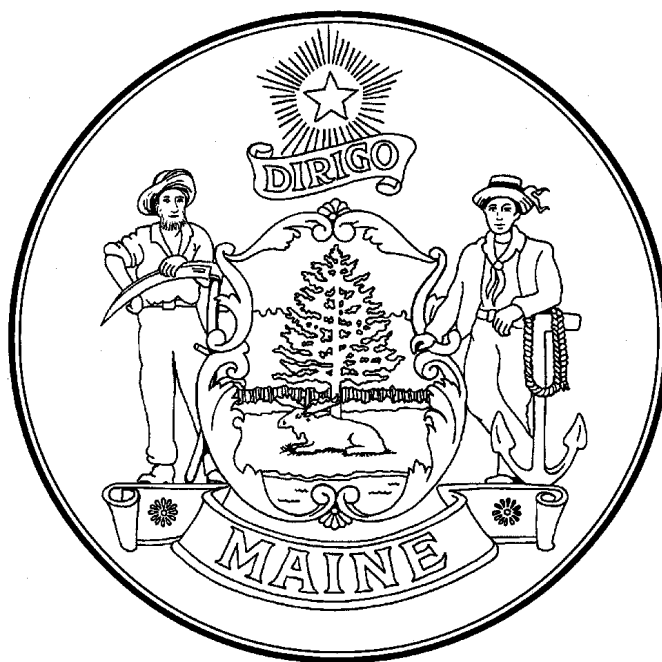


MAINE STATE LEGISLATURE

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)

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 <i>LD 1088</i> § 9604 p. 8 § 9609 (3,4) p. 15-16 <i>LD 1224</i> § 9604 p. 7-8 § 9609 (3,4) p. 14 <i>LD 1822</i> § 9606 p. 9-10 § 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 opt the consumer out of processing that personal data</u>	❖ 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 — <u>unless the controller is required by law to retain the personal data</u> • <u>When processing is by automatic means</u>, obtain a portable copy of own personal data from a controller; if technically feasible, in a way that can be transmitted to another controller • <u>Obtain a list of 3rd parties to which controller sold the consumer's personal data (or anyone's personal data)</u> <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. 8-9 • 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, <u>technically infeasible</u> 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> § 9606(5) p. 11 <u>LD 1224</u> § 9606(5) p. 10 <u>LD 1822</u> § 9608(4) p. 13	❖ 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 ^{§ 9608(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 ^{§ 9608(1)(A) p.12}
Consent requirements <u>LD 1088</u> § 9606(1-3) p.10-11 § 9604(1)(E) p.8 <u>LD 1224</u> § 9606(1-3) p.9-10 § 9604(1)(E) p.7-8 <u>LD 1822</u> § 9608(1-2) p.12-13 § 9606(1)(9) p.9	❖ 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 — <u>as a matter of law, sale of sensitive data is not “reasonably necessary [or] compatible”</u> - 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. ❖ 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	❖ 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. ❖ 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	❖ 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” ❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person <u>not known to be <18</u>) - For targeted advertising - For sale (<i>same exceptions to “sale” as in LD 1088 & 1224</i>) - 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) <i>p. 8</i> - 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) <i>p. 7</i> - 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) <i>p. 8</i> - 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 <i>§ 9606(7) p. 12</i> ❖ Opt-Out mechanism / requirements: <i>§ 9605 p. 9-10</i> 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) - 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 <i>§ 9606(7) p. 11</i> ❖ Opt-Out mechanism / requirements: <i>§ 9605 p. 9</i> 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) - 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 <i>§ 9605(5) p. 13-14</i> ❖ Opt-Out mechanism / requirements: <i>§ 9607 p. 11-12</i> 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) - Must be secure and reliable and may not require new account. <i>§ 9608(6) p. 14</i> 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
	<i>§ 9606 (6-8) p. 12-13</i>	<i>§ 9606 (6-8) p. 10-11</i>	<i>§ 9608 (6)(c)(2) p. 14-15</i>

