Commented [CMF7]:** This change better covers targeted advertising b/c it covers targeting based on profiling regardless of the source of the data, not just from tracking across websites.

(A) advertisements based on activities within a controller's own Internet web sites or online applications, provided that the processing necessary to generate such advertisements does not include sensitive data;

(B) advertisements based on the context of a consumer's current search query, visit to an Internet web site or online application in which the advertisement appears and does not vary based on who is viewing the advertisement~~,~~;

(C) advertisements directed to a consumer or consumer's device in response to the consumer's specific request for information or feedback~~,~~; or

(D) processing personal data strictly necessary for the sole purpose of measuring ~~solely to measure~~ or reporting advertising frequency, performance or reach.

(37) "Third party" means a person, including a controller, that collects, processes or transfers personal data and is not a consumer-facing business with which the consumer linked or reasonably linkable to that personal data expects and intends to interact and is not a processor with respect to that data. "Third party" does not include a person that collects personal data from another entity if the 2 entities are related by common ownership or corporate control unless a reasonable consumer's reasonable expectation would be that the entities share information. ~~, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller.~~

(38) "Trade secret" has the same meaning as provided in Title 10, section 1542, subsection 4. ~~section 35-51 of the general statutes.~~

(39) "Transfer" means to disclose, release, disseminate, make available, license, rent, or share personal data orally, in writing, electronically, or by any other means.

§X. Geofencing. No person shall use a geofence to establish a virtual boundary that is within 1,750 feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's consumer health data.

**§9602. Applicability**.

**Commented [CMF8]:** Need this clarification because if we're putting in place the restriction that sensitive data cannot be used for targeted advertising, this exemption would allow for the use of sensitive data say Google has for targeted ads within Google's websites.

**Formatted:** Indent: Left: 0.5"

**Formatted:** Not Highlight

**Formatted:** Not Highlight

**Formatted:** Not Highlight

**Formatted:** Not Highlight

**Formatted:** Not Highlight

**Formatted:** Font: Not Bold

**Formatted:** Font color: Accent 6

**Formatted:** Font color: Accent 6

**Commented [CMF9]:** This is the geofence provision CT added in 2023, but I'm not sure where to put it.

**Formatted:** Font color: Accent 6

The provisions of this chapter apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year:

(1) Controlled or processed the personal data of not less than ~~one hundred thousand~~35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not less than ~~twenty-five thousand~~10,000 consumers and derived more than ~~twenty-five~~20 per cent of their gross revenue from the sale of personal data.

**§9603. Scope.**

(a) The provisions of this chapter do not apply to any:

(1) A Federal, State, Tribal, territorial, or local government entity such as a ~~B~~body, authority, board, bureau, commission, district or agency of this state or of any political subdivision of this state; or

(2) provider of broadband internet access service, as defined in Title 35-A, Section 9301.

~~(2) nonprofit organization;~~

~~(3) institution of higher education;~~

~~(4) national securities association that is registered under 15 USC 78o-3 of the Securities Exchange Act of 1934, as amended from time to time;~~

~~(5) financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.; or~~

~~(6) covered entity or business associate, as defined in 45 CFR 160.103; or~~

~~(7) air carrier, as defined in 49 USC 40102, as amended from time to time, and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be amended from time to time.~~

**Commented [CMF10]:** This is the threshold in Delaware, which has a similar population to Maine.

**Commented [ma11R10]:** This is what we got NH lawmakers to include in their most recent draft as well.

**Commented [CMF12]:** This exempts ISPs so that they are covered by the ISP privacy law instead, but I'm not sure if we should add a clarifying clause to ensure that if that law is repealed, they are covered under this instead

(b) The following information and data is exempt from the provisions of this chapter:

(1) Personal information collected, processed, sold, or disclosed subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.;

(1) Protected health information that is collected by a covered entity or business associate~~under HIPAA~~;

(2) patient-identifying information for purposes of 42 USC 290dd-2;

(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46;

(4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

(5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law;

(6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.;

(7) patient safety work product for purposes of ~~section 19a-127o of the general statutes and~~ the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time;

