

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)

Revised for WS 5/23/25

Marked up to show 1822-Sponsor's proposed Amend.

§ 9602 (34) p. 5

Revised

is amend.

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), LD 1224 (Henderson), LD 1822 (Kuhn)			
	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Protected Data	❖ "Personal data": § 9602 (17) p. 3 - Data linked or reasonably linkable to an identifiable individual (a "consumer") who is a Maine resident Excludes: "Publicly available information" (excludes biometric data, genetic data not revealed to the general public by the consumer; inferences from a combination of publicly available information and personal data; obscene visual depictions or intimate images created or shared without consent); and "de-identified data" § 9602 (24) p. 3-4	❖ "Personal data": § 9602 (16) p. 3 - Data linked or reasonably linkable to an identifiable individual (a "consumer") who is a Maine resident Excludes: "Publicly available information" (defined in a way that does not exclude the categories of information excluded in LD 1088 and LD 1822 as described in left hand column of this table), and § 9602 (23) p. 3-4 "de-identified data" § 9602 (13) p. 2	❖ "Personal data": § 9602 (24) p. 4 - Data linked or reasonably linkable to (a) an identifiable individual (a "consumer") who is a Maine resident or (b) a device linked or reasonably linked to a consumer Excludes: - Definition adjusted in sponsor's amend "Publicly available information" (defined differently than LD 1088 but excludes all of the same categories of information excluded in LD 1088 as described in the left-hand column of this table); and § 9602 (31) p. 4-5 "de-identified data" § 9602 (14) p. 2
	❖ "Sensitive data": subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions/diagnoses; sexual orientation; citizenship or immigration status - Genetic or "biometric data" (defined on as certain data "capable of being used" to ID a specific individual) - Consumer health data (reveals condition or diagnosis) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Social security, driver's license or nondriver ID number (except last 4 digits of these numbers) - Account number, log-in info, or credit or debit card number that, in combination with a security code or password, permits access to a financial account - Data concerning individual's status as a crime victim	❖ "Sensitive data": subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, medical history, mental or physical health conditions or diagnoses by a medical professional; sexual orientation; citizenship or immigration status - The processing of genetic or "biometric data" to uniquely ID an individual ("biometric data" defined as certain data "used" to ID a specific individual) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Data concerning individual's status as a crime victim	❖ "Sensitive data": subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs; sexual activity; sexual orientation; gender identity; national origin; citizenship or immigration status "Genetic" / "biometric data" (biometric: defined as data that "can be used" to uniquely identify an individual) - Consumer health data (used to ID physical or mental health status, e.g., gender-affirming or reproductive care) - Personal data of a person the controller knows or should know is a minor (<18) - Precise geolocation data (within 1,750 feet) - Social security, driver's license or nondriver ID number (including the last 4 digits of these numbers); - Billing, financial or payment method information (Except last 4 digits of credit card or similar number) - Account or device log-in, security codes or passwords - Data concerning consumer's status as a crime victim
	❖ Exception (both types of data above): § 9602 (26) p. 5 "Consumer" is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ Exception (both types of data above): § 9602 (25) p. 4 "Consumer" is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ Exception (both types of data above): § 9602 (25) p. 2 "Consumer" is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context
Who is regulated?	❖ Controller: § 9602 (26) p. 2 person that alone or jointly with others determines purpose and means of processing personal data ❖ Processor: § 9602 (26) p. 3 person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller	❖ Controller: § 9602 (25) p. 2 person that alone or jointly with others determines purpose and means of processing personal data ❖ Processor: § 9602 (25) p. 3 person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller	❖ Controller: § 9602 (24) p. 2 person that alone or jointly with others determines purpose and means of processing personal data ❖ Processor: § 9602 (24) p. 4 person that processes (uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller

Prepared by Office of Policy and Legal Analysis (J.Stocco) (for Work Session May 14, 2025)