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 <u>LD 1088</u> § 9606(3)(D)+(L) p. 11 <u>LD 1224</u> § 9606(3)(D)+(L) p. 10 <u>LD 1822</u> § 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)(B) 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)(B) 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 - Except: 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 <u>who enters the virtual perimeter</u> <u>Exception:</u> § 9606 p. 16 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 <u>Exception:</u> § 9605(3) p. 9 Facility operator's geofence (ex: to check in patients)
Data Security and Retention § 9606(2)(B) 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)(A) 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)(A) 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 ❖ Controller must establish and implement a data retention schedule requiring <u>destruction or permanent deletion</u> of data when retention of the data is "no longer necessary" for the <u>processing purpose</u> — <u>unless consumer consents</u> to longer time or controller is required to retain the personal data longer by law § 9608(2)(B) 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 <u>not</u>: §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 <u>not</u>: §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 <u>conduct</u> independent assessments of its own services ○ <u>After giving controller opportunity to object to use of subcontractor</u>, require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract ○ <u>Establish and implement reasonable data security practices for data confidentiality and integrity</u> ○ <u>Stop processing data on request of controller in response to consumer's authenticated request</u> ❖ Processor may <u>not</u>: §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	❖ <u>Third party that receives personal data must</u>: §9610 p.17 • <u>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</u>
Duties involving de-identified data	❖ <u>Controller in possession of de-identified data must</u>: • <u>Take reasonable measures to prevent re-identifying data</u> • <u>Publicly commit to not attempting to re-identify data</u> • <u>Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations</u> §9609(1) p.15	❖ <u>Controller in possession of de-identified data must</u>: • <u>Take reasonable measures to prevent re-identifying data</u> • <u>Publicly commit to not attempting to re-identify data</u> • <u>Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations</u> §9609(1) p.13-14	❖ <u>Controller in possession of de-identified data must</u>: • <u>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</u> §9612 p.19
Additional Consumer health data Requirements	n/a	n/a	❖ <u>Person may not provide employee or contractor with access to consumer health data unless</u>: • <u>Employer or contractor is subject to contractual or statutory duty of confidentiality; or</u> • <u>Confidentiality is a condition of employment</u> ❖ <u>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</u>

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	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 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 ≥<u>35,000</u> Maine residents (except solely for purposes of payment transactions) <u>or</u> - Of ≥<u>10,000</u> Maine residents and derived ><u>20%</u> 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 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	
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 <u>Health care information defined in 22 M.R.S. §1711-C</u> 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, <u>any state</u> or local laws - Complying with investigations, subpoenas or summonses by federal, <u>any state</u> or tribal authorities - Cooperating with federal, <u>state</u> or tribal law enforcement concerning conduct the entity believes in good faith may violate federal or <u>state</u> 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 <u>or local</u> laws or rules - Complying with investigations, subpoenas or summonses by federal, Maine or tribal authorities - Cooperating with federal, Maine or tribal law enforce. concerning conduct the entity believes in good faith may violate federal, Maine <u>or local</u> 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 <i>LD 1088</i> <i>§ 9612 p.18-19</i> <i>LD 1224</i> <i>§ 9611 p.17</i> <i>LD 1822</i> <i>§ 9614 p.21-22</i>	❖ 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 — <u>unless show facts in affidavit demonstrating immediate irreparable harm to consumers in the State if notice is given</u> ❖ 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: §9611(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 and (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)

Majority

ROS

1
COPY 2

L.D. 1822

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. 1220, L.D. 1822, “An Act to Enact the
10 Maine Online Data Privacy Act”

11 Amend the bill in section 1 in c. 1057 in §9601 in the first indented paragraph in the
12 first line (page 1, line 6 in L.D.) by striking out the following: “Data Privacy and Protection”
13 and inserting the following: ‘Online Data Privacy’

14 Amend the bill in section 1 in c. 1057 in §9602 in subsection 7 in paragraph A in the
15 2nd line (page 2, line 2 in L.D.) by inserting after the following: “the” the following:
16 ‘collection or’

17 Amend the bill in section 1 in c. 1057 in §9602 in subsection 7 in paragraph B in
18 subparagraph (1) in the 2nd line (page 2, line 7 in L.D.) by inserting after the following:
19 “data” the following: ‘collection or’

20 Amend the bill in section 1 in c. 1057 in §9602 in subsection 11 in the last line (page
21 2, line 30 in L.D.) by inserting after the following: “of” the following: ‘collecting or’

22 Amend the bill in section 1 in c. 1057 in §9602 by striking out all of subsection 14
23 (page 2, lines 36 to 41 and page 3, lines 1 to 4 in L.D.) and inserting the following:

