Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	Redlined LD 1977 (O'Neil) – *structure much closer to LD 1973/CTDPA*
Data and information **NOT** protected by the legislation	❖ "**Publicly available information**": information made available via: • Government records • Disclosure to public required by law; • Widely distributed media; • Publicly accessible (fee or for free) website or online service (unless person providing info. restricts it to a specific audience); • Visual observation of person or device in a public place; **Exceptions** (not considered publicly available) • Obscene visual depictions • All biometric information • Genetic info. unless made public by the individual themselves • Intimate images known to be created or shared w/o consent	❖ "**Publicly available info.**": info. lawfully made available to public via: • Government records – if follow restrictions from government; • Disclosure to public required by law; • Widely distributed media; • Publicly accessible (fee or for free) website or online service (unless person providing info. restricts it to a specific audience); • Visual observation of person or device in a public place; **Exceptions** (not considered publicly available) • Obscene visual depictions • All biometric information • Genetic info. unless made public by the individual themselves • Intimate images known to be created or shared w/o consent • Inferences of sensitive data from multiple public info. sources • Publicly available info. combined with (protected) personal data
Protected Data *Note: These definitions are not limited to the data of Maine "consumers" but the bills' protections apply to consumers*	❖ "**Personal data**": • Data linked or reasonably linkable to an identifiable individual (a "consumer") who is a Maine resident Excludes: "Publicly available information" (definition above) and "de-identified data" (see duties listed in chart below)	❖ "**Personal data**": • Info. linked or reasonably linkable, alone or with other info., to identifiable individual (a "consumer") who is a Maine resident or to a device reasonably linkable to an individual Excludes: "Publicly available information" (definition above) and "de-identified data" (see duties listed in chart below)
	❖ "**Sensitive data**": subset of personal data including: • Data revealing race, ethnicity, religion, mental or physical health, sexual orientation, citizenship or immigration status • Biometric or genetic data processing to uniquely ID a person • Precise geolocation data (within 1,750 feet) of individual • Personal data of a known child <13 years of age • Social security, driver's license or ID number – processing of it • Billing, financial or payment method info. – processing of it	❖ "**Sensitive data":** subset of personal data including: • Data revealing race, ethnicity, religion, mental or physical health (including pregnancy status), sexual orientation, union membership, citizenship or immigration status • Consumer health data (data used to ID physical or mental health condition or diagnosis, including gender-affirming health data and reproductive or sexual health data) • Biometric data (same definition as LD 1973) and genetic data • Precise past or present geolocation data within 1,750 feet) of individual or device • Information of person known to be a minor <18 y.o. • Social security, passport or driver's license or ID number • Financial account # or credit/debit card # (except last 4 digits) • Private communications (email, text, DM, voicemail, mail) and metadata information about their transmission

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	Redlined LD 1977 (O'Neil) – *structure much closer to LD 1973/CTDPA*
		• Account or device log-in credentials or access codes • Calendar and address book info., phone or text logs, photos, audio recordings, and videos if those are for private use, whether on individual's device or remotely stored (except if sent to or from employer-provided device) • Photo or video images of naked or undergarment-clad genitals • Information about video content requested by an individual • Information about individual's online activities over time • Data about individual's status as a crime victim
	Exception (both types of data above): • "Consumer" is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	*Same as LD 1973*
Size and Maine connection requirements for regulation	❖ **Law only applies to** persons that: • Conduct business in Maine or target Maine residents (other than solely for purpose of billing for requested product/service)	❖ **Law only applies to** persons that: • Conduct business in Maine or target Maine residents • In last calendar year, controlled or processed personal data of: ○ ≥35,000 Maine residents (except solely for purposes of payment transactions) **or** ○ ≥10,000 Maine residents and derived > 20% of gross revenue from the sale of personal data
Types of entities regulated	❖ **Controller:** person that alone or jointly with others determines purpose and means of processing personal data ❖ **Processor:** person that processes (collects, uses, stores, discloses, analyzes or deletes) personal data for a controller	*Same as LD 1973*
Exceptions to applicability Note: *for LD 1973, see lists on pp. 4-6 and 12-14*	❖ **Law not applicable to (types of entities)**: • State or its political subdivisions or boards or agencies, • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Financial institution subject to federal GLBA [*sponsor may narrow*] • Covered entities or business associates under HIPAA	**Law not applicable to (types of entities)** • Federal, state, tribal or local government (inc. boards/agencies) • ISPs covered by 35-A M.R.S. §9301 (ISP law)
	❖ **Law not applicable to (types of data)**: • Data subject to federal GLBA • HIPAA data: "protected health information"; intermingled information held by HIPAA-regulated entities; de-identified info. and info. for public health activities under HIPAA	❖ **Law not applicable to (types of data)**: • Data collected, processed, sold or disclosed under GLBA • HIPAA data: "protected health information"; intermingled information held by HIPAA-regulated entities; de-identified info. and info. for public health activities under HIPAA

