

MAINE STATE LEGISLATURE

The following document is provided by the
LAW AND LEGISLATIVE DIGITAL LIBRARY
at the Maine State Law and Legislative Reference Library
<http://legislature.maine.gov/lawlib>



Reproduced from scanned originals with text recognition applied
(searchable text may contain some errors and/or omissions)

Public Records Exceptions Review
Judiciary Committee — 132nd Legislature

LD _____ from _____ Committee

Proposed citation: _____ Brief description: _____

Statutory Review Criteria 1 M.R.S. §434(2), (2-A) & (2-B)	Notes
A. Whether a record protected by the proposed exception needs to be collected and maintained ;	
B. The value to the agency or official or to the public in maintaining a record protected by the proposed exception;	
C. Whether federal law requires a record covered by the proposed exception to be confidential;	
<i>Does the proposed public record exception meet one or more of the following (D, E, F, or G)?</i>	
D. Whether the proposed exception protects an individual's privacy interest and, if so, whether that interest substantially outweighs the public interest in the disclosure of records;	
E. Whether public disclosure puts a business at a competitive disadvantage and, if so, whether that business's interest substantially outweighs the public interest in the disclosure of records;	
F. Whether public disclosure compromises the position of a public body in negotiations and, if so, whether that public body's interest substantially outweighs the public interest in the disclosure of records;	
G. Whether public disclosure jeopardizes the safety of a member of the public or the public in general and, if so, whether that safety interest substantially outweighs the public interest in the disclosure of records;	
G-1. Whether public access to the record ensures or would ensure that members of the public are able to make informed health and safety decisions ;	
<i>This criterion applies to all reviews:</i>	
H. Whether the proposed exception is as narrowly tailored as possible;	
I. Any other criteria that assist the review committee in determining the value of the proposed exception as compared to the public's interest in the record protected by the proposed exception.	
<i>If the public records exception creates broad confidentiality for an agency:</i>	
2-A. Accountability review of agency or official. In evaluating each proposed public records exception, the review committee shall, in addition to applying the criteria [above], determine whether there is a publicly accountable entity that has authority to review the agency or official that collects, maintains or uses the record subject to the exception in order to ensure that information collection, maintenance and use are consistent with the purpose of the exception and that public access to public records is not hindered.	
2-B. Accessibility of public records. In reviewing and evaluating whether a proposal may affect the accessibility of a public record, the review committee may consider any factors that affect the accessibility of public records, including but not limited to fees, request procedures and timeliness of responses.	
ARCHIVES NOTE: 5 MRSA §95-C(1)(C) provides that records of archival value that are transferred to the Maine State Archives for permanent retention lose their confidential status, even if the statute designates such records as confidential, when they have been in existence for 75 years. <i>Note: The committee may suggest exempting specific types of public records from this law or suggest that a different time frame apply to specific types of public records under this law.</i>	

Public Records Exceptions Review
Judiciary Committee — 132nd Legislature

LD _____ from _____ Committee

Judiciary Committee Recommendation

Date _____

- ☐ The proposed public records exception meets the criteria listed in Title 1, section 434 and the Judiciary Committee approves the proposed language:

☐ Without change;

☐ With a suggestion that the records be exempt from Title 5, section 95-C(1)(C), under which records transferred to the Maine State Archives for permanent retention lose their confidential status when they have been in existence for 75 years.

Proposal (length of time to retain confidential status): _____

- ☐ The proposed public records exception does not meet the criteria listed in Title 1, section 434 for the following reasons:

and the Judiciary Committee recommends that the committee of jurisdiction consider making the following changes in the language of the proposed public records exception to address the(se) issue(s):

Vote: For:

Against:

Absent

Minority report(s):

HOUSE No. 378**The Commonwealth of Massachusetts**

PRESENTED BY:

Jessica Ann Giannino

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act for the protection and privacy of social care information.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
Jessica Ann Giannino	16th Suffolk	1/17/2025
Brian W. Murray	10th Worcester	4/3/2025

HOUSE DOCKET, NO. 3628 FILED ON: 1/17/2025

HOUSE No. 378

By Representative Giannino of Revere, a petition (accompanied by bill, House, No. 378) of Jessica Ann Giannino relative to the protection and privacy of information about an individual's social needs. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act for the protection and privacy of social care information.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws, as appearing in the 2022 Official Edition, are hereby amended by inserting after chapter 93L the following chapter:

CHAPTER 93M. Protection and Privacy of Social Care Information

SECTION 2. Definitions

"Closed-Loop Referral System" or "CLRS" means any system that stores the social care information of one or more individuals; enables the sharing of social care information with and between participating entities for the purpose of referring individuals for social care; and is capable of updating or showing updated referral activity, including data related to participating organizations completing referrals.

"Participating organization" means any entity that has the ability to create, receive, or update referrals, or other social care information in a CLRS, including, but not limited to, healthcare providers, health plans, public agencies, charitable and nonprofit organizations, CLRS technology vendors, and entities that provide social care.

“Social care” means care, services, goods, or supplies related to an individual’s social needs. “Social care” includes, but is not limited to, support and assistance for an individual’s food stability and nutritional needs, housing, transportation, economic stability, employment, education access and quality, child care and family relationship needs, and environmental and physical safety.

“Social care information” means any information that relates to the need for, payment for, or provision of social care, and identifies the person receiving social care, or for which there is a reasonable basis to believe the information can be used to identify the individual receiving social care.

SECTION 3.

(a) In a manner that is consistent with federal and State law, a participating organization shall not sell or license social care information that is stored in or transmitted through a closed-loop referral system.

(b) In a manner that is consistent with federal and State law, social care information stored in or transmitted through a closed-loop referral system shall not be used for any purpose other than the purpose for which that information was collected or generated.

(c) A participating organization that sells, offers for sale, licenses, or otherwise furnishes, provides, or transmits to any other individual or entity social care information in violation of this section shall be liable to a civil penalty of \$1,000 for each violation.

(d) A civil penalty assessed pursuant to this section shall be collected and enforced by the attorney general.

SECTION 4. Implementation

The attorney general may adopt, amend, or repeal rules and regulations as shall be necessary for the implementation, administration, and enforcement of this chapter.

SECTION 5. Effective Date

This act shall take effect 90 days following the date of enactment.

Stocco, Janet

From: Stocco, Janet
Sent: Wednesday, May 7, 2025 9:33 AM
To: Legislature: Committee on Judiciary
Subject: FW: privacy laws & private rights of action & damages

Dear Judiciary Committee Members,

Please find below an answer from Caitriona Fitzgerald of EPIC to a question posed at the public hearing on the consumer data privacy bills — specifically whether any other state's consumer data privacy legislation provides a private right of action.

Sincerely, Janet

From: Caitriona Fitzgerald <fitzgerald@epic.org>
Sent: Tuesday, May 6, 2025 3:50 PM
To: Stocco, Janet <Janet.Stocco@legislature.maine.gov>
Subject: privacy laws & private rights of action & damages

This message originates from outside the Maine Legislature.

Janet,

Here's information for the question you received on for any states have that privacy legislation with private rights of action, what form of damages to they have:

No state has enacted a comprehensive privacy law with a private right of action. A few sectorial privacy laws have private rights of action:

- **Illinois Biometric Privacy Act:** originally passed in 2008, a number of cases have been brought under this law. Until recently, the law provided for statutory damages of up to \$1,000 per negligent violation and \$5,000 per intentional or reckless violation. After the Illinois Supreme Court ruled that each time an entity scanned or transmitted a biometric identifier was an individual violation, the Illinois Legislature last year passed a law limiting damages to \$5,000. A couple of examples of cases brought under BIPA:
 - <https://www.aclu.org/cases/aclu-v-clearview-ai>
 - <https://www.reuters.com/legal/legalindustry/facebook-pivots-facial-recognition-system-following-biometric-privacy-suit-2022-01-26/>
- **Washington My Health My Data Act:** passed in 2023, it provides that a private right of action may be brought under the Washington Consumer Protection Act for violations. The Consumer Protection Act states "It shall be presumed that damages to the consumer are equal to the cost of the service provided plus two hundred dollars. Additional damages must be proved."
 - The law only came into effect recently, and the first case was filed in February 2025: <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250220-first-lawsuit-filed-under-washingtons-my-health-my-data-act>

- **Virginia** just passed updates to its privacy law to protect reproductive and sexual health information and applied a private right of action to those sections. Penalties may include the greater of actual damages or \$500 (if violation is willful, this increases to the greater of treble actual damages or \$1,000), as well as attorney fees and costs.
- **New Jersey** passed Daniel's Law in 2020, a statute that prohibits public disclosure of home addresses or unpublished telephone numbers of certain law enforcement officers, judicial officers, and prosecutors, including by data brokers. Penalties include \$1,000 per violation.

Hope this helps!

Best,
Caitriona

--

Caitriona Fitzgerald (she/her)
Deputy Director
Electronic Privacy Information Center (EPIC)
202.483.1140 x105
epic.org | [@epicprivacy](https://twitter.com/epicprivacy)



132nd MAINE LEGISLATURE

LD 1088

LR 2064(01)

An Act to Enact the Maine Consumer Data Privacy Act

Preliminary Fiscal Impact Statement for Original Bill

Sponsor: Rep. Henderson of Rumford

Committee: Judiciary

Fiscal Note Required: Yes

Preliminary Fiscal Impact Statement

	FY 2025-26	FY 2026-27	Projections FY 2027-28	Projections FY 2028-29
Appropriations/Allocations				
Other Special Revenue Funds	\$500	\$500	\$500	\$500

Correctional and Judicial Impact Statements

This bill may increase the number of civil suits filed in the court system. The additional workload associated with the minimal number of new cases filed in the court system does not require additional funding at this time. The collection of additional filing fees will increase General Fund revenue by minor amounts.

Fiscal Detail and Notes

The bill establishes the Maine Privacy Fund within the Office of the Attorney General with a base Other Special Revenue Funds allocation of \$500 beginning in fiscal year 2025-26.

Any additional costs to the Office of the Attorney General associated with enforcing the Maine consumer data privacy act are expected to be minor and can be absorbed within existing budgeted resources.

Sec. Appropriations and allocations.

The following appropriations and allocations are made.

ATTORNEY GENERAL, DEPARTMENT OF THE**Maine Privacy Fund N530**

Initiative: Establishes the Maine Privacy Fund with a base Other Special Revenue Funds allocation of \$500.