Page 1 of 12

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

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Consumer Rights LD 1088 § 9604 p 8 § 9609 (3-4) p 15-16 LD 1224 § 9604 p 7-8 § 9609 (3-4) p 14 LD 1822 § 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 Exceptions: • 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 — unless the controller is required by law to retain the personal data • When processing is by automatic means, obtain a portable copy of own personal data from a controller; if technically feasible, in a way that can be transmitted to another controller • Obtain a list of 3rd parties to which controller sold the consumer's personal data (or anyone's personal data) Exceptions: • 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	❖ A consumer (or parent if child <13, guardian or conservator) has a right, upon making an authenticated request, to: • Confirm whether controller processes personal data • Access own personal data processed by controller • Correct inaccuracies in own personal data • Delete personal data about the consumer — unless the controller is required by law to retain the personal data • When processing is by automatic means, obtain a portable copy of own personal data from a controller; if technically feasible, in a way that can be transmitted to another controller • Obtain a list of 3rd parties to which controller sold the consumer's personal data (or anyone's personal data) Exceptions: • 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 except 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 except 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 except controller may charge a reasonable fee or decline a manifestly unfounded, excessive, technically infeasible or repetitive requests • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must respond without undue delay and within 45 days of request (may extend once for 45 days) • If declines a request, must do so within 45 days, giving a justification and info. on how to appeal the decision

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), 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 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 LD 1088 § 9606(5) p. 11 LD 1224 § 9606(5) p. 10 LD 1822 § 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 (of 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 <u>or on a device identified by a unique identifier</u> 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 <u>that are unaffiliated with each other</u> 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) <u>Processing</u> 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), LD 1224 (Kuhn) 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. 4 “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
Consent requirements	❖ Prohibited activities (regardless of consent) • Process personal data of a minor known (or willfully disregarded) to be 13-15 for targeted advertising • Process data of a known child <13 years old in violation of federal COPPA law/regulation requirements ❖ Activities permitted only with consent (opt-in) • Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose — as a matter of law, sale of sensitive data is not “reasonably necessary, or compatible” • Process sensitive data for any purpose (this consent requires disclosure of specific processing purpose, categories of sensitive data to be processed, and identity of any 3rd parties to whom the data is sold. If there is no contact for 24 months, customer must opt-in again). • Sell personal data of a minor known (or willfully disregarded) to be age 13-15 Exceptions: “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction.	❖ Prohibited activities (regardless of consent) • Process personal data of a minor known (or willfully disregarded) to be 13-15 for targeted advertising • Process data of a known child <13 years old in violation of federal COPPA law/regulation requirements ❖ Activities permitted only with consent (opt-in) • Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose • Process sensitive data for any purpose • Sell personal data of a minor known (or willfully disregarded) to be age 13-15 Exceptions: “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction.	❖ Prohibited activities (regardless of consent) • Sell any consumer’s sensitive data (includes personal data of known (reasonably should know) minor (<18)) • Process personal data of a known (reasonably should know) 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 not known to be <16) • For targeted advertising • For sale (see exceptions to “sale” above) • For profiling in furtherance of automated decisions producing legal or similarly significant effects	❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <16) • For targeted advertising • For sale (see exceptions to “sale” above) • For profiling in furtherance of automated decisions producing legal or similarly significant effects	❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <18) • For targeted advertising • For sale (same exceptions to “sale” as in LD 1088 & 1224) • For profiling in furtherance of automated decisions producing legal or similarly significant effects

Revised to include “collecting”

LD 1822 prohibited activities

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

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

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

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Retaliation prohibition LD 1088 (3)(d) + (4) p. 11 LD 1224 (3)(d) + (4) p. 12 LD 1822 (3)(d) + (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 Exceptions: • 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 Exceptions: • 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 Exceptions: • 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: • Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers	❖ Controller may not: • Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers § 9606(3)(b) p. 10 revised to include "collect"	❖ Controller may not: • 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 diversity applicant pool. Does not apply to a private club exempt from Title II of the Civil Rights Act. § 9608 (1)(c), (f) p. 12
Geofence prohibition	❖ Person may not use geofence (1,750 foot virtual perimeter) around health care facility for purpose of identifying, tracking, collecting data from or sending notices regarding consumer health data to a consumer who enters the virtual perimeter § 9606 p. 16 Exception: • 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 to a consumer § 9605(3) p. 9 Exception: • 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)(c) p. 10	❖ Controller must establish and implement reasonable data security practices to protect confidentiality, accessibility and integrity of data appropriate to the volume and nature of data No data retention schedule required § 9606(2)(4) p. 9	❖ 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 destruction or permanent deletion of data when retention of the data is "no longer necessary" for the processing purpose — unless consumer consents to longer time or controller is required to retain the personal data longer by law § 9608 (2)(b) p. 12-13