(8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program

or qualified service organization, as specified in 42 USC 290dd-2, as amended from time to time;

(10) information used for public health activities and purposes as authorized by HIPAA, community health activities and population health activities;

(11) the collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time;

(12) personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time;

(13) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time;

(14) personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq., as amended from time to time;

(15) data processed or maintained

(A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role,

(B) as the emergency contact information of an individual under this chapter used for emergency contact purposes, or

(C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits; and

**Formatted:** Highlight

(16) personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Federal Aviation Act of 1958, 49 USC 40101 et seq., to the extent this chapter is preempted by the Federal Aviation Act of 1958, as said acts may be amended from time to time.

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to this chapter.

**§9604. Consumer rights**.

(a) A consumer shall have the right to:

(1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, unless such confirmation or access would require the controller to reveal a trade secret;

(2) obtain from a controller, a list of specific third parties, other than natural persons, to which the controller has disclosed either: (i) the consumer's personal data; or (ii) any personal data;

**Commented [CMF13]:** Oregon included this in their privacy law.

(~~2~~3) 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;

(~~3~~4) delete personal data provided by, or obtained about, the consumer;

(~~4~~5) 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 without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret; and

(~~5~~6) opt out of the processing of the personal data for purposes of

(A) targeted advertising,

(B) the sale of personal data~~, except as provided in subsection (b) of section 6 of this act~~, or

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

(b) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 9605 of this act to exercise the rights of such consumer ~~to opt out of the processing of such consumer's personal data for purposes of subdivision (5) of subsection (a) of this~~specified in this section on behalf of the consumer. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

**Commented [CMF14]:** Striking this allows individuals to use an authorized agent to exercise any of their rights, not just the opt-out. See Consumer Reports report on this: https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-authorized-agents-can-empower-people-to-exercise-their-digital-privacy-rights-in-california/

(c) Except as otherwise provided in this chapter a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to said sections as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period by forty-five additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than forty-five days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (45), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights. A controller shall not be required to authenticate an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (34) of subsection (a) of this section by

(A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to this chapter, or

(B) opting the consumer out of the processing of such personal data for any purpose except for those exempted pursuant to the provisions of this chapter.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall

also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

(e) A controller may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in this section through—

(1) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) the use of dark patterns.

**§9605. Authorized agent.**

A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to ~~opt out of the processing of such consumer's personal data for one or more of the purposes~~exercise rights specified in ~~subdivision (5) of~~ subsection (a) of section 9604 of this act. The consumer may designate such authorized agent by way of, among other things, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt out of such processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

**§9606. Actions of controllers.**

(a) A controller shall:

(1) Limit the collection, processing, and transfer of personal data to what is ~~adequate, relevant and~~ reasonably necessary and proportionate to provide or maintain a specific product or service requested by ~~in relation to the purposes for which such data is processed, as disclosed to~~ the consumer to whom the data pertains;

~~(2) except as otherwise provided in sections 1 to 11, inclusive, of this act, not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;~~

Formatted: No bullets or numbering

Commented [CMF15]: This ensures that controllers can't use dark patterns to make exercising privacy rights more difficult

Formatted: Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.55" + Indent at: 0.95"

Commented [CMF16]: This is the section where we propose adding the data minimization rules from LD1977

~~(3) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue;~~

(~~4~~2) not collect, process, or transfer sensitive data concerning a consumer except when the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the sensitive data pertains~~without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with COPPA~~;

(3) not process sensitive data for the purposes of targeted advertising;

~~(5) not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers;~~

(~~6~~4) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon revocation of such consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request; and

(~~7~~5) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data without the consumer's consent, under circumstances where a controller has actual knowledge, or wilfully disregards, that the consumer is ~~at least thirteen years of age but younger than sixteen years of age~~a minor. A controller shall not discriminate or retaliate against a consumer for exercising any of the consumer rights contained in this chapter, or for refusing to agree to the collection or processing of personal data for a separate product or service, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

(b) Nothing in subsection (a) of this section shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including

**Commented [CMF17]:** Deleting because we are suggesting a new data security section below that it applies to both controllers and processors, not just controllers.