OTHER SPECIAL REVENUE FUNDS**2025-26****2026-27**

All Other

\$500

\$500

OTHER SPECIAL REVENUE FUNDS TOTAL

\$500

\$500

ATTORNEY GENERAL, DEPARTMENT OF THE**DEPARTMENT TOTALS****2025-26****2026-27****OTHER SPECIAL REVENUE FUNDS**

\$500

\$500

DEPARTMENT TOTAL - ALL FUNDS

\$500

\$500

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Protected Data	❖ “Personal data”: § 9602 (17) p. 3 - Data linked or reasonably linkable to an identifiable individual (a “consumer”) who is a Maine resident <u>Excludes:</u> § 9602 (14) p. 34 “Publicly available information” (excludes biometric data, genetic data not revealed to the general public by the consumer; inferences from a combination of publicly available information and personal data; obscene visual depictions or intimate images created or shared without consent); and “de-identified data” § 9602 (13) p. 2	❖ “Personal data”: § 9602 (16) p. 3 - Data linked or reasonably linkable to an identifiable individual (a “consumer”) who is a Maine resident <u>Excludes:</u> “Publicly available information” (defined in a way that does not exclude the categories of information excluded in LD 1088 and LD 1822 as described in left-hand column of this table), and § 9602 (23) p. 34 “de-identified data” § 9602 (13) p. 2	❖ “Personal data”: § 9602 (24) p. 4 - Data linked or reasonably linkable to (a) an identifiable individual (a “consumer”) who is a Maine resident or (b) a device linked or reasonably linked to a consumer <u>Excludes:</u> “Publicly available information” (defined differently than LD 1088 but excludes all of the same categories of information excluded in LD 1088 as described in the left-hand column of this table); and § 9602 (21) p. 45 “de-identified data” § 9602 (14) p. 2
	❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions/diagnoses; sexual orientation; citizenship or immigration status - Genetic or “biometric data” (defined on as certain data “capable of being used” to ID a specific individual) - Consumer health data (reveals condition or diagnosis) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Social security, driver’s license or nondriver ID number (except last 4 digits of these numbers); - Account number, log-in info, or credit or debit card number that, in combination with a security code or password, permits access to a financial account - Data concerning individual’s status as a crime victim § 9602 (26) p. 5	❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, medical history, mental or physical health conditions or diagnoses by a medical professional; sexual orientation; citizenship or immigration status - The processing of genetic or “biometric data” to uniquely ID an individual (“biometric data” defined as certain data “used” to ID a specific individual) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Data concerning individual’s status as a crime victim § 9602 (25) p. 4	❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs; sexual activity; sexual orientation; gender identity; national origin, citizenship or immigration status “Genetic”/ “biometric data” (biometric: defined as data that “can be used” to uniquely identify an individual) - Consumer health data (used to ID physical or mental health status, e.g., gender-affirming or reproductive care) - Personal data of a person the controller knows or should know is a minor (<18) - Precise geolocation data (within 1,750 feet) - Social security, driver’s license or nondriver ID number (including the last 4 digits of these numbers); - Billing, financial or payment method information (Except last 4 digits of credit card or similar number) - Account or device log-in, security codes or passwords - Data concerning consumer’s status as a crime victim § 9602 (33) p. 5
	❖ <u>Exception</u> (both types of data above): p. 2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ <u>Exception</u> (both types of data above): p. 1-2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ <u>Exception</u> (both types of data above): p. 2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context
Who is regulated?	❖ Controller: person that alone or jointly with others determines purpose and means of processing personal data p. 2 ❖ Processor: person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p. 3	❖ Controller: person that alone or jointly with others determines purpose and means of processing personal data p. 2 ❖ Processor: person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p. 3	❖ Controller: person that alone or jointly with others determines purpose and means of processing personal data p. 2 ❖ Processor: person that processes (uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p. 4

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Consumer Rights <u>LD 1088</u> § 9604 p. 8 § 9609 (3,4) p. 15-16 <u>LD 1224</u> § 9604 p. 7-8 § 9609 (3,4) p. 14 <u>LD 1822</u> § 9606 p. 7-10 § 9612 (2) p. 19	❖ A consumer (or parent if child <13, guardian or conservator) has a right, upon making an authenticated request, to: • Confirm whether controller processes personal data • Access own personal data processed by controller • Correct inaccuracies in own personal data • Delete personal data about the consumer • Obtain a portable copy of own personal data from a controller; and, if technically feasible, in a way that can be transmitted to another controller <u>Exceptions:</u> • Controller need not disclose: (a) info. that would reveal a trade secret; (b) de-identified data or data controller is not reasonably capable of associating w/the consumer; (c) data it does not use to recognize the consumer; or (d) pseudonymous data if the information necessary to associate it with consumer is kept separately • If the controller does not sell the personal data or voluntarily disclose the data to anyone other than a processor, it need not respond to a consumer request • If controller did not itself collect the data the consumer requests be deleted, it may retain the minimum data necessary to ensure data remains deleted in its system and not use it for any other purpose	❖ A consumer (or parent if child <13, guardian or conservator) has a right, upon making an authenticated request, to: • Confirm whether controller processes personal data • Access own personal data processed by controller • Correct inaccuracies in own personal data • Delete personal data about the consumer • Obtain a portable copy of own personal data from a controller; and, if technically feasible, in a way that can be transmitted to another controller <u>Exceptions:</u> • Controller need not disclose: (a) info. that would reveal a trade secret; (b) de-identified data or data controller is not reasonably capable of associating w/the consumer; (c) data it does not use to recognize the consumer; or (d) pseudonymous data if the information necessary to associate it with consumer is kept separately • If the controller does not sell the personal data or voluntarily disclose the data to anyone other than a processor, it need not respond to a consumer request • If controller did not itself collect the data the consumer requests be deleted, it may retain the minimum data necessary to ensure data remains deleted in its system and not use it for any other purpose <u>or</u> opt the consumer out of processing that personal data	❖ A consumer (or parent if child <13, guardian or conservator) has a right, upon making an authenticated request, to: • Confirm whether controller processes personal data • Access own personal data processed by controller • Correct inaccuracies in own personal data • Delete personal data about the consumer — unless the controller is required by law to retain the personal data • When processing is by automatic means, obtain a portable copy of own personal data from a controller; if technically feasible, in a way that can be transmitted to another controller • Obtain a list of 3rd parties to which controller sold the consumer's personal data (or anyone's personal data) <u>Exceptions:</u> • Controller need not disclose: (a) info. that would reveal a trade secret; (b) de-identified data or data controller is not reasonably capable of associating w/the consumer; or (c) data it does not use to recognize the consumer • If the controller does not sell the personal data or voluntarily disclose the data to anyone other than a processor, it need not respond to a consumer request • If controller did not itself collect the data the consumer requests be deleted, it may retain the minimum data necessary to ensure data remains deleted in its system and not use it for any other purpose
Exercising consumer rights	❖ Request / appeal process: § 9604 (3-4) p. 9 • Each consumer may make one free request per year <u>except</u> controller may charge a reasonable fee or decline manifestly unfounded, excessive or repetitive requests • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must respond without undue delay and within 45 days of request (may extend once for 45 days) • If declines a request, must do so within 45 days, giving a justification and info. on how to appeal the decision	❖ Request / appeal process: § 9604 (3-4) p. 9 • Each consumer may make one free request per year <u>except</u> controller may charge a reasonable fee or decline manifestly unfounded, excessive or repetitive requests • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must respond without undue delay and within 45 days of request (may extend once for 45 days) • If declines a request, must do so within 45 days, giving a justification and info. on how to appeal the decision	❖ Request / appeal process: § 9606 (5-6) p. 10-11 • Each consumer may make one free request per year <u>except</u> controller may charge a reasonable fee or decline a manifestly unfounded, excessive, technically infeasible or repetitive requests • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must respond without undue delay and within 45 days of request (may extend once for 45 days) • If declines a request, must do so within 45 days, giving a justification and info. on how to appeal the decision

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG
Required privacy notice <u>LD 1088</u> <u>§ 9606(5) p. 11</u> <u>LD 1224</u> <u>§ 9606(5) p. 10</u> <u>LD 1822</u> <u>§ 9608(4) p. 13</u>	❖ Controller must provide accessible, clear privacy notice in plain language understandable by reasonable consumer stating: • Categories of personal data processed (remember, process includes collection) by controller • Purpose for processing personal data • How consumers may exercise their consumer rights • Categories of personal data shared with 3rd parties • Categories of 3rd parties personal data is shared with • Controller's contact information (active e-mail or other)	❖ Controller must provide accessible, clear privacy notice in plain language understandable by reasonable consumer stating: • Categories of personal data processed (remember, process includes collection) by controller • Purpose for processing personal data • How consumers may exercise their consumer rights • Categories of personal data shared with 3rd parties • Categories of 3rd parties personal data is shared with • Controller's contact information (active e-mail or other)	❖ Controller must provide accessible, clear privacy notice in plain language understandable by reasonable consumer stating: • Categories of personal data, including sensitive data, processed (does not include collecting) by controller • Purpose for processing personal data • How long controller intends to retain each category of personal data (or criteria for deciding how long) • How consumers may exercise their consumer rights • Categories of personal data, including sensitive data, shared with 3rd parties • Categories of 3rd parties personal data is shared with — with level of detail to allow consumer to understand type of processing conducted by each category • Controller's contact information (active e-mail or other)
Targeted Advertising Definition	"Targeted advertising" means displaying an advertisement 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. p. 5	"Targeted advertising" means displaying an advertisement 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. p. 4	"Targeted advertising": A. Means displaying advertisements to a consumer or on a device identified by a unique identifier when the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications that are unaffiliated with each other in order to predict the consumer's preferences or interests; and B. Does not include: (1) Advertisements based on the context of a consumer's current search query or visit to a website or online application; (2) Advertisements based on a consumer's activities within a controller's own websites or online applications; (3) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or (4) Processing personal data solely to measure or report advertising frequency, performance or reach. p. 6

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Data minimization	❖ Must limit collection of personal data to what is §9606(1) P.10 “adequate, relevant and reasonably necessary” to the processing purpose disclosed to the consumer (in the privacy notice) ❖ Must process minimum amount of personal data “reasonably necessary, adequate or relevant” to each disclosed purpose (in the privacy notice)	❖ Must limit collection of personal data to what is §9606(1) P.9 “adequate, relevant and reasonably necessary” to the processing purpose disclosed to the consumer (in the privacy notice)	❖ Must limit collection of personal data to what is §9605(2)(a) P.12 “reasonably necessary and proportionate to provide or maintain the specific product or service requested by the consumer” ❖ Must limit collection and processing of sensitive data to what is “strictly necessary” to provide or maintain the specific product or service requested by the consumer §9605(1)(a) P.12
Consent requirements	LD 1088 §9606(1-3) P.10-11 §9604(1)(E) P.8 ❖ Prohibited activities (regardless of consent) - Process personal data of a minor known (or willfully disregarded) to be 13-15 for targeted advertising - Process data of a known child <13 years old in violation of federal COPPA law/regulation requirements ❖ Activities permitted only with consent (opt-in) - Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose — as a matter of law, sale of sensitive data is not “reasonably necessary [or] compatible” - Process sensitive data for any purpose (this consent requires disclosure of specific processing purpose, categories of sensitive data to be processed, and identity of any 3rd parties to whom the data is sold. If there is no contact for 24 months, customer must opt-in again). - Sell personal data of a minor known (or willfully disregarded) to be age 13-15 <u>Exceptions:</u> “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction.	❖ Prohibited activities (regardless of consent) - Process personal data of a minor known (or willfully disregarded) to be 13-15 for targeted advertising - Process data of a known child <13 years old in violation of federal COPPA law/regulation requirements ❖ Activities permitted only with consent (opt-in) - Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose - Process sensitive data for any purpose - Sell personal data of a minor known (or willfully disregarded) to be age 13-15 <u>Exceptions:</u> “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction.	❖ Prohibited activities (regardless of consent) - Sell any consumer’s sensitive data (includes all personal data of known (should know) minor (<18)) - Process personal data of a person known (should know) to be a minor (<18) for targeted advertising ❖ Activities permitted only with consent (opt-in) - Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose Retain personal data past the time “when it is no longer necessary for the purpose for which the data was processed”
	LD 1224 §9606(1-3) P.9-10 §9604(1)(E) P.7-8 ❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <16) - For targeted advertising - For sale (see exceptions to “sale” above) - For profiling in furtherance of automated decisions producing legal or similarly significant effects	LD 1822 §9608(1-2) P.12-13 §9606(1)(G) P.9 ❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <16) - For targeted advertising - For sale (see exceptions to “sale” above) - For profiling in furtherance of automated decisions producing legal or similarly significant effects	❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <18) - For targeted advertising - For sale (same exceptions to “sale” as in LD 1088 & 1224) - For profiling in furtherance of automated decisions producing legal or similarly significant effects