24 ‘14. De-identified data. “De-identified data” means data that does not identify, cannot
25 reasonably be used to infer information about and cannot otherwise be linked to an
26 identified or identifiable consumer, or a device that may be linked to an identified or
27 identifiable consumer, if the controller that possesses the data:

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

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

32 C. Contractually obligates recipients of the data to satisfy the criteria and commitments
33 in paragraphs A and B.’

ROS

1 Amend the bill in section 1 in c. 1057 in §9602 in subsection 26 in paragraph A in the
2 2nd line (page 4, line 10 in L.D.) by striking out the following: "specific location of a
3 Consumer" and inserting the following: 'past or present specific location of a consumer'

4 Amend the bill in section 1 in c. 1057 in §9602 in subsection 27 in the last line (page
5 4, line 18 in L.D.) by inserting after the following: "data" the following: 'but not including
6 the collection of personal data'

7 Amend the bill in section 1 in c. 1057 in §9602 by striking out all of subsection 31
8 (page 4, lines 27 to 39 and page 5, lines 1 to 7 in L.D.) and inserting the following:

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 Amend the bill in section 1 in c. 1057 in §9602 in subsection 33 in paragraph B in
33 subparagraph (4) in the last line (page 5, line 22 in L.D.) by inserting after the following:
34 "party;" the following: 'or'

35 Amend the bill in section 1 in c. 1057 in §9602 in subsection 33 in paragraph B in
36 subparagraph (5) in division (b) in the first line (page 5, line 25 in L.D.) by striking out the
37 following: "audience; or" and inserting the following: 'audience.'

38 Amend the bill in section 1 in c. 1057 in §9602 in subsection 33 in paragraph B by
39 striking out all of subparagraph (6) (page 5, lines 26 to 28 in L.D.).

ROS.

1 Amend the bill in section 1 in c. 1057 in §9602 in subsection 34 by striking out all of
2 paragraph F (page 5, lines 38 and 39 in L.D.) and inserting the following:

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

6 Amend the bill in section 1 in c. 1057 in §9602 in subsection 37 in paragraph B in
7 subparagraph (4) in the first line (page 6, line 21 in L.D.) by striking out the following:
8 "Processing" and inserting the following: 'Collecting or processing'

9 Amend the bill in section 1 in c. 1057 in §9603 in subsection 1 in the first line (page 6,
10 line 28 in L.D.) by striking out the following: "July" and inserting the following:
11 'September'

12 Amend the bill in section 1 in c. 1057 in §9604 in subsection 2 in paragraph O in the
13 first line (page 8, line 26 in L.D.) by inserting after the following: "Data" the following:
14 'collected.'

15 Amend the bill in section 1 in c. 1057 in §9604 in subsection 2 in paragraph O in
16 subparagraph (3) in the last line (page 8, line 34 in L.D.) by striking out the following: "or"

17 Amend the bill in section 1 in c. 1057 in §9604 in subsection 2 in paragraph P in the
18 last line (page 8, line 39 in L.D.) by striking out the following: "41713." and inserting the
19 following: '41713; or'

20 Amend the bill in section 1 in c. 1057 in §9604 in subsection 2 by inserting after
21 paragraph P the following:

22 'Q. Personal data collected and used pursuant to the federal Controlled Substances Act,
23 21 United States Code, Section 830.'

24 Amend the bill in section 1 in c. 1057 in §9606 by striking out all of subsection 1 (page
25 9, lines 19 to 39 in L.D.) and inserting the following:

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

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

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

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

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

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

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

ROS.

1 to which the controller has sold the personal data of the specific consumer, obtain a list
2 of the 3rd parties to which the controller has sold any consumer's personal data; and

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

5 (1) Targeted advertising;

6 (2) The sale of personal data; or

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

9 Amend the bill in section 1 in c. 1057 in §9606 by striking out all of subsection 3 (page
10 10, lines 3 to 8 in L.D.) and inserting the following:

11 '3. Exercise of consumer rights. This subsection governs the exercise of the
12 consumer rights established in subsection 1.