**Formatted:** Indent: Left: 0"

**Formatted:** No underline

**Commented [CMF18]:** Suggest cutting as long as the standalone subsection on discrimination that applies to both controllers & processors is added below. Otherwise, keep — but there are a lot of gaps in state & federal discrimination laws that make the below language better.

**Commented [CMF19]:** Connecticut changed the "and" to an "or" in its 2023 updates to the law.

offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a financial incentive program such as a bona fide loyalty, rewards, premium features, discounts or club card program, provided that the controller may not transfer personal data to a 3rd party as part of such program unless:

(1) the transfer is functionally necessary to enable the 3rd party to provide a benefit to which the consumer is entitled;

(2) the transfer of personal data to the 3rd party is clearly disclosed in the terms of the program; and

(3) the 3rd party uses the personal data only for purposes of facilitating a benefit to which the consumer is entitled and does not process or transfer the personal data for any other purpose.

The sale of personal data shall not be considered functionally necessary to provide a financial incentive program. A controller shall not use financial incentive practices that are unjust, unreasonable, coercive or usurious in nature.

(c) A controller shall provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes:

(1) The categories of personal data processed by the controller, including a separate list of categories of sensitive data processed by the controller, described in a level of detail that provides consumers a meaningful understanding of the type of personal data processed;

(2) the purpose for processing each category of personal data the controller collects or processes described in a way that gives consumers a meaningful understanding of how each category of their personal data will be used;

(3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(4) the categories of personal data that the controller ~~shares with~~transfers to third parties, if any;

**Formatted:** No underline

**Formatted:** No underline

**Formatted:** Indent: Left: 0.5"

**Commented [CMF20]:** These additions protect legitimate loyalty programs while prohibiting them from being used as a way for companies to make money off their customer's personal data

**Formatted:** No underline

**Commented [CMF21]:** This language is from the regs in CA

**Commented [CMF22]:** This is from the Colorado Data Privacy Act regulations

**Commented [CMF23]:** This is from the Colorado Data Privacy Act regulations

(5) the categories of third parties, if any, ~~with~~ to which the controller ~~shares~~ transfers personal data;

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

(~~6~~7) an active electronic mail address or other online mechanism that the consumer may use to contact the controller.

If a controller makes a material change to its privacy notice, the controller shall notify each consumer affected by the material change before implementing the material change with respect to prospectively collected controller and provide a reasonable opportunity for each consumer to withdraw consent to further materially different collection, processing or transfer of previously collected personal data under the changed policy. The controller shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy notice to each affected consumer, taking into account available technology and the nature of the relationship.

**Formatted:** Indent: Left: 0"

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing.

(e) (1) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(A)

(i) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and

(ii) Not later than January 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

~~(I) Not unfairly disadvantage another controller;~~

~~(II) Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any processing of such consumer's personal data pursuant to sections 1 to 11, inclusive, of this act;~~

(~~III~~) Be consumer-friendly and easy to use by the average consumer;

~~(IV) Be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation;~~ and

(~~V~~II) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising. For purposes of this subsection, the use of an internet protocol address to estimate the consumer's location shall be considered sufficient to accurately determine residency.

(B) If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent in accordance with the provisions of subparagraph (A) of this subdivision conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's ~~bona fide loyalty, rewards, premium features, discounts or club card program~~financial incentive program, the controller shall comply with such

**Formatted:** Highlight

**Commented [CMF24]:** If a consumer selects a privacy-focused browser such as Duck Duck Go or Brave — or a tracker blocker such as Privacy Badger or Disconnect.me — it should be assumed that they do not want to be tracked across the web, and they should not have to take additional steps to toggle that setting.

**Commented [CMF25]:** Should this be changed to "present in this state"?

consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(2) If a controller responds to consumer opt-out requests received pursuant to subparagraph (A) of subdivision (1) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, use, sale or ~~sharing~~ transfer of the consumer's personal data.