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Consent Mechanisms <i>Opt-In</i> <i>See "consent" definitions p.1 all bills</i> <i>Revoke</i> <i>1088 - p.10</i> <i>1224 - p.9-10</i> <i>1822 - p.13</i>	❖ Opt-In "consent" mechanism / requirements: - Opt-in consent may be provided by (a) consumer or (b) parent or legal guardian of minor consumer <13 years old (in accordance with federal COPPA law) p. 8 - Clear, affirmative act unambiguously signaling consent - In language consumer uses to obtain the product or service and reasonably accessible to those w/ disabilities May not be based on: (a) Accepting a terms of use agreement (containing info. unrelated to consenting); (b) hovering over, muting, pausing or closing content; or (c) use of dark pattern to obtain agreement Mechanism to revoke consent must be at least as easy as mechanism to provide consent and controller must cease processing within 15 days of revocation	❖ Opt-In "consent" mechanism / requirements: - Opt-in consent may be provided by (a) consumer or (b) parent or legal guardian of minor consumer <13 years old (in accordance with federal COPPA law) p. 7 - Clear, affirmative act unambiguously signaling consent May not be based on: (a) Accepting a terms of use agreement (containing info. unrelated to consenting); (b) hovering over, muting, pausing or closing content; or (c) use of dark pattern to obtain agreement Mechanism to revoke consent must be at least as easy as mechanism to provide consent and controller must cease processing within 15 days of revocation	❖ Opt-In "consent" mechanism / requirements: - Opt-in consent may be provided by (a) consumer or (b) parent or legal guardian of minor consumer <13 years old (in accordance with federal COPPA law) p. 8 - Clear, affirmative act unambiguously signaling consent to process personal data for a particular purpose May not be based on: (a) Accepting a terms of use agreement (containing info. unrelated to consenting); (b) hovering over, muting, pausing or closing content; or (c) use of dark pattern to obtain agreement Mechanism to revoke consent must be at least as easy as mechanism to provide consent and controller must cease processing within 30 days of revocation
	❖ Opt-out notice: Controller must clearly and conspicuously disclose on website the following & the method for opting out: - That it sells personal data to 3rd parties - That it processes personal data for targeted advertising § 9606(7) p.12 ❖ Opt-Out mechanism / requirements: - Consumer (or parent if child <13 or a guardian or conservator) or designated agent may exercise opt-out rights (e.g., via browser or global device setting) § 9605 p.7-10 - Must be secure and reliable and may not require new account. Must use links similar to "Do not sell my personal data" or "Opt me out of targeted advertising" or a single link similar to "Your Privacy Choices" By Dec. 1, 2027 – Universal Opt-Out: must allow consumer to use an opt-out signal sent by a platform, technology or other mechanism used by the consumer that is consumer friendly; does not unfairly disadvantage another controller; does not use a default setting; is consistent with other opt-out mechanisms required by federal or state law; and allows controller to reasonably determine the consumer is a Maine resident	❖ Opt-out notice: Controller must clearly and conspicuously disclose on website the following & the method for opting out: - That it sells personal data to 3rd parties - That it processes personal data for targeted advertising § 9606(7) p.11 ❖ Opt-Out mechanism / requirements: - Consumer (or parent if child <13, or a guardian or conservator) or – to opt out of only sale or targeted advertising, but not profiling: designated agent may exercise opt-out rights (e.g., via browser setting or global device setting) § 9605 p.7 - Must be secure and reliable and may not require new account By Dec. 1, 2027 – Universal Opt-Out: must allow consumer to use an opt-out signal sent by a platform, technology or other mechanism used by the consumer that is consumer friendly; does not unfairly disadvantage another controller; does not use a default setting; is consistent with other opt-out mechanisms required by federal or state law; and allows controller to reasonably determine the consumer is a Maine resident	❖ Opt-out notice: Controller must clearly and conspicuously disclose on website the following & the method for opting out: - That it sells personal data to 3rd parties - That it processes personal data for targeted advertising - That it processes personal data for profiling § 9605(5) p.13-14 ❖ Opt-Out mechanism / requirements: - Consumer (or parent if child <13 or a guardian or conservator) or designated agent may exercise opt-out rights (e.g., via browser or global device setting) § 9607 p.12 - Must be secure and reliable and may not require new account § 9608(6) p.14 By July 1, 2026 – Universal Opt-Out: must allow consumer to use an opt-out signal sent by a platform, technology or other mechanism used by the consumer that is consumer friendly and in easy-to-understand language; does not unfairly disadvantage another controller; does not use a default setting; is consistent with other opt-out mechanisms required by federal or state law; and allows controller to reasonably determine the consumer is a Maine resident — if conflicts with loyalty program, may notify and ask to confirm opt-out
	§ 9606 (6-8) p.12-13	§ 9606 (6-8) p.10-11	§ 9608 (6)(C)(2) p.14-15

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Retaliation prohibition § 9606(3)(D)+(4) p.11 LD 1224 § 9606(3)(D)+(4) p.10 LD 1822 § 9608(1)(E)+(3) p.12	❖ Controller may not discriminate against consumer for exercising a right under this law, including by: - Denying or charging different prices for goods/services - Providing different level or quality of goods or services <u>Exceptions:</u> - Need not offer product or service without having required personal data - May offer different price, quality or selection of goods or services via a voluntary consumer loyalty program	❖ Controller may not discriminate against consumer for exercising a right under this law, including by: - Denying or charging different prices for goods/services - Providing different level or quality of goods or services <u>Exceptions:</u> - Need not offer product or service without having required personal data - May offer different price, quality or selection of goods or services via a voluntary consumer loyalty program	❖ Controller may not discriminate against consumer for exercising a right under this law, including by: - Denying or charging different prices for goods/services - Providing different level or quality of goods or services <u>Exceptions:</u> - Need not offer product or service without having required personal data - May offer different price, quality or selection of goods or services via a voluntary consumer loyalty program - sale of personal data may not be a program condition
Discrimination prohibitions	❖ Controller may not § 9606(3)(E) p.11 Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers	❖ Controller may not: § 9606(3)(E) p.10 Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers	❖ Controller may not: § 9608(1)(C),(F) p.12 - Process (use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers - Collect, process or disclose personal data or publicly available info. in a way that unlawfully discriminates or prevents equal enjoyment of goods or services on basis of individual's actual or perceived protected class status <u>Except:</u> may self-test to prevent discrimination or diversify applicant pool. Does not apply to a private club exempt from Title II of the Civil Rights Act.
Geofence prohibition	❖ Person may not use geofence (1,750 foot virtual perimeter) around health care facility for purpose of identifying, tracking, collecting data from or sending notices regarding consumer health data to a consumer who enters the virtual perimeter § 9606 p.16 <u>Exception:</u> Facility operator's geofence (ex: to check in patients)	No geofence prohibition	❖ Person may not use geofence (1,750 foot virtual perimeter) around health care facility for purpose of identifying, tracking, collecting data from or sending notices regarding consumer health data a consumer § 9605(3) p.7 <u>Exception:</u> Facility operator's geofence (ex: to check in patients)
Data Security and Retention § 9606(2)(C) p.10	❖ Controller must establish and implement reasonable data security practices to protect confidentiality, accessibility and integrity of data appropriate to the volume and nature of data ❖ Controller must establish and implement a data retention schedule requiring deletion or de-identification when retention of the data is "no longer reasonably necessary and relevant" to disclosed purposes for processing data—unless controller is required to retain the personal data longer by law § 9606(2)(C) p.10	❖ Controller must establish and implement reasonable data security practices to protect confidentiality, accessibility and integrity of data appropriate to the volume and nature of data § 9606(2)(C) p.9 No data retention schedule required	❖ Controller must establish and implement reasonable data security practices to protect confidentiality, accessibility and integrity of data appropriate to the volume and nature of data § 9608(2)(C) p.12 ❖ Controller must establish and implement a data retention schedule requiring destruction or permanent deletion of data when retention of the data is "no longer necessary" for the processing purpose — unless consumer consents to longer time or controller is required to retain the personal data longer by law § 9608(2)(C) p.12-13

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Data Protection Assessments <u>LD 1088</u> §9608 p. 14-15 <u>LD 1224</u> §9608 p. 12-13 <u>LD 1822</u> §9611 p. 17-18	❖ Controller must conduct and document data protection assessment(s) weighing direct and indirect benefits to controller, consumer and public of processing the data against the risks to consumers of processing the data, as mitigated by safeguards employable by the controller What activities must be assessed? All activities presenting a heightened risk to consumers that are created or initiated after July 1, 2026, including: • Processing of sensitive data • Processing personal data for targeted advertising • Sale of personal data • Processing of personal data for profiling that presents a reasonably foreseeable risk of unfair treatment of consumers, of physical, reputational or financial injury to consumers, offensive intrusion on consumer's private affairs; or other "substantial injury" Copy to AG: Must provide copy of assessment to AG on request (if relevant to an investigation). • Assessment is confidential (for FOAA purposes) • Disclosure to AG as required by law doesn't waive attorney-client or work-product privileges	❖ Controller must conduct and document data protection assessment(s) weighing direct and indirect benefits to controller, consumer and public of processing the data against the risks to consumers of processing the data, as mitigated by safeguards employable by the controller What activities must be assessed? All activities presenting a heightened risk to consumers that are created or initiated after July 1, 2026, including: • Processing of sensitive data • Processing personal data for targeted advertising • Sale of personal data • Processing of personal data for profiling that presents a reasonably foreseeable risk of unfair treatment of consumers, of physical, reputational or financial injury to consumers, offensive intrusion on consumer's private affairs; or other "substantial injury" Copy to AG: Must provide copy of assessment to AG on request (if relevant to an investigation). • Assessment is confidential (for FOAA purposes) • Disclosure to AG as required by law doesn't waive attorney-client or work-product privileges	❖ Controller must conduct and document data protection assessment(s) weighing direct and indirect benefits to controller, consumer and public of processing the data against the risks to consumers of processing the data, as mitigated by safeguards employable by the controller and the necessity and proportionality of processing vs stated processing purpose What activities must be assessed? All activities presenting a heightened risk to consumers, including each algorithm that is used, that occur after July 1, 2026, including: • Processing of sensitive data • Processing personal data for targeted advertising • Sale of personal data • Processing of personal data for profiling that presents a reasonably foreseeable risk of unfair treatment of consumers, of physical, reputational or financial injury to consumers, offensive intrusion on consumer's private affairs; or other "substantial injury" When required? Within 6 months of first engaging in the activity or of making a material change to that activity Copy to AG: Must provide copy of assessment to AG on request (if relevant to an investigation). • Assessment is confidential (for FOAA purposes) • AG may use the assessment in an enforcement action • Disclosure to AG as required by law doesn't waive attorney-client or work-product privileges
Processor duties and prohibitions	❖ Processor must: §9607 p. 13-14 • Assist controller with meeting obligations of this law • Assist controller with responding to consumer requests • Notify controller of any security breach in processor's system (when notice to consumer of a security breach is required by current Maine law: Title 10, chapter 210-B) • Provide necessary information to enable controller to conduct data protection assessments • Act only under contract with controller requiring it to: ◦ Ensure each person processing personal data is subject to a duty of confidentiality	❖ Processor must: §9607 p. 11-12 • Assist controller with meeting obligations of this law • Assist controller with responding to consumer requests • Notify controller of any security breach in processor's system (when notice to consumer of a security breach is required by current Maine law: Title 10, chapter 210-B) • Provide necessary information to enable controller to conduct data protection assessments • Act only under contract with controller requiring it to: ◦ Ensure each person processing personal data is subject to a duty of confidentiality	❖ Processor must: §9609 p. 15-16 • Assist controller with meeting obligations of this law • Assist controller with responding to consumer requests • Notify controller of any security breach in processor's system (when notice to consumer of a security breach is required by current Maine law: Title 10, chapter 210-B) • Provide necessary information to enable controller to conduct data protection assessments • Act only under contract with controller requiring it to: ◦ Ensure each person processing personal data is subject to a duty of confidentiality

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	○ Delete or return personal data at end of processing activity, unless retention required by law ○ Give controller requested information to demonstrate processor's compliance with law ○ Cooperate with controller assessments or share independent assessments of its own services ○ Require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract ❖ Processor may not: §9607(4) p.14 • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1088)	○ Delete or return personal data at end of processing activity, unless retention required by law ○ Give controller requested information to demonstrate processor's compliance with law ○ Cooperate with controller assessments or share independent assessments of its own services ○ Require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract ❖ Processor may not: §9607(4) p.12 • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1224)	○ Delete or return personal data at end of processing activity, unless retention required by law ○ Give controller requested information to demonstrate processor's compliance with law ○ Cooperate with controller assessments or conduct independent assessments of its own services ○ After giving controller opportunity to object to use of subcontractor, require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract ○ Establish and implement reasonable data security practices for data confidentiality and integrity ○ Stop processing data on request of controller in response to consumer's authenticated request ❖ Processor may not: §9609(4) p.16-17 • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1822)
Third-party responsibilities	n/a	n/a	❖ Third party that receives personal data must: §9610 p.17 • Notify consumer if it intends to use or share the data in a manner inconsistent with disclosures made at the time the data was collected — with enough time to permit the consumer to exercise the consumer's rights
Duties involving de-identified data	❖ Controller in possession of de-identified data must: • Take reasonable measures to prevent re-identifying data • Publicly commit to not attempting to re-identify data • Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations §9609(4) p.15	❖ Controller in possession of de-identified data must: • Take reasonable measures to prevent re-identifying data • Publicly commit to not attempting to re-identify data • Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations §9609(4) p.14	❖ Controller in possession of de-identified data must: • Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations — whether the steps are reasonable depends in part on whether the data would be sensitive data if re-identified §9612 p.19
Additional Consumer health data Requirements	n/a	n/a	❖ Person may not provide employee or contractor with access to consumer health data unless: • Employer or contractor is subject to contractual or statutory duty of confidentiality; or • Confidentiality is a condition of employment ❖ Person may not provide processor with access to consumer health data unless the person requires the processor to protect the data via the processing contract described above