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), LD 1222 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1222 (Kuhn)
Data Protection Assessments LD 1088 § 9608 p. 14-15 LD 1224 § 9608 p. 12-13 LD 1222 § 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: ^{§ 9609 removed in sponsor’s amend.} - Processing of sensitive data - Processing personal data for targeted advertising - Sale of personal data ^{§ 9609 revised to include “collecting”} - 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” <u>When required? Within 6 months of first engaging in the activity or of making a material change to that activity</u> 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), LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	o Delete or return personal data at end of processing activity, unless retention required by law o Give controller requested information to demonstrate processor's compliance with law o Cooperate with controller assessments or share independent assessments of its own services o 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)	o Delete or return personal data at end of processing activity, unless retention required by law o Give controller requested information to demonstrate processor's compliance with law o Cooperate with controller assessments or share independent assessments of its own services o 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)	o Delete or return personal data at end of processing activity, unless retention required by law o Give controller requested information to demonstrate processor's compliance with law o Cooperate with controller assessments or conduct independent assessments of its own services o After giving controller opportunity to object to use of subcontractor, require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract o Establish and implement reasonable data security practices for data confidentiality and integrity o Stop processing data on request of controller in response to consumer's authenticated request ❖ 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	❖ Third party that receives personal data must: § 9610 p. 17 Notify consumer if it intends to use or share the data in a manner inconsistent with disclosures made at the time the data was collected — with enough time to permit the consumer to exercise the consumer's rights
Duties involving de-identified data	❖ Controller in possession of de-identified data must: § 9609(4) p. 15 Take reasonable measures to prevent re-identifying data Publicly commit to not attempting to re-identify data Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations	❖ Controller in possession of de-identified data must: § 9609(4) p. 13-14 Take reasonable measures to prevent re-identifying data Publicly commit to not attempting to re-identify data Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations	❖ Controller in possession of de-identified data must: § 9612 p. 19 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 ❖ Person may not provide employee or contractor with access to consumer health data unless: Employer or contractor is subject to contractual or statutory duty of confidentiality; or Confidentiality is a condition of employment ❖ Person may not provide processor with access to consumer health data unless the person requires the processor to protect the data via the processing contract described above
Additional Consumer health data Requirements	n/a	n/a	

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

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
“Small business” exception LD 1088 § 9603(1-2) p 5-6 LD 1224 § 9603(1-2) p 5 LD 1822 § 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) or ◦ 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) or ◦ 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) or ◦ 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) or ◦ Of ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	Beginning July 1, 2026: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & Last calendar year, controlled/processed personal data: ◦ Of ≥35,000 Maine residents (except solely for purposes of payment transactions) or ◦ Of ≥10,000 Maine residents and derived >20% of gross revenue from the sale of personal data
Exempt entities LD 1088 § 9603(3) p 6 LD 1224 § 9603(3) p 5 LD 1822 § 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; • 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	❖ 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), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	• HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA • Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) • Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines • Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 • Info. created for purposes of or info. regulated by: ◦ Health Care Quality Improvement Act of 1986 ◦ Family Educational Rights and Privacy Act of 1974 ◦ Airline Deregulation Act of 1978 • Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: ◦ Fair Credit Reporting Act ◦ Driver’s Privacy Protection Act of 1994 ◦ Farm Credit Act of 1971 • Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives	• HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA • Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) • Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines • Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 • Health care information defined in 22 M.R.S. §171-C Info. created for purposes of or regulated by: ◦ Health Care Quality Improvement Act of 1986 ◦ Family Educational Rights and Privacy Act of 1974 ◦ Airline Deregulation Act of 1978 • Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: ◦ Fair Credit Reporting Act ◦ Driver’s Privacy Protection Act of 1994 ◦ Farm Credit Act of 1971 • Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives	• HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA • Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) • Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines • Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 • Info. created for purposes of or regulated by: ◦ Health Care Quality Improvement Act of 1986 ◦ Family Educational Rights and Privacy Act of 1974 ◦ Airline Deregulation Act of 1978 • Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: ◦ Fair Credit Reporting Act ◦ Driver’s Privacy Protection Act of 1994 ◦ Farm Credit Act of 1971 • Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives Subserved by Data collected & used for Controlled Act
Exempt activities LD 1088 §9611 (1-2) p. 16-17 LD 1224 §9610 (1-2) p. 14-15 LD 1822 §9613 (1-2) p. 19-20	❖ Controller / Processor activities not 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 not affected by LD 1224: • Complying with federal, any state or local laws • Complying with investigations, subpoenas or summonses by federal, any state or tribal authorities • Cooperating with federal, state or tribal law enforcement conduct the entity believes in good faith may violate federal or state laws or rules • Investigating, exercising or defending legal claims • Providing product or service requested by consumer, including performing contracted services (ex: warranty) • Taking requested steps prior to entering a contract • Taking immediate steps to protect the life or physical safety of a consumer or other individual	❖ Controller / Processor activities not affected by LD 1224: • Complying with federal, Maine or local laws or rules • Complying with investigations, subpoenas or summonses by federal, Maine or tribal authorities • Cooperating with federal, Maine or tribal law enforcement concerning conduct the entity believes in good faith may violate federal, Maine or local laws or rules • Investigating, exercising or defending legal claims • Providing product or service requested by consumer, including performing contracted services (ex: warranty) • Taking requested steps prior to entering a contract • Taking immediate steps to the life or physical safety of a consumer or other individual