Formatted: Highlight

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

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Such assistance shall include:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

(2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a ~~breach of~~ security breach, as defined in ~~section 36a-701b~~Title 10, section 1347 ~~of the general statutes~~, of the system of the processor, in order to meet the controller's obligations; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The processor shall adhere to the instructions of the controller and only collect, process, and transfer the data it receives from the controller to the extent necessary and proportionate to provide a

service requested by the controller, as set out in the contract. The contract shall also require that the processor:

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

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

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

(4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data;

(5) be prohibited from combining personal data obtained from the controller with personal data which the processor receives from or on behalf of another controller or person or collects from the interaction of the processor with an individual; and

Formatted: No underline

(5) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in this chapter.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to

adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor 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 such processing and may be subject to an enforcement action under this chapter.

(e) A controller or processor may not collect, process or transfer personal data in a manner that discriminates against individuals, or otherwise makes unavailable the equal enjoyment of goods or services, on the basis of individual's actual or perceived race, color, sex, sexual orientation or gender identity, physical or mental disability, religion, ancestry or national origin.

**Commented [CMF26]:** These are the categories covered under the public accommodations protections of the Maine Human Rights Act

(f) Subsection(e) does not apply to:

(1) The collection, processing or transfer of personal data for the purpose of:

(A) A controller or processor's self-testing to prevent or mitigate unlawful discrimination; or

(B) Diversifying an applicant, participant or customer pool; or

(2) A private establishment, as described in 42 United States Code, Section 2000a(e).

**§9608. Data Security**

(a) A controller or processor shall establish, implement and maintain reasonable administrative, technical and physical data security practices and procedures to protect personal data against unauthorized access. The practices must be appropriate to:

(1) the size and complexity of the controller or processor;

(2) the nature and scope of the controller or processor's collecting, processing or transferring of personal data;

(3) the volume and nature of the personal data collected, processed or transferred by the controller or processor;

(4) the sensitivity of the personal data collected, processed or transferred;

(5) the current state-of-the-art administrative, technical and physical safeguards for protecting personal data; and

(6) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access of personal data in relation to the risks and nature of the personal data.

(b) The data security practices of the controller and of the processor required under this subsection must include, for the respective entity's own system, at a minimum, the following practices:

(1) identifying and assessing internal and external risk to the security of each system maintained by the controller that collects, processes or transfers personal data, or processor that collects, processes or transfers personal data on behalf of the controller;

(2) a plan to receive and reasonably respond to unsolicited reports of vulnerabilities by an entity or individual by performing a reasonable investigation of those reports;

(3) taking preventive and corrective action designed to mitigate reasonably foreseeable risks or vulnerabilities to personal data identified by the controller or processor, consistent with the nature of the risk or vulnerability and the entity's role in collecting, processing or transferring the data. Corrective action may include implementing administrative, technical or physical safeguards or changes to data security practices or the architecture, installation or implementation of network or operating software;

(4) disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed or transferred, unless a consumer has provided affirmative consent to that retention. Disposal may include destroying, permanently erasing or otherwise modifying the personal data to make the data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section. A processor shall establish practices to delete or return personal data to a controller as requested at the end of the provision of services unless retention of the personal data is required by law;

(5) training each employee with access to personal data on how to safeguard personal data and updating the training as necessary; and

(6) implementing procedures to detect, respond to or recover from security incidents, including breaches.

**§9609. Data Protection Assessments.**

Formatted: Font: Bold

(a) A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment for each of the controller's processing activities that presents such~~a~~ heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

Commented [CMF27]: This is from the Colorado Data Privacy Act.

(1) The processing of personal data for the purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers,

(B) financial, physical or reputational injury to consumers,

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or

(D) other substantial injury to consumers; and

(4) the processing of sensitive data.