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
"Small business" exception <u>LD 1088</u> § 9603(1-2) p. 5-6 <u>LD 1224</u> § 9603(1-2) p. 5 <u>LD 1822</u> § 9603 p. 6	From July 1, 2026, to December 31, 2027: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥100,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived >25% of gross revenue from the sale of personal data Beginning January 1, 2028: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥50,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	From July 1, 2026, to December 31, 2027: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥100,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived >25% of gross revenue from the sale of personal data Beginning January 1, 2028: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥50,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	Beginning July 1, 2026: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥35,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥10,000 Maine residents and derived >20% of gross revenue from the sale of personal data
Exempt entities <u>LD 1088</u> § 9603(3) p. 6 <u>LD 1224</u> § 9603(3) p. 5 <u>LD 1822</u> § 9604(1) p. 6-7	❖ Law <u>not</u> applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Financial institution, affiliate or "service corporation" (defined in Title 9-B) subject to the federal Gramm-Leach-Bliley Act — only if it is directly and solely engaged in financial activities described in GLBA • A "licensee" under Maine's insurance laws — to the extent it is complying with any applicable data security and privacy requirements in Maine insurance law	❖ Law <u>not</u> applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Financial institution, affiliate or "service corporation" (defined in Title 9-B) subject to the federal Gramm-Leach-Bliley Act • A "licensee" under Maine's insurance laws — to the extent it is complying with any applicable data security and privacy requirements in Maine insurance law • A nonprofit organization established to detect and prevent fraudulent acts in connection with insurance (NICB)	❖ Law <u>not</u> applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • Nonprofit corporation (501(c)(3), (4), (6), and (12)); • Institution of higher education; • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA); • A supervised financial organization or service corp. (defined in Title 9-A & 9-B of Maine banking laws); • A health care facility or practitioner (as defined in state law) or affiliate that qualifies as a business associate serving only covered entities under HIPAA; • A "licensee" under Maine's insurance laws — to the extent it is complying with any applicable data security and privacy requirements in Maine insurance law • An ISP covered by 35-A M.R.S. §9301 — but only to the extent it is providing ISP services
Exempt data	❖ Law <u>not</u> applicable to (types of data): § 9603(4) p. 6-7 • Data regulated by GLBA if it is collected, processed, sold or disclosed in accordance with the GLBA	❖ Law <u>not</u> applicable to (types of data): § 9603(4) p. 5-7 • Data regulated by GLBA if it is collected, processed, sold or disclosed in accordance with the GLBA	❖ Law <u>not</u> applicable to (types of data): § 9604(2) p. 7-8 • Data regulated by GLBA if it is collected, processed, sold or disclosed in accordance with the GLBA

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	- HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA - Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) - Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines - Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 - Info. created for purposes of or info. regulated by: - Health Care Quality Improvement Act of 1986 - Family Educational Rights and Privacy Act of 1974 - Airline Deregulation Act of 1978 - Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: - Fair Credit Reporting Act - Driver’s Privacy Protection Act of 1994 - Farm Credit Act of 1971 - Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives	- HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA - Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) - Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines - Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 - Health care information defined in 22 M.R.S. §1711-C Info. created for purposes of or regulated by: - Health Care Quality Improvement Act of 1986 - Family Educational Rights and Privacy Act of 1974 - Airline Deregulation Act of 1978 - Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: - Fair Credit Reporting Act - Driver’s Privacy Protection Act of 1994 - Farm Credit Act of 1971 - Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives	- HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA - Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) - Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines - Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 - Info. created for purposes of or regulated by: - Health Care Quality Improvement Act of 1986 - Family Educational Rights and Privacy Act of 1974 - Airline Deregulation Act of 1978 - Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: - Fair Credit Reporting Act - Driver’s Privacy Protection Act of 1994 - Farm Credit Act of 1971 - Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives
Exempt activities <u>LD 1088</u> §9611 (1-2) p. 16-17 <u>LD 1224</u> §9610 (1-2) p. 14-15 <u>LD 1822</u> §9613 (1-2) p. 19-20	❖ Controller / Processor activities <u>not</u> affected by LD 1088: - Complying with federal or Maine laws or rules - Complying with investigations, subpoenas or summonses by federal, Maine or tribal authorities - Cooperating with federal, Maine or tribal law enforcement concerning conduct the entity believes in good faith may violate federal or Maine laws or rules - Investigating, exercising or defending legal claims - Providing product or service requested by consumer, including performing contracted services (ex: warranty) - Taking requested steps prior to entering a contract - Taking immediate steps to protect life or physical safety of a consumer or other individual	❖ Controller / Processor activities <u>not</u> affected by LD 1224: - Complying with federal, any state or local laws - Complying with investigations, subpoenas or summonses by federal, any state or tribal authorities - Cooperating with federal, state or tribal law enforcement concerning conduct the entity believes in good faith may violate federal or state laws or rules - Investigating, exercising or defending legal claims - Providing product or service requested by consumer, including performing contracted services (ex: warranty) - Taking requested steps prior to entering a contract - Taking immediate steps to protect the life or physical safety of a consumer or other individual	❖ Controller / Processor activities <u>not</u> affected by LD 1224: - Complying with federal, Maine or local laws or rules - Complying with investigations, subpoenas or summonses by federal, Maine or tribal authorities - Cooperating with federal, Maine or tribal law enforcement concerning conduct the entity believes in good faith may violate federal, Maine or local laws or rules - Investigating, exercising or defending legal claims - Providing product or service requested by consumer, including performing contracted services (ex: warranty) - Taking requested steps prior to entering a contract - Taking immediate steps to the life or physical safety of a consumer or other individual

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	- Preventing or responding to security incidents, identity theft, fraud, harassment, deceptive or illegal activity, system integrity or reporting those incidents - Engaging in scientific or statistical research in the public interest that adheres to all other ethics and privacy laws and is overseen by an Institutional Review Board (IRB) - Assisting another controller, processor or 3rd party with its compliance with this law - Process personal data for public health purposes subject to confidentiality obligations of federal or state laws - Collection, use or retention of data for internal use: - Internal R&D to improve or repair products, - Product recalls, - Identifying and repairing technical errors, and - Internal operations reasonably aligned with expectations of the consumer or compatible with processing data to provide a product or service specifically requested by the consumer	- Preventing or responding to security incidents, identity theft, fraud, harassment, deceptive or illegal activity, system integrity or reporting those incidents - Engaging in scientific or statistical research in the public interest that adheres to all other ethics and privacy laws and is overseen by an IRB - Assisting another controller, processor or 3rd party with its compliance with this law - Process personal data for public health purposes subject to confidentiality obligations of federal or state laws - Collection, use or retention of data for internal use: - Internal R&D to improve/repair products, - Product recalls, - Identifying and repairing technical errors, and - Internal operations reasonably aligned with expectations of the consumer or compatible with processing data to provide a product or service specifically requested by the consumer	- Preventing or responding to security incidents, identity theft, fraud, harassment, deceptive or illegal activity, system integrity or reporting those incidents (<i>slightly different wording from LD 1088 and LD 1224</i>) - Assisting another controller, processor or 3rd party with its compliance with this law - Collection, use or retention of data for internal use: - Product recalls, - Identifying and repairing technical errors, and - Internal operations reasonably aligned with expectations of the consumer or compatible with processing data to provide a product or service specifically requested by the consumer
Remedies for violations <u>LD 1088</u> § 9612 p.18-19 <u>LD 1224</u> § 9611 p.17 <u>LD 1822</u> § 9614 p.21-22	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Must provide at least 30-days advance notice and opportunity to confer with AG's Office — unless show facts in affidavit demonstrating immediate irreparable harm to consumers in the State if notice is given ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Must provide at least 30-days advance notice - AG may not bring action unless controller fails to cure an alleged violation listed in the notice within 30 days ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: Until April 1, 2027, if AG believes it is possible for a controller or processor to cure a violation, may choose to give notice of the violation prior to initiating suit - If notice is given, AG may not bring action unless violation is not cured within 60 days - Factors regarding whether to give notice: number of violations, size and complexity of defendant, nature and extent of defendant's processing activities, likelihood of injury to public, degree to which violations affect safety, whether the alleged violation was likely a human or technical error, and past violations by defendant of this or similar laws ❖ No private right of action ❖ AG rulemaking authority under UTPA to interpret law

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Other exemptions	❖ Law does not / may not be construed to: §9611(3.5) p. 17 - Apply if compliance requires violation of an evidentiary privilege under Maine law - Apply to processing of personal data by person purely for own household use - Impose an obligation that adversely affects rights of freedom of speech or of the press (including state law on confidentiality of journalist's confidential sources)	❖ Law does not / may not be construed to: §9610(3.5) p. 16 - Apply if compliance requires violation of an evidentiary privilege under Maine law - Apply to processing of personal data by person purely for own household use - Impose an obligation that adversely affects rights of freedom of speech or of the press (including state law on confidentiality of journalist's sources)	❖ Law does not / may not be construed to: §9613(3.5) p. 20 - Apply if compliance requires violation of an evidentiary privilege under state law - Apply to processing of personal data by person purely for own household use - Impose an obligation that adversely affects the rights or freedoms of any person, including freedom of speech or of the press or freedom to engage in political activity
Exceptions to liability	❖ Exceptions to liability: §9614(4) p. 18 - Controller not liable if processor or 3rd party violates law absent actual knowledge that it would do so - Processor/3rd party not liable for controller's violations	❖ Exceptions to liability: §9610(4) p. 16 - Controller not liable if processor or 3rd party violates law absent actual knowledge that it would do so - Processor/3rd party not liable for controller's violations	❖ Exceptions to liability: §9613(4) p. 20 - Controller not liable if both (1) processor or 3rd party violates law absent actual knowledge that it would do so <u>and</u> (2) controller has remained in compliance with law - Processor/3rd party not liable for controller's violations
Maine Privacy Fund 1088 - §9613 p. 19 1224 - §9612 p. 17	❖ Establishes nonlapsing Maine Privacy Fund consisting of: - All monetary penalties, attorneys fees or costs - Any appropriations, donations and interest earned ❖ Uses: funds must be used to provide funding for the staff and activities necessary to the Attorney General under this law	❖ Establishes nonlapsing Maine Privacy Fund consisting of: - All monetary penalties, attorneys fees or costs - Any appropriations, donations and interest earned ❖ Uses: funds must be used to provide funding for the staff and activities necessary to the Attorney General under this law	Does not establish a Maine Privacy Fund
Effect on current Maine ISP Law	❖ Repeals 35-A M.R.S. §9301, which generally requires Internet Service Providers (ISPs) to obtain consent before using, disclosing or selling a customer's personally identifying info. p. 19	Does not repeal ISP law	Does not repeal ISP law (but exempts ISPs to extent they are acting solely as ISPs)
Preemption of local laws	n/a	❖ Law preempts any ordinance or other regulation adopted by a political subdivision of the State re: processing (includes collection) of personal data by controllers/processors §9611(4) p. 17	n/a
Effective Date	July 1, 2026 p. 20	July 1, 2026 p. 18	July 1, 2026 p. 22
Reporting Requirement	❖ Attorney General must submit report by January 1, 2028, to the Judiciary Committee containing: - Data on number of 30-day notices of violation sent; nature of the alleged violations; number that conferred with OAG to prevent enforcement action; number of civil actions brought to enforce the law - Any recommendations for improving the law Committee may report out legislation in 133rd Legislature (R2)	❖ Attorney General must submit report by February 1, 2027, to the Judiciary Committee containing: - Data on number of notices of violation sent; nature of the alleged violations; number that conferred with OAG to prevent enforcement action; number of civil actions brought to enforce the law - Any recommendations for improving the law Committee may report out legislation in 133rd Legislature (R1)	❖ Attorney General must submit report by February 1, 2027, to the Judiciary Committee containing: - Data on number of notices of violation sent; nature of the alleged violations; number that conferred with OAG to prevent enforcement action; number of civil actions brought to enforce the law - Any recommendations for improving the law Committee may report out legislation in 133rd Legislature (R1)



Approved: 04/28/25 **LRL**

132nd MAINE LEGISLATURE

LD 1088

LR 2064(01)

An Act to Enact the Maine Consumer Data Privacy Act

Preliminary Fiscal Impact Statement for Original Bill

Sponsor: Rep. Henderson of Rumford

Committee: Judiciary

Fiscal Note Required: Yes

Preliminary Fiscal Impact Statement

	FY 2025-26	FY 2026-27	Projections FY 2027-28	Projections FY 2028-29
Appropriations/Allocations				
Other Special Revenue Funds	\$500	\$500	\$500	\$500

Correctional and Judicial Impact Statements

This bill may increase the number of civil suits filed in the court system. The additional workload associated with the minimal number of new cases filed in the court system does not require additional funding at this time. The collection of additional filing fees will increase General Fund revenue by minor amounts.