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), 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>(which 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 <i>ⓧNew - transfer personal data to successor as a result of merger or bankruptcy only if provide advance notice to consumers & allow consumers to request their data & deleted</i>
Remedies for violations <i>LD 1088 § 9612 p.18-19</i> <i>LD 1224 § 9611 p.17</i> <i>LD 1822 § 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 — unless show facts in affidavit demonstrating immediate irreparable harm to consumers in the State if notice is given ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Must provide at least 30-days advance notice - AG may not bring action unless controller fails to cure an alleged violation listed in the notice within 30 days ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Until April 1, 2027, if AG believes it is possible for a controller or processor to cure a violation, may choose to give notice of the violation prior to initiating suit - If notice is given, AG may not bring action unless violation is not cured within 60 days - Factors regarding whether to give notice: number of violations, size and complexity of defendant nature and extent of defendant's processing activities, likelihood of injury to public, degree to which violations affect safety, whether the alleged violation was likely a human or technical error, and past violations by defendant of this or similar laws ❖ No private right of action ❖ AG rulemaking authority under UTPA to interpret law

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), 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.14	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	Does not repeal ISP law	n/a
Effective Date	July 1, 2026 p.20	July 1, 2026 p.18	(X) September 1, 2026 p.22 July 1, 2026
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)