Formatted: Indent: Left: 0", First line: 0.5"

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify the categories of personal data collected, the purposes for collecting such personal data, whether personal data is being transferred to third parties, and identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards

that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

For processing activities that involve profiling, as required to be included by subsection (a)(3), the data protection assessment shall include:

A. A detailed description of the design process and methodologies of the algorithm used in furtherance of profiling;

B. A statement of the purpose and reasonably foreseeable uses of the algorithm;

C. The types of data used by the algorithm, including the specific categories and sources of data that will be processed as input and data used to train the model that the algorithm relies on, if applicable;

D. A description of the outputs produced by the algorithm;

E. An assessment of the necessity and proportionality of the algorithm in relation to its stated purpose;

F. A detailed description of steps the controller has taken or will take to mitigate potential harm from the algorithm to a consumer or group of consumers, including steps related to decisions that produce legal or similarly significant effects concerning the consumer.

G. Any other information as required by the Attorney General.

(c) No later than 30 days after completing a data protection assessment under this section, a controller shall submit a report of the data protection assessment or evaluation to the Attorney General. The report must include a summary of the data protection assessment and the controller shall make the summary publicly available in a place that is easily accessible to consumers. Controllers may redact trade secrets or other confidential or proprietary information, from the report.~~The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General.~~ The Attorney General

**Formatted:** No underline

**Formatted:** No underline

**Formatted:** No underline

**Formatted:** No underline

**Formatted:** No underline

**Commented [CMF28]:** This pulls in the language from the algorithmic impact assessment section of LD1977 and makes it part of the data protection assessment

**Formatted:** Indent: Left: 0.5"

**Formatted:** No underline

may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. ~~Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes.~~ To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) A controller shall conduct and document a data protection assessment before initiating a processing activity that presents a heightened risk of harm to a consumer shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data processed and level of risk presented by the processing, throughout the processing activity's lifecycle in order to: 1) monitor for harm caused by the processing and adjust safeguards accordingly; and 2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing. ~~Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.~~

**Commented [CMF29]:** This is from the Colorado AG's Colorado Data Privacy Act rules

**§9610. De-identified data.**

**Formatted:** Font: Bold

(a) Any controller in possession of de-identified data shall:

(1) Take ~~reasonable~~ technical measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(b) Nothing in this chapter shall be construed to:

(1) Require a controller or processor to re-identify de-identified data ~~or pseudonymous data~~; or

(2) maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) Is not reasonably capable of associating the request with the personal data or it would be ~~unreasonably~~ unduly burdensome for the controller to associate the request with the personal data;

(2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer~~; and~~

~~(3) does not sell the personal data to any third party or otherwise voluntarily disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.~~

~~(d) The rights afforded under subdivisions (1) to (4), inclusive, of subsection (a) of section 4 of this act shall not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information.~~

(e) A controller that ~~discloses~~ transfers ~~pseudonymous data or~~ de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the ~~pseudonymous data or~~ de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

**Formatted:** Not Highlight

**Formatted:** Indent: Left: 0"

**Formatted:** Indent: Left: 0.5"

**Commented [CMF30]:** This is a huge loophole that allows anyone who isn't "selling" data to not comply with the consumer rights in this bill.

**Commented [CMF31]:** pseudonymous data includes IP addresses or device IDs, so this is a big loophole for big ad tech companies

**§9611. Limitations.**

Formatted: Keep with next

(a) Nothing in this chapter shall be construed to restrict a controller's or processor's ability to collect or process data, or to transfer non-sensitive data, to the extent reasonably necessary and proportionate, or, in the case of sensitive data, strictly necessary, to:

(1) Comply with federal, state or municipal ordinances or regulations;

(2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state, municipal or other governmental authorities;

(3) cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state or municipal ordinances or regulations;

(4) investigate, establish, exercise, prepare for or defend legal claims;

(5) provide a product or service specifically requested by ~~a~~ the consumer to whom the data pertains;

(6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer prior to entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;

(9) prevent, detect, protect against or respond to security incidents~~,~~. For purposes of this paragraph, "security incident" means a network security or physical security incident, including an intrusion or trespass, medical alert or fire alarm;

Formatted: No underline

(10) prevent, detect, protect against or respond to identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity targeted at or involving the controller or processor or its services, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action. For purposes of this paragraph, the term "illegal activity" means a

violation of a federal, state or local law punishable as a crime that can directly cause harm to another person;