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*

	• Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2)
	• Identifiable info. collected as part of human subject research conducted under certain federal laws or international guidelines
	• Info. created, collected, processed, sold or disclosed in compliance with the following federal laws:
	  ○ Health Care Quality Improvement Act of 1986
	  ○ Fair Credit Reporting Act [*sponsor open to narrowing*]
	  ○ Driver's Privacy Protection Act of 1994
	  ○ Farm Credit Act of 1971
	• (Education) data regulated by FERPA [*sponsor open to narrowing*]
	• Info. of applicants or employees of a controller, processor or third party or to administer benefits to employees and relatives
	• Disclosures that violate an evidentiary privilege under state law
	• Disclosures that violate freedom of speech or press
		• Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2)
		• Identifiable info. collected as part of human subject research conducted under certain federal laws or international guidelines
		• Info. created, collected, processed, sold or disclosed in compliance with the following federal laws:
		  ○ Health Care Quality Improvement Act of 1986
		  ○ Fair Credit Reporting Act
		  ○ Driver's Privacy Protection Act of 1994
		  ○ Farm Credit Act of 1971
		  ○ Federal Aviation Act of 1958
		• (Education) data regulated by federal FERPA
		• Info. of applicants or employees of a controller, processor or third party or to administer benefits to employees and relatives
		• Patient safety work product under Patient Safety and Quality Improvement Act, 42 U.S.C. §299b-21 et seq.
		• Disclosures that violate an evidentiary privilege under state law
		• Disclosures that violate freedom of speech or press

	❖ **Controller / Processor activities <u>not</u> affected by LD 1973**: • Complying with federal or state (Maine) laws or regulations • Complying with federal or state (Maine) investigations, subpoenas/summonses • Cooperate w/law enforcement re: conduct controller/processor reasonably believes may violate federal, state or local law • Investigating, exercising or defending legal claims • Providing product/service requested by consumer, • Performing services of contract with consumer (ex: warranty) • Taking immediate steps to protect an interest essential for the life or physical safety of a consumer or other individual • Preventing or responding to security incidents, identity theft, fraud, harassment or illegal activity or report those incidents • Engaging in scientific or statistical research that adheres to all other ethics and privacy laws and is overseen by an IRB	❖ **Controller / Processor activities <u>not</u> affected by LD 1977**: (*as long as those activities meet the applicable data minimization standards*) • Complying with federal, state or local laws or regulations • Complying with federal, state or local investigations, subpoenas/summonses • Cooperate w/law enforcement re: conduct controller/processor reasonably believes may violate federal, state or local law • Investigating, exercising or defending legal claims • Providing product/service requested by consumer (whose data it is) , • Performing services of contract with consumer (ex: warranty) • Taking immediate steps to protect an interest essential for the life or physical safety of a consumer or other individual • Preventing or responding to security incidents, identity theft, fraud, harassment or illegal activity targeted to or involving the controller or processer, or report those incidents (newly defines "security incident" and "illegal activity" on pp. 31-32) • Engaging in scientific or statistical research that adheres to all relevant laws and regulations and is overseen by an IRB

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
	• Assisting another controller or processer with its compliance • Process personal data for public health purposes subject to confidentiality obligations of federal or state laws • Processing of personal data by person for own household use • Collection, use or retention of data for internal use, including R&D, product recalls, identifying and repairing technical errors	• Assisting another controller or processer with its compliance • Process personal data for public health purposes subject to confidentiality obligations of federal or state laws • Processing of personal data by person for own household use • Processing data previously collected under LD 1977 for: R&D; product recalls: identifying and repairing technical errors; system maintenance; to protect against spam; or for targeted advertising to adults who have not exercised the right to opt out • Ensure data security and integrity of personal data • To deliver a non-advertisement communication to a consumer (if reasonably anticipated by the consumer) • To deliver a communication at the direction of a consumer • Support/promote participation in civic engagement, including voting, petitioning, unionizing, providing indigent legal services • Transferring assets to successor in interest after notice to affected individuals and reasonable opportunity to withdraw consent or request deletion of personal data
Data minimization requirements	❖ Controller must limit **collection** of **personal data** to: • What is **adequate, relevant and reasonably necessary** to provide the service requested by the consumer ❖ Controller must limit **processing of sensitive data of child < 13** in accordance with federal Children's Online Privacy Protection Act of 1988 (generally requires parental consent)	❖ Controller must limit **collection**, **processing and transferring** of **personal data** to: • What is **reasonably necessary & proportionate** to provide or maintain the product or service requested by the consumer ❖ Controller must limit **collection**, **processing and transferring** of **sensitive data** (except biometric data) to: • What is **strictly necessary** to provide or maintain the product or service requested by the consumer ❖ Controller may not **collect biometric data** without **consent (opt-in)**