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

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

18 Amend the bill in section 1 in c. 1057 in §9606 in subsection 4 in paragraph A in the
19 2nd line (page 10, line 12 in L.D.) by inserting after the following: "the" the following:
20 'collection and'

21 Amend the bill in section 1 in c. 1057 by striking out all of §9607 (page 11, lines 34 to
22 42 and page 12, lines 1 to 6 in L.D.) and inserting the following:

23 '§9607. Authorized agent

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

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

33 3. Authentication of agent's opt-out request. A controller shall comply with a
34 request received from an authorized agent to exercise the consumer's right under section
35 9606, subsection 1, paragraph G to opt out of the collection and processing of personal data
36 if, using commercially reasonable efforts, the controller is able to authenticate:

37 A. The identity of the consumer; and

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

39 Amend the bill in section 1 in c. 1057 in §9608 in subsection 1 in paragraph C in the
40 first line (page 12, line 13 in L.D.) by striking out the following: "Process" and inserting
41 the following: 'Collect or process'

ROS

1 Amend the bill in section 1 in c. 1057 in §9608 in subsection 1 in paragraph D in
2 subparagraph (1) in the first line (page 12, line 16 in L.D.) by striking out the following:
3 "Process" and inserting the following: 'Collect or process'

4 Amend the bill in section 1 in c. 1057 in §9608 in subsection 2 in paragraph A in the
5 last line (page 12, line 38 in L.D.) by inserting after the following: "pertains" the following:
6 'including any routine administrative, operational, website or account-servicing activity
7 that is consistent with the reasonable expectations of the consumer under the circumstances.
8 This paragraph does not prevent a controller from processing personal data collected in
9 accordance with this paragraph to provide advertising to a consumer based on the
10 consumer's activities within the controller's own websites or online applications'

11 Amend the bill in section 1 in c. 1057 in §9608 in subsection 4 in paragraph A in the
12 first line (page 13, line 25 in L.D.) by inserting after the following: "sensitive data," the
13 following: 'collected or'

14 Amend the bill in section 1 in c. 1057 in §9608 in subsection 4 in paragraph B in the
15 first line (page 13, line 27 in L.D.) by inserting after the following: "for" the following:
16 'collecting and'

17 Amend the bill in section 1 in c. 1057 in §9608 by striking out all of subsection 5 (page
18 13, lines 41 and 42 and page 14, lines 1 to 7 in L.D.) and inserting the following:

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

28 Amend the bill in section 1 in c. 1057 in §9608 in subsection 6 by striking out all of
29 paragraph C (page 14, lines 21 to 41 and page 15, lines 1 to 8 in L.D.) and inserting the
30 following:

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

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

39 (2) No later than September 1, 2026, allowing a consumer to opt out of any
40 collection or processing of the consumer's personal data for the purposes of
41 targeted advertising or any sale of personal data through an opt-out preference
42 signal sent, with the consumer's consent, by a platform, technology or mechanism
43 to the controller indicating the consumer's intent to opt out of the collection,

1 processing or sale as described in section 9607, subsection 2. The platform,
2 technology or mechanism:

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

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

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

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

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

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

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

18 Amend the bill in section 1 in c. 1057 in §9608 in subsection 6 in paragraph D in the
19 first line (page 15, line 9 in L.D.) by inserting after the following: "any" the following:
20 'collection or'

21 Amend the bill in section 1 in c. 1057 in §9609 in subsection 1 in paragraph B in
22 subparagraph (6) in the first line (page 16, line 4 in L.D.) by striking out the following:
23 "After providing the controller an opportunity to object, engage a" and inserting the
24 following: 'Engage any'

25 Amend the bill in section 1 in c. 1057 in §9609 in subsection 2 in paragraph C in the
26 last line (page 16, line 31 in L.D.) by striking out the following: "9611" and inserting the
27 following: '9610'

28 Amend the bill in section 1 in c. 1057 in §9609 in subsection 4 in paragraph C in the
29 last line (page 17, line 8 in L.D.) by striking out the following: "9614" and inserting the
30 following: '9613'

31 Amend the bill in section 1 in c. 1057 by striking out all of §9610 (page 17, lines 12 to
32 20 in L.D.).

33 Amend the bill in section 1 in c. 1057 in §9611 in subsection 1 in paragraph A in the
34 first line (page 17, line 24 in L.D.) by inserting after the following: "The" the following:
35 'collection or'

36 Amend the bill in section 1 in c. 1057 in §9611 in subsection 1 in paragraph C in the
37 first line (page 17, line 26 in L.D.) by inserting after the following: "The" the following:
38 'collection or'

39 Amend the bill in section 1 in c. 1057 in §9611 by striking out all of subsection 2 (page
40 17, lines 36 to 40 in L.D.) and inserting the following:

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

6 Amend the bill in section 1 in c. 1057 in §9611 by striking out all of subsection 3 (page
7 18, lines 1 to 16 in L.D.) and inserting the following:

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

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

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

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

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

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

20 (2) The reasonable expectations of consumers;

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

22 (4) The relationship between the controller and the consumer whose personal data
23 will be collected or processed.'