Fiscal Detail and Notes

The bill establishes the Maine Privacy Fund within the Office of the Attorney General with a base Other Special Revenue Funds allocation of \$500 beginning in fiscal year 2025-26.

Any additional costs to the Office of the Attorney General associated with enforcing the Maine consumer data privacy act are expected to be minor and can be absorbed within existing budgeted resources.

ROS
COPY¹
2

L.D. 1088

Date:

(Filing No. H-)

JUDICIARY

Reproduced and distributed under the direction of the Clerk of the House.

**STATE OF MAINE
HOUSE OF REPRESENTATIVES
132ND LEGISLATURE
FIRST SPECIAL SESSION**

COMMITTEE AMENDMENT " " to H.P. 710, L.D. 1088, "An Act to Enact the
Maine Consumer Data Privacy Act"

Amend the bill by striking out all of section 1 and inserting the following:

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

CHAPTER 1057

MAINE CONSUMER DATA PRIVACY ACT

§9601. Short title

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

§9602. Definitions

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

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

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

A. A digital or physical photograph;

B. An audio or video recording;

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

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

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

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

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

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

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

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

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

25 **7. Control.** "Control" means:

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

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

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

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

33 **9. COPPA.** "COPPA" means the federal Children's Online Privacy Protection Act of
34 1998, 15 United States Code, Section 6501 et seq. and the regulations, rules, guidance and
35 exemptions adopted pursuant to that Act, as that Act and such regulations, rules, guidance
36 and exemptions may be amended from time to time.

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

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

ROS

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

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

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

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

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

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

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

26 **16. Personal data.** "Personal data" means information that is linked or reasonably
 27 linkable to an identified or identifiable consumer or that is linked or reasonably linkable to
 28 a device that is linked or reasonably linkable to an identified or identifiable consumer.
 29 "Personal data" does not include de-identified data or publicly available information.

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

35 A. The content of communications; or

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

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

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

ROS

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

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

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

14 23. Publicly available information. "Publicly available information" means
15 information that:

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

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

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

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

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

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

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

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

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

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

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

37 25. Sensitive data. "Sensitive data" means personal data that includes:

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

41 B. Genetic or biometric data;

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

2 D. Precise geolocation data;

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

6 F. A consumer's account number, log-in information, financial account number or
7 credit or debit card number that, in combination with any required security code, access
8 code or password, permits access to a consumer's financial account; or

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

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

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

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

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

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

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

27 **§9603. Scope**

28 **1. Applicability; July 1, 2026 to December 31, 2027.** From July 1, 2026 to December
29 31, 2027, the provisions of this chapter apply to persons that conduct business in this State
30 or persons that produce products or services that are targeted to residents of this State and
31 that during the preceding calendar year:

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

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

37 **2. Applicability; beginning January 1, 2028.** Beginning January 1, 2028, the
38 provisions of this chapter apply to persons that conduct business in this State or persons
39 that produce products or services that are targeted to residents of this State and that during
40 the preceding calendar year:

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

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

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

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

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

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

14 D. A person or entity that qualifies as a licensee under Title 24-A, section 2263,
15 subsection 8;

16 E. A covered entity or business associate;

17 F. A nonprofit organization that:

18 (1) Does not receive any revenue from the sale of personal data; or

19 (2) That is established to detect and prevent fraudulent acts in connection with
20 insurance; or

21 G. A person or entity that is a motor vehicle dealer franchisee as described in section
22 1171, subsection 7.

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

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

27 B. Health care information as defined in Title 22, section 1711-C, subsection 1,
28 paragraph E;

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

32 D. Patient-identifying information as described in 42 United States Code, Section
33 290dd-2;

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

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

1 G. The protection of human subjects in research under 21 Code of Federal Regulations,
2 Parts 50 and 56, or personal data used or shared in research, as defined in 45 Code of
3 Federal Regulations, Section 164.501, that is conducted in accordance with the
4 standards set forth in paragraphs E and F, or other research conducted in accordance
5 with applicable law;

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

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

13 J. Information that originates from information described in paragraphs C to I, or
14 information that is intermingled so as to be indistinguishable from information
15 described in paragraphs C to I, that a covered entity, business associate or program or
16 activity relating to substance use disorder as described in 42 United States Code,
17 Section 290dd-2, creates, processes or maintains in the same manner as is required
18 under the applicable laws and regulations cited in paragraphs C to I;

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

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

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

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

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

36 P. Data processed or maintained:

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

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

ROS

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

Q. 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.

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

§9604. Consumer rights

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

A. Confirm whether or not a controller is processing the consumer's personal data and to access that personal data, unless such 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;

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; and

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

(1) Targeted advertising;

(2) The sale of personal data; or

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

2. 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 9605 to exercise the rights of the consumer to opt out of the processing of the consumer's personal data as specified in subsection 1, paragraph E, subparagraphs (1) and (2). In the case of processing personal data of a consumer known to be 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.

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

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

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

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

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

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

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

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

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

43 **§9605. Authorized agent**

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

11 **§9606. Actions of controllers**

12 **1. Data minimization.** A controller must comply with the requirements of this
13 subsection.

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

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

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

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

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

28 B. In the case of the processing of sensitive data concerning a consumer known to be
29 a child, process the data in accordance with COPPA; and

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

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

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

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

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

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

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

4 D. Retaliate against a consumer for exercising a consumer right in this chapter or for
5 not agreeing to the collection or processing of personal data for a separate product or
6 service, including by denying goods or services, charging different prices or rates for
7 goods or services or providing a different level of quality of goods or services to the
8 consumer.

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

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

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

20 B. The purpose for processing personal data;

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

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

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

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

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

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

41 A. A clear and conspicuous link titled "Do Not Sell My Personal Data" or bearing a
42 substantially similar title on the controller's publicly accessible website that directs the

1 consumer, or an agent of the consumer, to a publicly accessible website that enables
2 the consumer, or an agent of the consumer, to opt out of the sale of the consumer's
3 personal data; and

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

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

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

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

28 B. May not unfairly disadvantage another controller;

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

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

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

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

39 **§9607. Responsibilities of processors and controllers**

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

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

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

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

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

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

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

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

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

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

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

38 **4. Fact-based determination.** Determining whether a person is acting as a controller
39 or processor with respect to a specific processing of data is a fact-based determination that
40 depends upon the context in which personal data is to be processed. A person who is not
41 limited in the person's processing of personal data pursuant to a controller's instructions, or
42 who fails to adhere to the instructions, is a controller and not a processor with respect to a
43 specific processing of data. A processor that continues to adhere to a controller's
44 instructions with respect to a specific processing of personal data remains a processor. If

1 a processor begins, alone or jointly with other persons, determining the purposes and means
2 of the processing of personal data, the processor acts as a controller with respect to the
3 processing and may be subject to an enforcement action under section 9611.

4 **§9608. Data protection assessments**

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

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

10 B. The sale of personal data;

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

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

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

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

18 (4) Other substantial injury to consumers; and

19 D. The processing of sensitive data.

20 **2. Required elements.** Data protection assessments conducted pursuant to subsection
21 1 must identify and weigh the benefits that may flow, directly and indirectly, from the
22 processing to the controller, the consumer, other stakeholders and the public against the
23 potential risks to the rights of the consumer associated with the processing, as mitigated by
24 safeguards that can be employed by the controller to reduce the risks. The controller shall
25 factor into the data protection assessment the use of de-identified data and the reasonable
26 expectations of consumers, as well as the context of the processing and the relationship
27 between the controller and the consumer whose personal data will be processed.

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

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

40 **5. Reciprocity.** If a controller conducts a data protection assessment for the purpose
41 of complying with another applicable law or regulation, the data protection assessment
42 satisfies the requirements established in this section if the data protection assessment is

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

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

5 **§9609. De-identified and pseudonymous data**

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

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

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

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

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

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

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

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

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

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

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

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

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

40 **§9610. Controller and processor; duties and obligations**

ROS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 B. Effectuate a product recall;

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

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

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

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

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

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

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

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

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

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

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

41 B. Adequate, relevant and limited to what is reasonably necessary in relation to the
42 specific purposes listed in this section. Personal data collected, used or retained

1 pursuant to subsection 2 must, when applicable, take into account the nature and
2 purpose of the collection, use or retention. The data must be subject to reasonable
3 administrative, technical and physical measures to protect the confidentiality, integrity
4 and accessibility of the personal data and to reduce reasonably foreseeable risks of
5 harm to consumers relating to the collection, use or retention of personal data.

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

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

12 **§9611. Enforcement**

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

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

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

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

33 **§9612. Maine Privacy Fund established**

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

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

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

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

C. Interest earned on fund balances; and

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

Amend the bill by striking out all of section 3 and inserting the following:

'Sec. 3. Report. By February 1, 2027, the Attorney General shall submit a report to the joint standing committee of the Legislature having jurisdiction over judiciary matters regarding the operation and implementation of the Maine Revised Statutes, Title 10, chapter 1057. The report must include, at a minimum, the following information:

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

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

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

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

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

Sec. 4. Appropriations and allocations. The following appropriations and allocations are made.

ATTORNEY GENERAL, DEPARTMENT OF THE

Administration - Attorney General 0310

Initiative: Provides funding for one Assistant Attorney General position, one Paralegal position, one Technician position and related costs to administer and enforce the Maine Consumer Data Privacy Act.

GENERAL FUND	2025-26	2026-27
POSITIONS - LEGISLATIVE COUNT	0.000	3.000
Personal Services	\$0	\$420,508
All Other	\$0	\$20,000
GENERAL FUND TOTAL	\$0	\$440,508

Maine Privacy Fund N496

Initiative: Provides funding to establish the Maine Privacy Fund to support staff and activities required to enforce the Maine Consumer Data Privacy Act.

OTHER SPECIAL REVENUE FUNDS	2025-26	2026-27
All Other	\$0	\$500

1	OTHER SPECIAL REVENUE FUNDS TOTAL	\$0	\$500
2			
3	ATTORNEY GENERAL, DEPARTMENT OF THE		
4	DEPARTMENT TOTALS	2025-26	2026-27
5			
6	GENERAL FUND	\$0	\$440,508
7	OTHER SPECIAL REVENUE FUNDS	\$0	\$500
8			
9	DEPARTMENT TOTAL - ALL FUNDS	\$0	\$441,008

11 Amend the bill by relettering or renumbering any nonconsecutive Part letter or section
12 number to read consecutively.

13 SUMMARY

14 This amendment, which is a minority report of the committee, replaces the bill.

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

29 A consumer has the right, under the Act, to confirm whether a controller is processing
30 the consumer's personal data; to require the controller to correct inaccuracies in or delete
31 the consumer's personal data; to obtain a copy of the consumer's personal data; and to opt
32 out of the processing of the consumer's personal data for purposes of targeted advertising,
33 sale or profiling in furtherance of decisions about the consumer's access to financial or
34 lending services, housing, insurance, education, criminal justice, employment
35 opportunities, health care services and essential goods and services. The privacy notice
36 must describe how a consumer may exercise these rights. The controller must obtain the
37 affirmative, informed consent of a consumer before processing the consumer's sensitive
38 data, including data revealing the consumer's race or ethnic origins, religious beliefs,
39 medical history or mental or physical health conditions or diagnoses, sexual orientation or
40 citizenship or immigration status; genetic or biometric data; precise geolocation data; data
41 of a known child who has not attained 13 years of age; social security, driver's license or
42 nondriver identification card number; information that permits access to a consumer's
43 financial account; or data concerning the consumer's status as the victim of a crime. If the
44 controller knows that the consumer has not attained 13 years of age, the controller may not

1 process the consumer's data for any purpose without parental consent. If the controller
2 knows or willfully disregards that the consumer is at least 13 years of age but has not
3 attained 16 years of age, the controller may not process the consumer's data for targeted
4 advertising and must obtain the consumer's consent before processing the consumer's data
5 for sale.