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	Redlined LD 1977 (O'Neil) – *structure much closer to LD 1973/CTDPA*
Consent requirements for protected data	❖ Activities permitted **without consent** • **Process** (collect, process & disclose but not sell) **non-sensitive personal data** for any disclosed purpose except targeted advertising	❖ Activities permitted **without consent** • **Process** (collect, process & disclose but not sell) **non-sensitive personal data** for any disclosed purpose except targeted advertising • **Collect/process/*disclose to processor*** (but not sell) most types of **sensitive data** (except SSNs, biometrics or data of minors) for any disclosed purpose except targeted advertising
	❖ Activities permitted only with **choice to opt-out** • Processing personal data for **targeted advertising** • **Selling** personal data Exceptions: "sale" defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate or (d) successor in interest after merger, bankruptcy or other transaction. • Process personal data for "**profiling**" (solely automated decisions producing legal or similarly significant effects)	❖ Activities permitted only with **choice to opt-out** • Processing personal data for **targeted advertising** • **Selling** personal data Exceptions: "sale" defined to exclude sharing personal data with (a) processor; (b) affiliate; or (c) 3rd party for whom consumer gives opt-in consent to disclose the data *[This last category (c) is confusing and may need clarification]* • Process personal data for "**profiling**" (solely automated decisions producing legal or similarly significant effects)
	❖ Activities permitted only **with consent (opt-in)** • Processing **sensitive data** for **any purpose** (recall this includes all personal data of any minor under age 13) • Processing **personal data** of minor age 13-15 for **targeted advertising** or for **sale** (see definition of "sale" above)	❖ Activities permitted only **with consent (opt-in)** • **Collect** any **biometric data** • **Transferring sensitive data** to a 3rd party Exceptions: may transfer (a) to comply with law; (b) to prevent imminent injury; (c) to a successor in interest; (d) to transfer password to identify reused passwords; (e) to transfer genetic info. for medical diagnosis or treatment • Processing **personal data** of minor under age 18 for **sale** (see definition of "sale" above)
		❖ Other **prohibited** activities (regardless of consent) • Process or transfer **SSNs** (except for limited reasons—*e.g.*, for credit extension, authentication, collection or payment of taxes, enforce a contract, prevent fraud/crime or as required by law) • Process **sensitive data** (recall this includes all personal data of any minor under age 18) for **targeted advertising**

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	Redlined LD 1977 (O'Neil) – *structure much closer to LD 1973/CTDPA*
Requirements for consent	❖ **Consent (opt-out)** requirements for **controllers**: • Provide 2 conspicuous links on homepage: "Do Not Sell My Personal Data" and "Opt Me Out of Targeted Advertising"; **or** provide single link to do both activities or all privacy activities • Treat like other consumer rights request (see below) – so must comply within 45 days, subject to appeal, etc.	❖ **Consent (opt-out)** requirements: • Provide conspicuous link on Internet website to opt-out page • Treat like other consumer rights request (see below) – so must comply within 45 days, subject to appeal, etc. • Need not authenticate request, but may deny request and notify requester if in good faith believe request is fraudulent
	❖ **Who may consent (opt-out):** Opt-out consent may be given by: (a) consumer, (b) designated agent, guardian or conservator; or (c) parent or legal guardian of minor consumer <13 years old	*Same as LD 1973*
	❖ **Mechanism to opt-out:** By July 1, 2025 (bill effective date): • Must be consumer-friendly and easy to use; • May not use a default setting; • Must be as consistent as possible with similar mechanisms required by other state or federal law; • Must enable controller reasonably to verify the Maine residency of the consumer & to verify legitimacy of opt-out request; and • Must also (?) accept an opt-out preference signal sent to controller from a (universal) platform, technology or mechanism (may accept opt-out preference signal approved by other state)	❖ **Mechanism to opt-out:** By Jan. 1, 2025 (after bill effective date): • Must be consumer-friendly and easy to use; • Must enable controller to accurately verify Maine residency (can use IP address to estimate customer's location for this purpose) & to verify legitimacy of opt-out request; • If opt-out request conflicts with prior privacy setting or with participation in consumer loyalty program, must follow opt-out but may notify consumer of the conflict