24 Amend the bill in section 1 in c. 1057 in §9611 by striking out all of subsection 7 (page
25 18, lines 33 to 38 in L.D.) and inserting the following:

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

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

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

32 Amend the bill in section 1 in c. 1057 in §9611 by striking out all of subsection 8 (page
33 18, lines 39 and 40 in L.D.) and inserting the following:

34 **'8. Application.** The requirement to conduct a data protection assessment under this
35 section applies only to collection or processing activities that occur on or after September
36 1, 2026.'

37 Amend the bill in section 1 in c. 1057 in §9613 in subsection 1 in paragraph J in the
38 first line (page 20, line 7 in L.D.) by striking out the following: "; or" and inserting the
39 following: ';

1 Amend the bill in section 1 in c. 1057 in §9613 in subsection 1 in paragraph K in the
2 last line (page 20, line 9 in L.D.) by striking out the following: "." and inserting the
3 following: "; or"

4 Amend the bill in section 1 in c. 1057 in §9613 in subsection 1 by inserting after
5 paragraph K the following:

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

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

13 (2) A reasonable opportunity to:

14 (a) Withdraw any previous consent related to the consumer's personal data;
15 and

16 (b) Request deletion of the consumer's personal data.'

17 Amend the bill in section 1 in c. 1057 in §9613 in subsection 5 in paragraph B in the
18 first line (page 21, line 7 in L.D.) by inserting after the following: "an individual's" the
19 following: "collection or"

20 Amend the bill in section 1 in c. 1057 in §9613 by striking out all of subsection 6 (page
21 21, lines 9 to 11 in L.D.) and inserting the following:

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

26 Amend the bill in section 1 in c. 1057 in §9613 by striking out all of subsection 7 (page
27 21, lines 12 to 20 in L.D.) and inserting the following:

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

31 A. Subject to reasonable administrative, technical and physical measures to protect the
32 confidentiality, integrity and accessibility of the personal data and reduce reasonably
33 foreseeable risks of harm to consumers relating to the collection, use or retention of
34 personal data;

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

36 C. Adequate, relevant and limited to what is necessary in relation to the specific
37 purposes listed in this section.'

38 Amend the bill in section 1 in c. 1057 in §9613 by striking out all of subsection 8 (page
39 21, lines 21 to 23 in L.D.) and inserting the following:

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

Amend the bill in section 1 in c. 1057 in §9614 in subsection 2 in paragraph C in the first line (page 21, line 42 in L.D.) by inserting after the following: "processor's" the following: 'collection or'

Amend the bill in section 1 in c. 1057 by inserting after §9614 the following:

'§9615. 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.'

Amend the bill in section 1 in chapter 1057 by renumbering the sections to read consecutively.

Amend the bill by striking out all of sections 2 and 3 and inserting the following:

'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

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 0
- 1

SUMMARY

1. It changes the effective date of the Maine Online Data Privacy Act from July 1, 2026 to September 1, 2026.

3. It amends the definition of "publicly available information" to exclude any information used to create a consumer profile, any information made available for sale and inferences derived from these types of information.

5. It provides that the Act does not prohibit the transfer of personal data as part of the transfer of assets to a 3rd party in the context of a merger, acquisition or bankruptcy as long as the controller provides an affected consumer with a notice describing the transfer, including the name of the entity acquiring the personal data and the entity's privacy policies as well as a reasonable opportunity for the consumer to withdraw any previous consent related to the consumer's personal data and to request deletion of the consumer's personal data.

7. It provides that, although a controller must limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer, such services include routine administrative, operational, website or account-servicing activities that are consistent with the reasonable expectations of the consumer under the circumstances, including collection of the consumer's personal data to provide advertising to the consumer based on the consumer's activities within the controller's own websites or online applications.

9. It removes the provision of the bill requiring 3rd parties to provide specific notices to consumers.

ROS

COMMITTEE AMENDMENT “ ” to H.P. 1220, L.D. 1822

1 10. It removes the requirement that controllers conduct data protection assessments for
2 each algorithm used on personal data.