(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and ~~privacy~~ relevant laws and regulations, including regulations for the protection of human subjects, and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine,

~~(A) whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller,~~

(B) the expected benefits of the research outweigh the privacy risks, and

(C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(11) assist another controller, processor or third party with any of the obligations under this chapter; or

(12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is

(A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and

(B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law; ~~or~~

(13) to deliver a communication that is not an advertisement to a consumer, if the communication is reasonably anticipated by the consumer within the context of the consumer's interactions with the controller;

(14) to deliver a communication at the direction of a consumer between such consumer and one or more individuals or entities;

**Commented [CMF32]:** This reference to deletion only seems odd here if the other protections are being added to the bill.

(15) to support or promote participation in civic engagement activities and democratic governance, including voting, petitioning, engaging with government proceedings, providing indigent legal aid services, and unionizing;

(16) to ensure the data security and integrity of personal data;

(17) for private school as defined in Title 20-A, section 1 and private institutions of higher education as defined by title I of the Higher Education Act of 1965, 20 United States Code, Section 1001 et seq., delete personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution; or

Commented [CMF33]: This is necessary if you're not exempting schools b/c you don't want students to be able to delete their grades

(18) to transfer assets to a 3rd party in the context of a merger, acquisition, bankruptcy or similar transaction when the 3rd party assumes control, in whole or in part, of the controller's assets, only if the controller, in a reasonable time prior to the transfer, provides an affected consumer with:

(A) A notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies; and

Formatted: Indent: Left: 1"

(B) A reasonable opportunity to withdraw previously given consent related to the consumer's personal data and a reasonable opportunity to request the deletion of the consumer's personal data;

Provided, however, that a controller shall:

(1) not collect biometric data without the affirmative consent of the consumer;

Commented [CMF34]: This imports the opt-in requirement for biometric data from LD 1705

Formatted: Indent: Left: 0.5"

(2) not process or transfer a social security number, except when necessary to facilitate an extension of credit, authentication, fraud and identity fraud detection and prevention, the payment or collection of taxes, the enforcement of a contract between parties or the prevention, investigation or prosecution of fraud or illegal activity or as otherwise required by federal, state or local law;

(b) Nothing in this chapter shall be construed to restrict a controller's or processor's ability to transfer sensitive data collected in compliance with section X to a third party provided:

Formatted: Highlight

(1) The transfer is made with the affirmative consent of the consumer;

(2) The transfer is necessary to comply with a legal obligation imposed by federal, state, tribal or local law or to investigate, establish, exercise or defend legal claims;

(3) The transfer is necessary to prevent an individual from imminent injury when the controller believes in good faith that the individual is at risk of death, serious physical injury or serious health risk;

(4) In the case of the transfer of a password, the transfer is necessary to use a designated password manager or the transfer is to a controller for the exclusive purpose of identifying passwords that are being reused across sites or accounts;

(5) In the case of the transfer of genetic information, the transfer is necessary to perform a medical diagnosis or medical treatment specifically requested by an consumer or to conduct medical research; or

(6) To transfer assets in the manner described in subsection (a), paragraph 18;

Formatted: Indent: Left: 0.5"

(b) The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor's ability to process data previously collected in accordance with this chapter to~~collect, use or retain data for internal use to:~~

(1) Conduct internal research to develop, improve or repair products, services or technology for which such data was collected;

(2) effectuate a product recall;

Formatted: Indent: Left: 0", First line: 0.5"

(3) identify and repair technical errors that impair existing or intended functionality of a service or product for which the data was collected;

(4) process the data as necessary to perform system maintenance or diagnostics;

Formatted: No underline

Formatted: No underline

(5) protect against spam;

Formatted: No underline

(6) process personal data that is not sensitive data to provide targeted advertising to consumers who are i) not minors; and ii) have not exercised the right to opt-out of targeted advertising under section 9603(a)(6).~~or~~

Formatted: Not Highlight

Formatted: No underline

Formatted: No underline, Not Highlight

Formatted: No underline

Formatted: Not Highlight

~~(4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.~~

(c) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) A controller or processor that discloses personal data to a processor or third-party controller in accordance with this chapter shall not be deemed to have violated said sections if the processor or third-party controller that receives and processes such personal data violates said sections, provided, at the time the disclosing controller or processor disclosed such personal data, the disclosing controller or processor did not have actual knowledge that the receiving processor or third-party controller would violate said sections. A third-party controller or processor receiving personal data from a controller or processor in compliance with this chapter is likewise not in violation of said sections for the transgressions of the controller or processor from which such third-party controller or processor receives such personal data.