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

19 The provisions of the Act do not apply to specifically enumerated persons, including
20 the State, political subdivisions of the State and federally recognized Indian tribes in the
21 State; financial institutions or their affiliates subject to the federal Gramm-Leach-Bliley
22 Act; state-licensed and authorized insurers; covered entities and business associates subject
23 to the federal Health Insurance Portability and Accountability Act of 1996; motor vehicle
24 dealer franchisees; nonprofits that do not receive any revenue from the sale of personal data
25 or that detect and prevent fraudulent insurance acts; and persons that both processed the
26 personal data of fewer than 25,000 consumers in the preceding calendar year and derived
27 no more than 25% of gross revenue from the sale of personal data. The Act also does not
28 apply to persons that controlled or processed the personal data for purposes other than
29 completing payment transactions of fewer than 100,000 consumers in the preceding
30 calendar year, except that, beginning January 1, 2028, this exception applies only to persons
31 that controlled or processed the personal data for purposes other than completing payment
32 transactions of fewer than 50,000 consumers in the preceding calendar year.

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

ROS

1 safety of consumers and preventing or responding to security incidents; and conducting
2 internal product research, effectuating a product recall or performing other internal
3 operations aligned with the expectations of a consumer.

4 Violations of the Act may be enforced exclusively by the Attorney General under the
5 Maine Unfair Trade Practices Act. The Attorney General is required to provide a potential
6 defendant with at least 30 days' notice prior to initiating an enforcement action, during
7 which time the potential defendant may cure any violation alleged in the notice. Any civil
8 penalties, attorney's fees or costs awarded to the State for a violation of the Act must be
9 deposited in the Maine Privacy Fund, which is established to provide funding for the
10 enforcement staff and activities of the Department of the Attorney General. The Act further
11 requires the Attorney General to submit a report by February 1, 2027 to the joint standing
12 committee of the Legislature having jurisdiction over judiciary matters regarding the
13 operation and implementation of the Act. The committee may report out legislation related
14 to the report to the 133rd Legislature in 2027.

15 The amendment also repeals the current law governing the privacy of broadband
16 Internet access service customer personal information because broadband Internet access
17 service providers are subject to the provisions of the Act.

18 **FISCAL NOTE REQUIRED**

19 (See attached)

**132nd MAINE LEGISLATURE****LD 1088****LR 2064(03)****An Act to Enact the Maine Consumer Data Privacy Act****Fiscal Note for Bill as Amended by Committee Amendment " "****Committee: Judiciary****Fiscal Note Required: Yes**

Fiscal Note

	FY 2025-26	FY 2026-27	Projections FY 2027-28	Projections FY 2028-29
Net Cost (Savings)				
General Fund	\$0	\$440,508	\$457,416	\$489,920
Appropriations/Allocations				
General Fund	\$0	\$440,508	\$457,416	\$489,920
Other Special Revenue Funds	\$0	\$500	\$500	\$500

Correctional and Judicial Impact Statements

This bill may increase the number of civil suits filed in the court system. The additional workload associated with the minimal number of new cases filed in the court system does not require additional funding at this time. The collection of additional filing fees will increase General Fund revenue by minor amounts.

Fiscal Detail and Notes

The bill includes a General Fund appropriation to the Office of the Attorney General of \$440,508 in fiscal year 2026-27 for one Assistant Attorney General position, one Paralegal position, one Technician position and related costs to administer and enforce the Maine Consumer Data Privacy Act.

The bill establishes the Maine Privacy Fund with a base Other Special Revenue Funds allocation of \$500 beginning in fiscal year 2026-27.

ROS
COPY

Report C
(Lee)

L.D. 1088

2

Date:

(Filing No. H-)

3

JUDICIARY

4

Reproduced and distributed under the direction of the Clerk of the House.

5

STATE OF MAINE

6

HOUSE OF REPRESENTATIVES

7

132ND LEGISLATURE

8

FIRST SPECIAL SESSION

9

COMMITTEE AMENDMENT “ ” to H.P. 710, L.D. 1088, “An Act to Enact the
Maine Consumer Data Privacy Act”

10

11

Amend the bill by striking out the title and substituting the following:

12

'An Act to Enact the Maine Online Data Privacy Act'

13

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

14

15

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

16

CHAPTER 1057

17

MAINE ONLINE DATA PRIVACY ACT

18

§9601. Short title

19

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

20

§9602. Definitions

21

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

22

23

1. Affiliate. "Affiliate" means a person that, directly or indirectly through one or more
intermediaries, controls, is controlled by or is under common control with another person,
such that the person:

24

25

26

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

27

28

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

29

30

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

COMMITTEE AMENDMENT

ROS

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

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

7 3. Biometric data. "Biometric data":

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

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

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

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

17 6. Collect. "Collect" means to purchase, rent, gather, obtain, receive, access or
18 otherwise acquire personal data.

19 7. Consent. "Consent":

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

25 B. Does not include:

26 (1) Acceptance of a general or broad terms of use document or similar document
27 that contains descriptions of personal data collection or processing along with other
28 unrelated information;

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

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

31 8. Consumer. "Consumer":

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

33 B. Does not include an individual acting in a commercial or employment context or an
34 individual acting as an employee, owner, director, officer or contractor of a company,
35 partnership, sole proprietorship, nonprofit organization or government entity whose
36 communications or transactions with a controller occur solely within the context of the
37 individual's role with the company, partnership, sole proprietorship, nonprofit
38 organization or government entity.

39 9. Consumer health data. "Consumer health data" means personal data that a
40 controller uses to identify a consumer's physical or mental health status, and includes, but

ROS

1 is not limited to, data related to gender-affirming health care services and reproductive
2 health care services.

3 **10. Control.** "Control" means:

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

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

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

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

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

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

16 **14. De-identified data.** "De-identified data" means data that does not identify, cannot
17 reasonably be used to infer information about and cannot otherwise be linked to an
18 identified or identifiable consumer, or a device that may be linked to an identified or
19 identifiable consumer, if the controller that possesses the data:

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

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

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

26 **15. Decisions that produce legal or similarly significant effects concerning the**
27 **consumer.** "Decisions that produce legal or similarly significant effects concerning the
28 consumer" means decisions that result in the provision or denial to the consumer of
29 financial or lending services; housing; insurance; education enrollment or opportunity;
30 criminal justice; employment opportunities; health care services; or access to essential
31 goods or services.

32 **16. Familial status.** "Familial status" has the same meaning as in Title 5, section
33 4553, subsection 5-A.

34 **17. Gender identity.** "Gender identity" has the same meaning as in Title 5, section
35 4553, subsection 5-C.

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

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

ROS

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

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

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

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

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

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

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

23 **24. Personal data.** "Personal data" means information that is linked or can be
24 reasonably linked to an identified or identifiable consumer or that is linked or reasonably
25 can be linked to a device that is linked or reasonably can be linked to an identified or
26 identifiable consumer. "Personal data" does not include de-identified data or publicly
27 available information.

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

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

31 A. Means information derived from technology that can precisely and accurately
32 identify the past or present specific location of a consumer within a radius of 1,750
33 feet. "Precise geolocation data" includes global positioning system level latitude and
34 longitude coordinates or data from other similar mechanisms; and

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

38 **27. Process.** "Process" means any operation or set of operations performed on
39 personal data or on sets of personal data by manual or automated means, including the use,
40 storage, disclosure, analysis, deletion or modification of personal data but not including the
41 collection of personal data.

ROS

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

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

7 30. Protected health information. "Protected health information" has the same
8 meaning as in HIPAA.

9 31. Publicly available information. "Publicly available information":

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

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

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

14 B. Does not include:

15 (1) Any obscene visual depiction as described in 18 United States Code, Section
16 1460;

17 (2) Biometric data;

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

20 (4) Any information that is collated or combined to create a consumer profile that
21 is made available to a user of a publicly available Internet website or mobile
22 application either for remuneration or free of charge;

23 (5) Any information that is made available for sale;

24 (6) Inferences derived from information described in subparagraph (4) or (5) or
25 inferences derived from a combination of publicly available information and other
26 personal data; or

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

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

34 33. Sale of personal data. "Sale of personal data":

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

37 B. Does not include:

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

ROS

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

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

(4) 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; or

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

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

(b) Did not restrict to a specific audience.

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

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

B. Genetic data or biometric data;

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

D. Precise geolocation data;

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

F. Account numbers, credit card numbers or debit card numbers, if circumstances exist wherein such numbers can be used without additional identifying information, access codes or passwords;

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

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

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

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

37. Targeted advertising. "Targeted advertising":

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

B. Does not include:

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

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

ROS

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

(4) Collecting or processing personal data solely to measure or report advertising frequency, performance or reach.

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

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

§9603. Applicability

1. Effective date. The requirements of this chapter take effect on September 1, 2026.

2. Persons affected. 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 35,000 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 10,000 consumers and derived more than 20% of gross revenue from the sale of personal data.

§9604. Exceptions

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

A. A body, authority, board, bureau, commission, district or agency of this State, a political subdivision of this State or a federally recognized Indian tribe in 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 supervised financial organization or a service corporation. For purposes of this paragraph, "supervised financial organization" has the same meaning as in Title 9-A, section 1-301, subsection 38-A and "service corporation" has the same meaning as in Title 9-B, section 131, subsection 37;

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

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

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

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

5 A. Nonpublic personal information regulated under and collected, processed, sold or
6 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,
7 15 United States Code, Section 6801 et seq. (1999);

8 B. Protected health information;

9 C. Patient-identifying information as described in 42 United States Code, Section
10 290dd-2;

11 D. Identifiable private information used for the purposes of the federal policy for the
12 protection of human subjects in research under 45 Code of Federal Regulations, Part
13 46;

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

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

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

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

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

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

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

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

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

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

7 O. Data collected, processed or maintained:

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

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

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

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

21 Q. Personal data collected and used pursuant to the federal Controlled Substances Act,
 22 21 United States Code, Section 830.

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

28 §9605. Consumer health data

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

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

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

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

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

1 **§9606. Consumer rights**

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

3 A. Confirm whether a controller is collecting or processing the consumer's personal
4 data;

5 B. If a controller collects or processes a consumer's personal data, access the
6 consumer's personal data;

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

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

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

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

19 G. Opt out of the collection and processing of the consumer's personal data for
20 purposes of:

21 (1) Targeted advertising;

22 (2) The sale of personal data; or

23 (3) Profiling in furtherance of any automated decision that produces any legal or
24 similarly significant effect concerning the consumer.

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

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

29 A. A controller shall establish a secure and reliable method pursuant to section 9608,
30 subsection 6 for a consumer to exercise a consumer right under this section.

31 B. A consumer may exercise a consumer right under this section, including through
32 another individual who has authority under subsection 4 to exercise the consumer's
33 rights, using the method established by the controller under paragraph A.

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

36 A. A consumer may designate an agent in accordance with section 9607 to exercise the
37 consumer's right under subsection 1, paragraph G to opt out of the collection and
38 processing of personal data.

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

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

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

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

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

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

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

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

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

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

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

25 (2) Decline to act on the request.

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

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

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

32 (2) Shall provide notice to the consumer that the controller is unable to authenticate
33 the request to exercise the right until the consumer or other person authorized to
34 exercise the consumer's rights provides additional information reasonably
35 necessary to authenticate the consumer and the consumer's request to exercise the
36 right.

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

39 F. A controller that has obtained personal data about a consumer from a source other
40 than the consumer is in compliance with a request to delete that data pursuant to

ROS.

subsection 1, paragraph D by retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data:

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

(2) Is not used for any other purpose.