3 11. Unlike the bill, which requires only a single report on February 1, 2027, it requires
4 the Attorney General to submit, beginning February 1, 2027, an annual report to the joint
5 standing committee of the Legislature having jurisdiction over judiciary matters regarding
6 the implementing and operation of the Act.

7 **FISCAL NOTE REQUIRED**
8 **(See attached)**

**132nd MAINE LEGISLATURE****LD 1822****LR 14(02)****An Act to Enact the Maine Online 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 Consumer Privacy Act.

ROS

COPY

Minority
(03)

L.D. 1822

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. 1220, L.D. 1822, “An Act to Enact the
Maine Online Data Privacy Act”

10

11

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

12

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

13

14

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

15

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

16

CHAPTER 1057

17

MAINE CONSUMER DATA PRIVACY ACT

18

§9601. Short title

19

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

24

25

26

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:

27

28

29

30

A. A digital or physical photograph;

- 1 B. An audio or video recording;
- 2 C. Any data generated from a digital or physical photograph or an audio or video
- 3 recording, unless the data is generated to identify a specific individual; or
- 4 D. Data collected, used or stored for health care treatment, payment or operations under
- 5 the federal Health Insurance Portability and Accountability Act of 1996, 42 United
- 6 States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and
- 7 exemptions adopted pursuant to that Act.
- 8 **3. Business associate.** "Business associate" has the same meaning as in 45 Code of
- 9 Federal Regulations, Section 160.103.
- 10 **4. Child.** "Child" means an individual who has not attained 13 years of age.
- 11 **5. Consent.** "Consent" means a clear affirmative act signifying a consumer's freely
- 12 given, specific, informed and unambiguous agreement to allow the processing of personal
- 13 data relating to the consumer. "Consent" may include a written statement, including by
- 14 electronic means, that is made in the language the consumer uses to obtain a product or
- 15 service from the controller and in a format that is reasonably accessible to and usable by
- 16 consumers with disabilities. "Consent" does not include:
- 17 A. Acceptance of a terms of use document or similar document that contains
- 18 descriptions of personal data processing along with other unrelated information;
- 19 B. Hovering over, muting, pausing or closing a given piece of content; or
- 20 C. Agreement obtained through the use of a dark pattern.
- 21 **6. Consumer.** "Consumer" means an individual who is a resident of this State.
- 22 "Consumer" does not include an individual acting in a commercial or employment context
- 23 or as an employee, owner, director, officer or contractor of a company, partnership, sole
- 24 proprietorship, nonprofit organization or government agency whose communications or
- 25 transactions with the controller occur solely within the context of that individual's role with
- 26 the company, partnership, sole proprietorship, nonprofit organization or government
- 27 agency.
- 28 **7. Control.** "Control" means:
- 29 A. Ownership of, or the power to vote, more than 50% of the outstanding shares of
- 30 any class of voting security of a company;
- 31 B. Control in any manner over the election of a majority of the directors of a company
- 32 or of individuals exercising similar functions in a company; or
- 33 C. Power to exercise controlling influence over the management of a company.
- 34 **8. Controller.** "Controller" means a person that, alone or jointly with other persons,
- 35 determines the purpose and means of processing personal data.
- 36 **9. COPPA.** "COPPA" means the federal Children's Online Privacy Protection Act of
- 37 1998, 15 United States Code, Section 6501 et seq. and the regulations, rules, guidance and
- 38 exemptions adopted pursuant to that Act, as that Act and such regulations, rules, guidance
- 39 and exemptions may be amended from time to time.
- 40 **10. Covered entity.** "Covered entity" has the same meaning as in 45 Code of Federal
- 41 Regulations, Section 160.103.

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

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

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

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

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

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

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

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

30 **16. Personal data.** "Personal data" means information that is linked or reasonably
31 linkable to an identified or identifiable consumer or that is linked or reasonably linkable to
32 a device that is linked or reasonably linkable to an identified or identifiable consumer.
33 "Personal data" does not include de-identified data or publicly available information.

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

39 A. The content of communications; or

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

ROS

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

4 19. Processor. "Processor" means a person that processes personal data on behalf of
5 a controller.

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

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

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

19 23. Publicly available information. "Publicly available information" means
20 information that:

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

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

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

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

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

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

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

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

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

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

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

1 **25. Sensitive data.** "Sensitive data" means personal data that includes:

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

5 B. Genetic or biometric data;

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

7 D. Precise geolocation data;

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

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

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

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

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

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

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

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

30 **27. Trade secret.** "Trade secret" has the same meaning as in section 1542, subsection
31 4.