(e) Nothing in this chapter shall be construed to:

(1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person

(A) to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution, or

(B) under ~~section 52-146t of the general statutes~~Title 16; or

(2) apply to any person's processing of personal data in the course of such person's purely personal or household activities.

(f) Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section, or, in the case of sensitive data, strictly necessary to the purposes listed in this section; ~~and~~

(2) adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of such collection, use or retention. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use or retention of personal data; and

(3) compliant with section 9607, subsection (e).

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in subsection (f) of this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to such processing.

**§9612. Rules.**

The Attorney General may adopt rules necessary to implement this chapter.

**§9613. Enforcement.**

(a) The Attorney General, a district attorney or a counsel for a municipality may bring a civil action in the name of the State or on behalf of the residents of the State against a controller or processor that violates this chapter to:

(1) Enjoin the act or practice that is in violation of this chapter;

(2) Enforce compliance with this chapter or a rule adopted under this chapter;

**Commented [CMF35]:** I think this section is redundant if we have data minimization plus the new data security section

**Commented [CMF36]:** Need to designate these rules as either "major substantive rules" or "routine technical rules" under ME law. Substantive rules are subject to legislative review.

**Formatted:** No underline

**Formatted:** No underline

**Formatted:** Font: Not Bold, No underline

**Formatted:** No underline

**Formatted:** No underline

**Formatted:** Indent: Left: 0.5"

**Formatted:** No underline

(3) Obtain damages, civil penalties, restitution or other compensation on behalf of the residents of the State; or

(4) Obtain reasonable attorney's fees and other litigation costs reasonably incurred.

(b) A violation of this chapter or a rule adopted under this chapter with respect to the personal data of a consumer constitutes an injury to that consumer. The injured consumer may bring a civil action against the party that commits the violation. In a civil action brought under this subsection in which a plaintiff prevails, the court may award the plaintiff:

(1) Damages in an amount not less than $5,000 per individual per violation, as adjusted annually to reflect an increase in the Consumer Price Index, or actual damages, whichever is greater;

(2) Punitive damages;

(3) Injunctive relief;

(4) Declaratory relief; and

(5) Reasonable attorney's fees and litigation costs.

(c) Notwithstanding any provision of law to the contrary, no predispute arbitration agreement or predispute joint-action waiver is valid or enforceable with respect to a dispute arising under this chapter. A determination as to whether this subsection applies to a dispute must be made by a court, rather than an arbitrator, without regard to whether an applicable agreement purports to delegate that determination to an arbitrator. For purposes of this subsection, "predispute arbitration agreement" means an agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement and "predispute joint-action waiver" means an agreement that would prohibit a party from participating in a joint, class or collective action in a judicial, arbitral, administrative or other forum, concerning a dispute that has not yet arisen at the time of the making of the agreement.

~~(a) The Attorney General shall have exclusive authority to enforce violations of sections 1 to 10, inclusive, of this act.~~

Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: Indent: Left: 0.5"
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: Font: Not Bold, No underline
Formatted: No underline
Formatted: Font: Not Bold, No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline
Formatted: No underline

(~~b~~d) During the period beginning on ~~July 1, 2023~~X, and ending on ~~December 31, 2024~~X, the Attorney General ~~shall~~may, prior to initiating any action for a violation of any provision of ~~sections 1 to 10, inclusive, of this act~~this chapter, issue a notice of violation to the controller if the Attorney General determines that a cure is possible. If the controller fails to cure such violation within sixty days of receipt of the notice of violation, the Attorney General may bring an action pursuant to this section. T~~Not later than February 1, 2024, the Attorney General shall submit a report, in accordance with section 11-4a of the general statutes, to the joint standing committee of the General Assembly having cognizance of matters relating to general law disclosing:~~