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

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

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

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

§9607. Authorized agent

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

2. Method of designating agent. The consumer may designate an authorized agent by way of, among other methods, a technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating the consumer's intent to exercise the consumer's right under section 9606, subsection 1, paragraph G to opt out of the collection and processing of personal data.

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

A. The identity of the consumer; and

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

§9608. Actions of controllers

1. Prohibitions. A controller may not:

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

B. Sell sensitive data;

1 C. Collect or process personal data in violation of state or federal laws that prohibit
2 unlawful discrimination;

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

4 (1) Collect or process personal data of the consumer for the purpose of targeted
5 advertising; or

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

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

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

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

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

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

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

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

24 A. Limit the collection of personal data to what is reasonably necessary and
25 proportionate to provide or maintain a specific product or service requested by the
26 consumer to whom the data pertains, including any routine administrative, operational,
27 website or account-servicing activity that is consistent with the reasonable expectations
28 of the consumer under the circumstances. This paragraph does not prevent a controller
29 from processing personal data collected in accordance with this paragraph to provide
30 advertising to a consumer based on the consumer's activities within the controller's own
31 websites or online applications;

32 B. Establish, implement and maintain reasonable administrative, technical and physical
33 data security practices to protect the confidentiality, integrity and accessibility of
34 personal data appropriate to the volume and nature of the personal data at issue. These
35 processes must include the disposal of personal data in accordance with a retention
36 schedule that requires the disposal of personal data by the controller when the data is
37 required to be deleted by law or when the data is no longer necessary for the purpose
38 for which the data was processed unless the consumer has consented to the retention
39 of the data for a longer period of time or retention of the data is required by law. For
40 purposes of this paragraph, "disposal of personal data" means the destruction or
41 permanent deletion of the data or other modification of the data to make the data
42 unreadable and unrecoverable; and

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

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

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

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

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

16 A. The categories of personal data, including sensitive data, collected or processed by
17 the controller;

18 B. The controller's purpose for collecting and processing personal data;

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

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

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

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

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

32 **5. Notice of sale of personal data, targeted advertising or profiling; opt-out**
33 **mechanism.** If a controller sells personal data to 3rd parties, collects or processes personal
34 data for the purposes of targeted advertising or processes personal data for the purposes of
35 profiling the consumer in furtherance of decisions that produce legal or similarly significant
36 effects concerning the consumer, the controller shall clearly and conspicuously disclose the
37 sale, collection or processing, as well as the manner in which a consumer may exercise the
38 right to opt out of the sale, collection or processing. The disclosure required under this
39 subsection must be prominently displayed on the controller's publicly accessible website
40 and the language used must be clear, easy to understand and unambiguous.

41 **6. Method for exercising consumer rights.** A controller shall establish, and shall
42 describe in the privacy notice as required by subsection 4, paragraph C, one or more secure

1 and reliable mechanisms for a consumer to submit a request to exercise each consumer
2 right under this chapter.

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

5 (1) The ways in which consumers normally interact with the controller;

6 (2) The need for secure and reliable communication of consumer requests; and

7 (3) The ability of the controller to verify the identity of a consumer making the
8 request.

9 B. A controller may not require a consumer to create a new account to exercise a
10 consumer right. A controller may require a consumer to use an existing account to
11 exercise a consumer right.

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

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

20 (2) No later than September 1, 2026, allowing a consumer to opt out of any
21 collection or processing of the consumer's personal data for the purposes of
22 targeted advertising or any sale of personal data through an opt-out preference
23 signal sent, with the consumer's consent, by a platform, technology or mechanism
24 to the controller indicating the consumer's intent to opt out of the collection,
25 processing or sale as described in section 9607, subsection 2. The platform,
26 technology or mechanism:

27 (a) Must be consumer-friendly and easy to use by the average consumer;

28 (b) Must use clear, easy to understand and unambiguous language;

29 (c) Must be as consistent as possible with any other similar platform,
30 technology or mechanism required by federal or state law, rule or regulation;

31 (d) Must enable the controller to reasonably determine whether the consumer
32 is a resident of the State, which reasonable determination may be based on the
33 location associated with the consumer's Internet protocol address, and whether
34 the consumer has made a legitimate request to opt out of any such collection,
35 processing or sale of the consumer's personal data;

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

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

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

ROS

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

§9609. Responsibilities of processors and controllers

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

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

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

B. The contract must 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) Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data, considering the volume and nature of the personal data;
- (3) Stop processing personal data on request by the controller made in accordance with a consumer's authenticated request;
- (4) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of service, unless retention of the personal data is required by law;
- (5) On the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this chapter;
- (6) Engage any subcontractor to assist with processing personal data on the controller's behalf only in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data under the processor's contract with the controller;
- (7) Allow and cooperate with reasonable assessments by the controller, the controller's designated assessor or a qualified and independent assessor arranged for by the processor to assess the processor's policies and technical and

organizational measures in support of the obligations under this chapter. An assessment conducted under this subparagraph must be conducted using an appropriate and accepted control standard framework and assessment procedure; and

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

2. Processor responsibilities. A processor shall:

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

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

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

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

C. Provide necessary information to enable the controller to conduct and document data protection assessments as required by section 9610.

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

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

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

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

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

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

C. If a processor or 3rd party begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under section 9613.

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

1 **§9610. Data protection assessments**

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

4 A. The collection or processing of personal data for the purposes of targeted
5 advertising;

6 B. The sale of personal data;

7 C. The collection or processing of sensitive data; and

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

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

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

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

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

16 (5) Other substantial injury to a consumer.

17 **2. Data protection assessments required.** A controller shall conduct and document
18 a data protection assessment for each of the controller's collection or processing activities
19 that present a heightened risk of harm to a consumer. A single data protection assessment
20 may address a comparable set of collection or processing operations that include similar
21 activities.

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

24 A. The data protection assessment must identify and weigh the benefits that may flow
25 directly and indirectly from the collection or processing to the controller, the consumer,
26 other interested parties and the public against:

27 (1) The potential risks to the rights of the consumer associated with the collection
28 or processing as mitigated by safeguards that may be employed by the controller
29 to reduce these risks; and

30 (2) The necessity and proportionality of collection or processing in relation to the
31 stated purpose of the collection or processing.

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

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

34 (2) The reasonable expectations of consumers;

35 (3) The context of the collection or processing; and

36 (4) The relationship between the controller and the consumer whose personal data
37 will be collected or processed.

38 **4. Disclosure to Attorney General.** The Attorney General may require that a
39 controller disclose to the Attorney General a data protection assessment that is relevant to

1 an investigation conducted by the Attorney General. The Attorney General may evaluate
2 the data protection assessment for compliance with the responsibilities set forth in this
3 chapter.

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

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

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

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

19 B. Within 6 months of making a material change to any collection or processing
20 activity that presents a heightened risk of harm to a consumer.

21 **8. Application.** The requirement to conduct a data protection assessment under this
22 section applies only to collection or processing activities that occur on or after September
23 1, 2026.

24 **§9611. De-identified data**

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

27 A. Re-identify de-identified data;

28 B. Maintain data in an identifiable form; or

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

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

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

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

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

1 **3. Contractual oversight.** A controller that discloses de-identified data shall exercise
2 reasonable oversight to monitor compliance with contractual commitments to which the
3 de-identified data is subject and shall take appropriate steps to address breaches of those
4 contractual commitments. Whether oversight is reasonable and whether steps taken to
5 address breaches of contractual commitments are appropriate depends in part on whether
6 the disclosed de-identified data would be considered sensitive data if the data were re-
7 identified.

8 **§9612. Exemptions**

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

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

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

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

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

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

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

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

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

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

31 J. Preserve the integrity or security of systems;

32 K. Assist another controller or processor or a 3rd party with an obligation under this
33 chapter; or

34 L. Transfer assets to a 3rd party in the context of a merger, acquisition, bankruptcy or
35 similar transaction when the 3rd party assumes control, in whole or in part, of the
36 controller's assets, but only if the controller, in a reasonable time prior to the transfer,
37 provides an affected consumer with:

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

41 (2) A reasonable opportunity to:

- 1 (a) Withdraw any previous consent related to the consumer's personal data; and
2 (b) Request deletion of the consumer's personal data.

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

6 A. Effectuate a product recall;

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

8 C. Perform internal operations that:

9 (1) Are reasonably aligned with the expectations of the consumer or can be
10 reasonably anticipated based on the consumer's existing relationship with the
11 controller; or

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

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

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

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

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

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

32 B. A 3rd-party controller or processor that receives personal data from a controller or
33 processor in compliance with this chapter is not in violation of this chapter for the
34 independent misconduct of the controller or processor from which the 3rd-party
35 controller or processor received the personal data.

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

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

1 B. Apply to an individual's collection or processing of personal data in the course of
2 the individual's purely personal or household activities.

3 **6. Burden of proof.** If a controller collects or processes personal data pursuant to an
4 exemption in this section, the controller bears the burden of demonstrating that the
5 collection or processing qualifies for the exemption and complies with the limitations in
6 subsection 7.

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

10 A. Subject to reasonable administrative, technical and physical measures to protect the
11 confidentiality, integrity and accessibility of the personal data and reduce reasonably
12 foreseeable risks of harm to consumers relating to the collection, use or retention of
13 personal data;

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

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

17 **8. Collecting or processing personal data pursuant to an exemption.** A person that
18 collects or processes personal data pursuant to an exemption in this section may not be
19 considered a controller solely based on that collection or processing of personal data.

20 **§9613. Enforcement**

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

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

36 A. The number of alleged violations;

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

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

40 D. The likelihood of injury to the public;

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

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

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

§9614. Report

By February 1, 2027 and annually thereafter, the Attorney General shall submit a report to the joint standing committee of the Legislature having jurisdiction over judiciary matters regarding the implementation and operation of this chapter. The report must include, at a minimum, the following information:

1. Number of notices. The number of notices the Attorney General has issued under section 9613, subsection 2 and the nature of the violations alleged in the notices;

2. Number of persons sent a notice. The number of persons sent a notice described in subsection 1 that conferred with the Attorney General during the notice period described in section 9613, subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair Trade Practices Act;

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

4. Recommendations. Any recommendations the Attorney General has for improving the operation of this chapter.

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

Sec. 2. Appropriations and allocations. The following appropriations and allocations are made.

ATTORNEY GENERAL, DEPARTMENT OF THE

Administration - Attorney General 0310

Initiative: Provides funding for one Assistant Attorney General position; one Paralegal position, one Technician position and related costs to administer and enforce the Maine Online Data Privacy Act.

GENERAL FUND	2025-26	2026-27
POSITIONS - LEGISLATIVE COUNT	0.000	3.000
Personal Services	\$0	\$420,508
All Other	\$0	\$20,000
GENERAL FUND TOTAL	\$0	\$440,508

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

Amend the bill by relettering or renumbering any nonconsecutive Part letter or section number to read consecutively.

SUMMARY

This amendment, which is a minority report of the committee, strikes the bill and changes the title. The amendment enacts the Maine Online Data Privacy Act, which takes effect September 1, 2026. The Act regulates the collection, use, processing, disclosure,

1 sale and deletion of nonpublicly available personal data by a person that conducts business
2 in this State or that produces products or services targeted to residents of this State, referred
3 to in the Act as a "controller," if the personal data is linked or can be reasonably linked to
4 an identified or identifiable individual who is a resident of this State, referred to in the Act
5 as a "consumer," or is linked or reasonably can be linked to a device that is linked or
6 reasonably can be linked to an identified or identifiable consumer. Under the Act, a
7 controller must limit the collection and processing of personal data to what is reasonably
8 necessary and proportionate to provide or maintain a specific product or service requested
9 by the consumer, including the collection of personal data to provide advertising to the
10 consumer based on the consumer's activities within the controller's own websites or online
11 applications. The controller must also limit the collection and processing of certain
12 sensitive data to what is strictly necessary to provide or maintain a specific product or
13 service requested by the consumer. Under the Act, "sensitive data" includes data revealing
14 a consumer's race or ethnic origins, religious beliefs, mental or physical health conditions
15 or diagnoses, sexual orientation, gender identity, citizenship or immigration status; genetic
16 or biometric data; precise geolocation data; social security, driver's license or nondriver
17 identification card numbers; specific financial information; data of a minor under 18 years
18 of age; or data concerning the consumer's status as the victim of a crime.