32 **§9603. Scope**

33 **1. Applicability; July 1, 2026 to December 31, 2027.** From July 1, 2026 to December
34 31, 2027, the provisions of this chapter apply to persons that conduct business in this State
35 or persons that produce products or services that are targeted to residents of this State and
36 that during the preceding calendar year:

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

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

ROS

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

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

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

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

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

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

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

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

20 E. A covered entity or business associate;

21 F. A nonprofit organization that:

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

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

25 G. A person or entity that is a motor vehicle dealer franchisee as described in section
26 1171, subsection 7.

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

28 A. Nonpublic personal information regulated under and collected, processed, sold or
29 disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act,
30 15 United States Code, Section 6801 et seq. (1999), as amended;

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

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

36 D. Patient-identifying information as described in 42 United States Code, Section
37 290dd-2;

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

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

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

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

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

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

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

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

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

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

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

40 P. Data processed or maintained:

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

ROS

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

(3) That is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under 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

ROS.

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

ROS

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.

ROS

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

ROS

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;

ROS

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.

Sec. 2. 35-A MRSA c. 94, as amended, is repealed.

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

10 **Sec. 5. Effective date.** This Act takes effect July 1, 2026.'

11 Amend the bill by relettering or renumbering any nonconsecutive Part letter or section

12 number to read consecutively.

14 This amendment, which is the minority report of the committee, replaces the bill and
15 changes the title.

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

ROS

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

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

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

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

ROS

1 a product or service specifically requested by the consumer; protecting life and physical
2 safety of consumers and preventing or responding to security incidents; and conducting
3 internal product research, effectuating a product recall or performing other internal
4 operations aligned with the expectations of a consumer.

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

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

19 **FISCAL NOTE REQUIRED**

20 (See attached)

**132nd MAINE LEGISLATURE****LD 1822****LR 14(03)****An Act to Enact the Maine Online 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 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.

**L.D. or
Confirmation**

UD 1822 Online Data Privacy Act

Date _____

Wednesday 14 May 2025

Motion

tabled

Motion by

Sen. CARNEY

Seconded by

Rep Sato

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	11					3	

JUDICIARY COMMITTEE VOTING SHEET

L.D. or Confirmation LD 1822 DATA PRIVACY (REP. KUHN)

Date KLIDY 23 MAY 2025

Motion tabled

Motion by Sen. Carney

Seconded by Rep. Sato

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 1822 DATA PRIVACY (Kuhn)
Date Friday 30 May 2025
Motion OTP-A
Motion by Rep Kuhn
Seconded by Sen. Talbot Ross

Those Voting in Favor of the Motion	Recommendation of those opposed to the Motion				Absent	Abstain
	<u>OTP-A</u>	<u>MB</u>				

Senator Carney (Chair)	<u>X</u>							
Rep. Kuhn (Chair)	<u>X</u>							
Senator Haggan		<u>X</u>						
Rep. Poirier			<u>JPX</u>					
Rep. O'Halloran	<u>X</u>							
Rep. Henderson		<u>X</u>						
Rep. Pugh	<u>X</u>							
Rep. Sinclair	<u>X</u>							
Senator Talbot Ross	<u>X</u>							
Rep. Lee	<u>X</u>							
Rep. Sato	<u>X</u>							
Rep. Dana						<u>X</u>		
Rep. Caruso		<u>X</u>	<u>MB</u>					
Rep. Babin		<u>X</u>	<u>MB</u>					
TOTALS	<u>(8)</u>	<u>(4)</u>	<u>(1)</u>			<u>(1)</u>		

COMMITTEE VOTING TALLY SHEET

LD # or Confirmation: LD 1822

Committee: Judiciary

Date: 05/30/2025

Motion: Ought To Pass As Amended

Motion by: Rep. Kuhn

Seconded by: Sen. Talbot Ross

Those Voting in Favor of the Motion	Recommendation of those opposed to the Motion					Absent	Abstain
	OTP-AM Haggan				ONTP		

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

to which was referred the following:

H.P. 1220

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

(Signature)	
SEN. CARNEY of Cumberland	
SEN. TALBOT ROSS of Cumberland	
REP. KUHN of Falmouth	
REP. LEE of Auburn	
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)

Printed on recycled paper