~~(1) The number of notices of violation the Attorney General has issued;~~

~~(2) the nature of each violation;~~

~~(3) the number of violations that were cured during the sixty-day cure period; and~~

~~(4) any other matter the Attorney General deems relevant for the purposes of such report.~~

~~(c) Beginning on January 1, 2025, t~~he Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider:

(1) The number of violations;

(2) the size and complexity of the controller or processor;

(3) the nature and extent of the controller's or processor's processing activities;

(4) the substantial likelihood of injury to the public;

(5) the safety of persons or property; and

(6) whether such alleged violation was likely caused by human or technical error.

~~(d) Nothing in sections 1 to 10, inclusive, of this act shall be construed as providing the basis for, or be subject to, a private right of action for violations of said sections or any other law.~~

**Commented [CMF37]:** This is the right to cure that the Committee was debating. I have left the CT text in place, though I have changed "shall" to "may" to give the AG discretion - I think if they have discretion you could remove the sunset. This would allow the AG's office to work with smaller businesses on a cure and prioritize using its resources for willful and especially harmful violations.

**Commented [CMF38]:** Change to relevant provision in Maine law

**Formatted:** Indent: Left: 0"

(~~e~~f) A violation of the requirements of this chapter shall constitute an unfair trade practice for purposes of ~~section 42-110b of the general statutes and shall be enforced solely by the Attorney General, provided the provisions of section 42-110g of the general statutes shall not apply to such violation~~X.

~~Sec. 12. (Effective from passage)~~

~~(a) Not later than September 1, 2022, the chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall convene a task force to study:~~

~~(1) Information sharing among health care providers and social care providers and make recommendations to eliminate health disparities and inequities across sectors, as described in subsection~~

~~(a) of section 19a-133b of the general statutes;~~

~~(2) Algorithmic decision-making and make recommendations concerning the proper use of data to reduce bias in such decision-making;~~

~~(3) Possible legislation that would require an operator, as defined in the Children's Online Privacy Protection Act, 15 USC 6501 et seq., as amended from time to time, to, upon a parent's request, delete the account of a child and cease to collect, use or maintain, in retrievable form, the child's personal data on the operator's Internet web site or online service directed to children, and provide parents with an accessible, reasonable and verifiable means to make such a request;~~

~~(4) Any means available to verify the age of a child who creates a social media account;~~

~~(5) Issues concerning data colocation, including, but not limited to, the impact that the provisions of sections 1 to 11, inclusive, of this act have on third parties that provide data storage and colocation services;~~

~~(6) Possible legislation that would expand the provisions of sections 1 to 11, inclusive, of this act to include additional persons or groups; and~~

~~(7) Other topics concerning data privacy.~~

~~(b) The chairpersons of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall serve as the chairpersons of the task force, and shall jointly appoint the members of the task force. Such members shall include, but need not be limited to:~~

~~(1) Representatives from business, academia, consumer advocacy groups, small and large companies and the office of the Attorney General; and~~

~~(2) Attorneys with experience in privacy law.~~

~~(c) The administrative staff of the joint standing committee of the General Assembly having cognizance of matters relating to general law shall serve as administrative staff of the task force.~~

~~(d) Not later than January 1, 2023, the task force shall submit a report on its findings and recommendations to the joint standing committee of the General Assembly having cognizance of matters relating to general law, in accordance with the provisions of section 11-4a of the general statutes. The task force shall terminate on the date that it submits such report or January 1, 2023, whichever is later.~~

**Sec. 2. Deadlines for certain actions.** The first data protection assessment required by the Maine Revised Statutes, Title 10, section 9609 are required to be completed not later than the first anniversary of the effective date of this Act.

**Sec. 3. Effective date.** This Act takes effect 180 days after the adjournment of the First Special Session of the 132nd Legislature.

**Formatted:** Font: Bold

**Formatted:** Font: Bold

**Formatted:** Font: Bold

**Formatted:** Font: Bold