131st MAINE LEGISLATURE

FIRST SPECIAL SESSION-2023

Legislative Document	**No. 1973**
S.P. 807	In Senate, May 18, 2023

An Act to Enact the Maine Consumer Privacy Act

Reference to the Committee on Judiciary suggested and ordered printed.

DAREK M. GRANT
Secretary of the Senate

Presented by Senator KEIM of Oxford.
Cosponsored by Representative MOONEN of Portland and
Senators: BENNETT of Oxford, BRAKEY of Androscoggin, DAUGHTRY of Cumberland, HICKMAN of Kennebec, LIBBY of Cumberland, Representatives: HENDERSON of Rumford, WHITE of Waterville.

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.

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 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. Agreement 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:

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 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 data cannot be associated with an individual;

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

C. Contractually obligates recipients of the 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.

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. "Publicly available information" means information that is:

A. Lawfully made available through federal, state or municipal government records or widely distributed media; and

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:

(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 child; or

D. Precise geolocation data.

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 100,000 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;

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.;

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 under 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. 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 the consumer opts in to the processing.

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 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.

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 the processing of the consumer's personal data for the purposes specified in section 9603, subsection 2. A controller shall comply with an opt-in 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 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

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. No later than July 1, 2025, a controller shall delete a consumer's personal data for the purposes of targeted advertising or sale of the personal data if the consumer has not opted in to the targeted advertising or sale. The platform, technology or mechanism for opting in 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 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

C. 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 in to the sale of the consumer's personal data or targeted advertising.

8. Opt-in preference signal. A controller that recognizes an opt-in 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. 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 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.

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 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, state or municipal ordinances;

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

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

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

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

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

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

K. 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.

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.

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

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.

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.