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

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Protected Data	❖ “Personal data”: § 9602 (17) p. 3 - Data linked or reasonably linkable to an identifiable individual (a “consumer”) who is a Maine resident Excludes: “Publicly available information” (excludes biometric data, genetic data not revealed to the general public by the consumer; inferences from a combination of publicly available information and personal data; obscene visual depictions or intimate images created or shared without consent); and “de-identified data” § 9602 (15) p. 2 ❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions/diagnoses; sexual orientation; citizenship or immigration status - Genetic or “biometric data” (defined on as certain data “capable of being used” to ID a specific individual) - Consumer health data (reveals condition or diagnosis) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Social security, driver’s license or nondriver ID number (except last 4 digits of these numbers); - Account number, log-in info, or credit or debit card number that, in combination with a security code or password, permits access to a financial account - Data concerning individual’s status as a crime victim § 9602 (20) p. 5 ❖ Exception (both types of data above): p. 2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context ❖ Controller: person that alone or jointly with others p. 2 determines purpose and means of processing personal data ❖ Processor: person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p. 3	❖ “Personal data”: § 9602 (16) p. 3 - Data linked or reasonably linkable to an identifiable individual (a “consumer”) who is a Maine resident Excludes: “Publicly available information” (defined in a way that does not exclude the categories of information excluded in LD 1088 and LD 1822 as described in left-hand column of this table), and § 9602 (23) p. 3-4 “de-identified data” § 9602 (13) p. 2 ❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, medical history, mental or physical health conditions or diagnoses by a medical professional; sexual orientation; citizenship or immigration status - The processing of genetic or “biometric data” to uniquely ID an individual (“biometric data” defined as certain data “used” to ID a specific individual) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Data concerning individual’s status as a crime victim § 9602 (25) p. 4 ❖ Exception (both types of data above): p. 1-2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context ❖ Controller: person that alone or jointly with others p. 2 determines purpose and means of processing personal data ❖ Processor: person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p. 3	❖ “Personal data”: § 9602 (24) p. 4 - Data linked or reasonably linkable to (a) an identifiable individual (a “consumer”) who is a Maine resident or (b) a device linked or reasonably linked to a consumer Excludes: “Publicly available information” (defined differently than LD 1088 but excludes all of the same categories of information excluded in LD 1088 as described in the left-hand column of this table); and § 9602 (31) p. 4-5 “de-identified data” § 9602 (14) p. 2 ❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs; sexual activity; sexual orientation; gender identity; national origin, citizenship or immigration status “Genetic”/ “biometric data” (biometric: defined as data that “can be used” to uniquely identify an individual) - Consumer health data (used to ID physical or mental health status, e.g., gender-affirming or reproductive care) - Personal data of a person the controller knows or should know is a minor (<18) - Precise geolocation data (within 1,750 feet) - Social security, driver’s license or nondriver ID number (including the last 4 digits of these numbers); - Billing, financial or payment method information (Except last 4 digits of credit card or similar number) - Account or device log-in, security codes or passwords - Data concerning consumer’s status as a crime victim ❖ Exception (both types of data above): p. 2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context ❖ Controller: person that alone or jointly with others p. 2 determines purpose and means of processing personal data ❖ Processor: person that processes (uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p. 4
Who is regulated?			

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

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

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

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG	• Appeal: Consumer may appeal controller's inaction 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	❖ 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)
LD 1088 § 9606(5) p. 11			
LD 1224 § 9606(5) p. 10			
LD 1822 § 9608 (4) p. 13			
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), 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)(b) “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(2)(A)	
Consent requirements	LD 1088 § 9606(1-3) p. 10-11 § 9604(1)(E) p. 8 LD 1224 § 9606(1-3) p. 9-10 § 9604(1)(E) p. 7-8 LD 1822 § 9608(1-2) p. 12-13 § 9606(1)(c) 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 — as a matter of law, sale of sensitive data is not “reasonably necessary [or] compatible” • Process sensitive data for any purpose (this consent requires disclosure of specific processing purpose, categories of sensitive data to be processed, and identity of any 3rd parties to whom the data is sold. If there is no contact for 24 months, customer must opt-in again). • Sell personal data of a minor known (or willfully disregarded) to be age 13-15 Exceptions: “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction.	❖ Prohibited activities (regardless of consent) • Process personal data of a minor known (or willfully disregarded) to be 13-15 for targeted advertising • Process data of a known child <13 years old in violation of federal COPPA law/regulation requirements ❖ Activities permitted only with consent (opt-in) • Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose • Process sensitive data for any purpose • Sell personal data of a minor known (or willfully disregarded) to be age 13-15 Exceptions: “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction.	❖ Prohibited activities (regardless of consent) • Sell any consumer’s sensitive data (includes all personal data of known (should know) minor (<18)) • Process personal data of a person known (should know) to be a minor (<18) for targeted advertising ❖ Activities permitted only with consent (opt-in) • Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose • Retain personal data past the time “when it is no longer necessary for the purpose for which the data was processed”
	❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <16) • For targeted advertising • For sale (see exceptions to “sale” above) • For profiling in furtherance of automated decisions producing legal or similarly significant effects	❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <16) • For targeted advertising • For sale (see exceptions to “sale” above) • For profiling in furtherance of automated decisions producing legal or similarly significant effects	❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <18) • For targeted advertising • For sale (same exceptions to “sale” as in LD 1088 & 1224) • For profiling in furtherance of automated decisions producing legal or similarly significant effects	