19 The Act establishes that consumers have the right to confirm whether a controller is
20 processing their data; correct inaccuracies in their personal data; require the controller to
21 delete any portion of their personal data that the controller is not required to maintain by
22 law; obtain a copy of their personal data in a format that can be readily transferred to
23 another controller; obtain a list of the 3rd parties to which the controller has sold personal
24 data; and opt out of the processing of their personal data for purposes of targeted
25 advertising, sale or consumer profiling. The Act also prohibits a controller from selling
26 any sensitive data; processing the personal data of a minor for purposes of targeted
27 advertising or sale; processing personal data in a manner that discriminates against a person
28 in violation of state or federal law; and retaliating against a consumer for exercising a
29 consumer's rights under the Act, except that a controller may offer different prices or
30 selection of goods in connection with a consumer's voluntary participation in a bona fide
31 loyalty or discount program.

32 The Act also requires a controller to provide consumers with a privacy notice
33 specifying how a consumer may exercise the consumer's rights under the Act; the
34 categories of personal data processed by the controller; the purposes for processing the
35 personal data; the categories of personal data transferred to 3rd parties; and the categories
36 of 3rd parties to whom personal data is shared. The controller must establish, implement
37 and maintain reasonable data security practices and a retention schedule that requires the
38 disposal of personal data by the controller either when deletion is required by law or when
39 the data is no longer necessary for the purpose for which it was processed and retention of
40 the data is not required by law. The controller must also require, by contract, that any
41 person who processes a consumer's personal data on behalf of the controller treats the
42 personal data confidentially and deletes or returns all personal data to the controller at the
43 end of the processing, unless retention of the data is required by law. If a controller engages
44 in a data processing activity that presents a heightened risk of harm to a consumer,
45 including processing any data for targeted advertising, sale or profiling or any processing
46 of sensitive data, the controller must conduct and document a data protection assessment
47 identifying and weighing the benefits and potential risks of the processing activity. The

1 controller may be required to disclose the data protection assessment to the Attorney
2 General, who must keep it confidential, when the assessment is relevant to an investigation
3 conducted by the Attorney General.

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

8 The provisions of the Act do not apply to specifically enumerated persons, including
9 the State, political subdivisions of the State and federally recognized Indian tribes in the
10 State; nonprofit organizations; institutions of higher education; federally registered national
11 securities associations; supervised financial organizations and service corporations; health
12 care facilities and health care practitioners as well as their affiliates that both qualify as
13 business associates and provide services only to covered entities; state-licensed and
14 authorized insurers that are in compliance with applicable Maine laws governing insurer
15 data security and data privacy; and broadband Internet service providers to the extent those
16 providers are subject to the data privacy requirements of the Maine Revised Statutes, Title
17 35-A, section 9301. In addition, the provisions of the Act do not apply to specifically
18 enumerated types of data, including, for example: nonpublic personal information
19 regulated under the federal Gramm-Leach-Bliley Act; protected health information under
20 the federal Health Insurance Portability and Accountability Act of 1996; personal data
21 regulated by the Family Educational Rights and Privacy Act of 1974; personal data
22 collected and used pursuant to the federal Controlled Substances Act; data processed and
23 maintained by the controller regarding an applicant for employment or employee to the
24 extent the data is collected and used within the context of that role; and data necessary for
25 the controller to administer benefits.

26 The Act also does not prohibit controllers from engaging in specifically enumerated
27 activities, including, for example: complying with state or federal law; complying with
28 investigations or subpoenas from federal, state or tribal governmental authorities;
29 cooperating with federal, tribal or Maine law enforcement agencies; providing a product or
30 service specifically requested by the consumer; protecting life and physical safety of
31 consumers; preventing or responding to security incidents; and transferring data as part of
32 a merger, acquisition or bankruptcy as long as the consumer is given advance notice and a
33 reasonable opportunity to request deletion of the consumer's personal data. The Act also
34 does not prohibit a controller from using personal data collected in a lawful manner to
35 effectuate a product recall, identify and repair technical errors and perform internal
36 operations that are reasonably aligned with a consumer's expectations or otherwise
37 compatible with providing the product or service specifically requested by the consumer.

38 Violations of the Act may be enforced exclusively by the Attorney General under the
39 Maine Unfair Trade Practices Act. If the violation occurs on or before April 1, 2027, the
40 Attorney General may provide a potential defendant with a notice of violation at least 60
41 days prior to initiating an enforcement action, during which time the potential defendant
42 may cure the violation to avoid the enforcement action. The amendment further requires
43 the Attorney General to submit a report by February 1, 2027, and annually thereafter, to
44 the joint standing committee of the Legislature having jurisdiction over judiciary matters

ROS
COMMITTEE AMENDMENT “ ” to H.P. 710, L.D. 1088

1 regarding the implementation and operation of the Act. The committee may report out
2 legislation related to the report to the 133rd Legislature in 2027.

3 **FISCAL NOTE REQUIRED**

4 (See attached)

**132nd MAINE LEGISLATURE****LD 1088****LR 2064(02)****An Act to Enact the Maine Consumer Data Privacy Act****Fiscal Note for Bill as Amended by Committee Amendment " "****Committee: Judiciary****Fiscal Note Required: Yes**

Fiscal Note

	FY 2025-26	FY 2026-27	Projections FY 2027-28	Projections FY 2028-29
Net Cost (Savings)				
General Fund	\$0	\$440,508	\$457,416	\$489,920
Appropriations/Allocations				
General Fund	\$0	\$440,508	\$457,416	\$489,920

Correctional and Judicial Impact Statements

This bill may increase the number of civil suits filed in the court system. The additional workload associated with the minimal number of new cases filed in the court system does not require additional funding at this time. The collection of additional filing fees will increase General Fund revenue by minor amounts.

Fiscal Detail and Notes

The bill includes a General Fund appropriation to the Office of the Attorney General of \$440,508 in fiscal year 2026-27 for one Assistant Attorney General position, one Paralegal position, one Technician position and related costs to administer and enforce the Maine Online Data Privacy Act.

L.D. or
Confirmation LD 1088 CONSUMER DATA PRIVACY

Date WEDNESDAY 14 MAY 2025

Motion tabled

Motion by Sen. Carney

Seconded by Rep. Sato

Revised on Monday, January 6, 2025

121088 CONSUMERS TRADING
WILSONS PT. MAI 2002
- 10/10/02
JUNIOR. NO. 2
P.O. 240

X

X

2

X

X
X
X
X
X
X
X
X

X
X

11

(Grozniy 45) 1000000000 8800 00
2000 1000 00 0000
0000 0000 0000
0000 0000 0000



10

XXXX

•

- JUNE 1 - reconsidered
on 4 June

DIVIDED
REPORT

JUDICIARY
COMMITTEE VOTING SHEET

L.D. or Confirmation LD 1088 DATA PRIVACY (Henderson)

Date Friday 30 May 2025

Motion OUTP

Motion by Rep. Henderson

for Seconded by Rep. Sato

Those Voting in Favor of the Motion	Recommendation of those opposed to the Motion				Absent	Abstain
	OT-P-A					

Senator Carney (Chair)	X							
Rep. Kuhn (Chair)	X							
Senator Haggan	X <i>DP</i>							
Rep. Poirier	X <i>JP</i>							
Rep. O'Halloran	X							
Rep. Henderson	X							
Rep. Pugh	X <i>DP</i>							
Rep. Sinclair	X							
Senator Talbot Ross	X							
Rep. Lee		X						
Rep. Sato	X							
Rep. Dana						X		
Rep. Caruso		X <i>EMC</i>						
Rep. Babin		X <i>MR</i>						
TOTALS	(10)	(3)				(1)		

RECEIVED
JAN 10 1988

1-10-88

TO: DIRECTOR, FBI
FROM: SAC, NEW YORK (100-100000)
SUBJECT: [REDACTED]
RE: [REDACTED]

100-100000
1-10-88

A-910

X

X

X

X

X

100-100000

1-10-88

100-100000

JUDICIARY COMMITTEE VOTING SHEET

L.D. or Confirmation LD 1088 Privacy

Date Wednesday 4 June 2025

Motion Reconsider

Motion by Rep. Henderson

Seconded by Rep. Pugh

9

Those Voting in Favor of the Motion	Recommendation of those opposed to the Motion					Absent	Abstain

Senator Carney (Chair)	X								
Rep. Kuhn (Chair)	X								
Senator Haggan						X			
Rep. Poirier						X			
Rep. O'Halloran						X			
Rep. Henderson	X								
Rep. Pugh	X								
Rep. Sinclair	X								
Senator Talbot Ross	X								
Rep. Lee	X								
Rep. Sato	X								
Rep. Dana						X			
Rep. Caruso	X								
Rep. Babin	X								
TOTALS	10					4			

- final -

DIVIDED
REPORT

JUDICIARY COMMITTEE VOTING SHEET

L.D. or Confirmation LD 1088 PRIVACY (Henderson)
Date WEDNESDAY 4 June 2025
Motion OTP-A
Motion by Rep. Henderson
Seconded by Rep. CARUSO

Those
Voting in
Favor of
the Motion

Recommendation of those opposed to
the
Motion

OTP LEE
OTP-A

Absent

Abstain

Senator Carney (Chair)		X							
Rep. Kuhn (Chair)		X							
Senator Haggan	X								
Rep. Poirier	X								
Rep. O'Halloran		X							
Rep. Henderson	X								
Rep. Pugh		X							
Rep. Sinclair		X							
Senator Talbot Ross		X							
Rep. Lee			X						
Rep. Sato		X							
Rep. Dana								X	
Rep. Caruso	X								
Rep. Babin	X								
TOTALS	(5)	(7)	(1)					(1)	

COMMITTEE VOTING TALLY SHEET

LD # or Confirmation: LD 1088

Committee: Judiciary

Date: 06/04/2025

Motion: Ought To Pass As Amended

Motion by: Rep. Henderson

Seconded by: Rep. Caruso

Those Voting in Favor of the Motion	Recommendation of those opposed to the Motion					Absent	Abstain
	ONT P	OT P-AM Lee					

Senators

Sen. Carney		X					
Sen. D. Haggan	X						
Sen. Talbot Ross		X					

Representatives

Rep. Kuhn		X					
Rep. Babin	X						
Rep. Caruso	X						
Rep. Dana						X	
Rep. Henderson	X						
Rep. Lee		X					
Rep. O'Halloran		X					
Rep. Poirier	X						
Rep. Pugh		X					
Rep. Sato		X					
Rep. Sinclair		X					

REPORT A

HOUSE REPORT

THE COMMITTEE ON Judiciary

to which was referred the following:

An Act to Enact the Maine Consumer Data Privacy Act

H.P. 710

L.D. 1088

has had the same under consideration, and asks leave to report that the same
 OUGHT NOT TO PASS

(Signature)

of
For the Committee

SEN. CARNEY of Cumberland

SEN. TALBOT ROSS of Cumberland

REP. KUHN of Falmouth

REP. O'HALLORAN of Brewer

REP. PUGH of Portland

REP. SATO of Gorham

REP. SINCLAIR of Bath

(Type)

Rep. of (Town) and/or Sen. of (County)

(Signatures)

HOUSE REPORT

REPORT B

to which was referred the following:

H.P. 710

L.D. 1088

has had the same under consideration, and asks leave to report that the same
 OUGHT TO PASS AS AMENDED BY COMMITTEE AMENDMENT " "

of
For the Committee

REP. BABIN of Fort Fairfield

REP. CARUSO of Caratunk

REP. HENDERSON of Rumford

REP. POIRIER of Skowhegan

(Type)

Rep. of (Town) and/or Sen. of (County)

(Signatures)

Printed on recycled paper

REPORT C

HOUSE REPORT

THE COMMITTEE ON Judiciary

to which was referred the following:

An Act to Enact the Maine Consumer Data Privacy Act

H.P. 710

L.D. 1088

has had the same under consideration, and asks leave to report that the same
 OUGHT TO PASS AS AMENDED BY COMMITTEE AMENDMENT " " "

(Signature)

of
For the Committee

REP. LEE of Auburn

(Type)

Rep. of (Town) and/or Sen. of (County)

(Signatures)

HOUSE REPORT

Printed on recycled paper