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

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

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

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Retaliation prohibition § 9406(3)(d) + (4) p. 11 LD 1224 § 9406(3)(d) + (4) p. 10 LD 1822 § 9408(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 - sale of personal data may not be a program condition	❖ 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: Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers	❖ Controller may not: Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers	❖ Controller may not: - Process (use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers - Collect, process or disclose personal data or publicly available info. in a way that unlawfully discriminates or prevents equal enjoyment of goods or services on basis of individual’s actual or perceived protected class status <u>Except:</u> may self-test to prevent discrimination or diversify applicant pool. Does not apply to a private club exempt from Title II of the Civil Rights Act.
Geofence prohibition	❖ Person may not use geofence (1,750 foot virtual perimeter) around health care facility for purpose of identifying, tracking, collecting data from or sending notices regarding consumer health data to a consumer <u>who enters the virtual perimeter</u> § 9406 p. 16 <u>Exception:</u> Facility operator’s geofence (ex: to check in patients)	No geofence prohibition	❖ Person may not use geofence (1,750 foot virtual perimeter) around health care facility for purpose of identifying, tracking, collecting data from or sending notices regarding consumer health data a consumer § 9405(3) p. 7 <u>Exception:</u> Facility operator’s geofence (ex: to check in patients)
Data Security and Retention § 9406(2)(c) + (d)	❖ 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 § 9406 (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 No data retention schedule required § 9406(2)(A) p. 7	❖ 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> — unless consumer <u>consents</u> to longer time or controller is required to retain the personal data longer by law § 9408 (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 LD 1088 § 9608 p. 14-15 LD 1224 § 9608 p. 12-13 LD 1822 § 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: - 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: - 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: - 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), LD 1224 (Roberts) and LD 1822 (Kuhn)

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

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), 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 <u>only</u> applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥100,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived >25% of gross revenue from the sale of personal data Beginning January 1, 2028: ❖ Law <u>only</u> applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥50,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	From July 1, 2026, to December 31, 2027: ❖ Law <u>only</u> applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥100,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived >25% of gross revenue from the sale of personal data Beginning January 1, 2028: ❖ Law <u>only</u> applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥50,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	Beginning July 1, 2026: ❖ Law <u>only</u> applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥35,000 Maine residents (except solely for purposes of payment transactions) <u>or</u> ○ Of ≥10,000 Maine residents and derived >20% of gross revenue from the sale of personal data
Exempt entities <u>LD 1088</u> § 9603(3) p. 6 <u>LD 1224</u> § 9603(3) p. 5 <u>LD 1822</u> § 9604(1) p. 6-7	❖ Law <u>not</u> applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Financial institution, affiliate or "service corporation" (defined in Title 9-B) subject to the federal Gramm-Leach-Bliley Act — only if it is directly and solely engaged in financial activities described in GLBA • A "licensee" under Maine's insurance laws — to the extent it is complying with any applicable data security and privacy requirements in Maine insurance law	❖ Law <u>not</u> applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • 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	❖ 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), LD 1224 (Roberts) and LD 1822 (Kuhn)

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

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), 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>highly different wording from LD 1088 and LD 1224</i>) - Assisting another controller, processor or 3rd party with its compliance with this law - Collection, use or retention of data for internal use: - Product recalls, - Identifying and repairing technical errors, and - Internal operations reasonably aligned with expectations of the consumer or compatible with processing data to provide a product or service specifically requested by the consumer
Remedies for violations <u>LD 1088</u> <u>§ 9612 p.18-19</u> <u>LD 1224</u> <u>§ 9611 p.17</u> <u>LD 1822</u> <u>§ 9614 p.21-22</u>	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Must provide at least 30-days advance notice and opportunity to confer with AG’s Office — unless show facts in affidavit demonstrating immediate irreparable harm to consumers in the State if notice is given ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Must provide at least 30-days advance notice - AG may not bring action unless controller fails to cure an alleged violation listed in the notice within 30 days ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Until April 1, 2027, if AG believes it is possible for a controller or processor to cure a violation, may choose to give notice of the violation prior to initiating suit - If notice is given, AG may not bring action unless violation is not cured within 60 days - Factors regarding whether to give notice: number of violations, size and complexity of defendant, nature and extent of defendant’s processing activities, likelihood of injury to public, degree to which violations affect safety, whether the alleged violation was likely a human or technical error, and past violations by defendant of this or similar laws ❖ No private right of action ❖ AG rulemaking authority under UTPA to interpret law

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts), 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. 26 • 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)