	❖ **Consent (opt-in)** requirements:
	• Affirmative written/electronic specific and unambiguous act
	• Freely given (user interface may not impair decision-making)
	• *(Not explicit)* presumably consumer must be informed of the purposes for which personal data is processed (perhaps the privacy notice is sufficient for this purpose?)
		❖ **Consent (opt-in)** requirements:
		• Affirmative act that is specific and unambiguous
		• Freely given (user interface may not be designed to impair decision-making and must not use material misrepresentations)
		• The option to refuse consent must be at least as prominent as to consent
		• Made after standalone opt-in request from controller:
		  ○ Made via primary medium used to offer product/service
		  ○ IDs specific categories of personal data to be collected, processed or transferred for each processing purpose
		  ○ In each language in which the product/service is provided
		  ○ Is reasonably accessible to consumers with disabilities

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
	❖ **Consent (opt-in)** may **not** be based on: • Accepting a terms of use agreement (must be separate) • Hovering over, muting, pausing or closing content	❖ **Consent (opt-in)** may **not** be based on: • Accepting a terms of use agreement (must be separate) • Hovering over, muting, pausing or closing content • Inaction by consumer or continued use of service/product
	❖ **Who may consent (opt-in):** Opt-in consent may be given by: (a) consumer, or (b) parent or legal guardian of minor <13 years old * *Note: not clear if agents, guardians or conservators can give opt-in consent*	*Same as LD 1973*
	❖ **Mechanism to revoke consent (opt-in)** • Must be at least as easy as mechanism to consent • Controller must comply within 45 days of receiving request	❖ **Mechanism to revoke consent (opt-in)** • Must be at least as easy as mechanism to consent • Controller must comply within 15 days of receiving request
Discrimination provisions	❖ **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 and processer** may not collect, process or transfer personal data in manner that discriminates based on actual or perceived membership in a class protected by the Maine Human Rights Act Exceptions: (a) self-testing to prevent discrimination; (b) collection or processing to diversify an applicant or customer pool; (c) private clubs not open to the public
Retaliation prohibitions	❖ **Controller** may not discriminate against consumer for exercising a right under this law, including by: • Denying or charging different prices for goods or services • Providing different level or quality of goods or services Exception: • Need not offer product or service if lack required personal data • May offer different price, quality or selection of goods or services via a **voluntary consumer loyalty program**	❖ **Controller** may not retaliate against consumer for exercising a right under this law (or for refusing to give any consent), including by: • Denying or charging different prices for goods or services • Providing different level or quality of goods or services Exceptions: • Need not offer product or service if lack required personal data • May offer different price, quality or selection of goods or services via a **voluntary consumer loyalty program** (referred to as a "financial incentive program" in redlined LD 1973) ○ **Only if** – (a) only necessary personal data is transferred to 3rd parties as part of the program, (b) data transfers are disclosed to program members and (c) transferred data is not retained for any other purpose by 3rd party. ○ Note: no sale of personal data may be considered necessary

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
Consumer / individual rights	❖ A **consumer has a right**, upon making an authenticated request personally or through a guardian or conservator, to: **It is not clear that omitting agents was intentional.* • **Confirm** whether controller processes personal data • **Access** own personal data processed by controller • **Correct inaccuracies** in personal data • **Delete** personal data about the consumer • Obtain a **portable copy** of own personal data from a controller Exceptions: • Controller need not disclose info. that reveals a trade secret • Controller need not disclose de-identified data or data the controller is not reasonably capable of associating or it would be unreasonably burdensome to associate with the consumer • Controller or processer need not comply with rights request if it does not either sell personal data to a 3rd party or voluntarily disclose the personal data to a 3rd party (unless it's de-identified)	❖ A **consumer has a right**, upon making an authenticated request personally or through an agent, guardian or conservator, to: • **Confirm** whether controller processes personal data • **Access** own personal data processed by controller • **Correct inaccuracies** in personal data • **Delete** personal data about the consumer • Obtain a **portable copy** of own personal data from a controller • Be told **list of 3rd parties** to which controller disclosed consumer's personal data or anyone's personal data Exceptions: • Controller need not disclose info. that reveals a trade secret • Controller need not disclose de-identified data or data the controller is not reasonably capable of associating or it would be unduly burdensome to associate with the consumer
	❖ **Request / appeal process**: • Must be secure and reliable • Each consumer may make one free request per year – ○ Except may charge a reasonable fee or decline to act on manifestly unfounded, technically infeasible, excessive or repetitive requests with explanation to requester • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must act respond or decline to act on the request within 45 days of request; • If decline to act, must provide justification and appeal info. • **Appeal:** Consumer may appeal controller's inaction within a reasonable time. Decision (with reasoning) due within 60 days. • **Complaint to AG:** If appeal is denied, must provide mechanism for consumer to submit a complaint to the AG	❖ **Request /appeal process**: • Must be secure and reliable – without use of false, fraudulent or materially misleading statements or request interfaces • Each consumer may make one free request per year – ○ Except may charge a reasonable fee or decline to act on manifestly unfounded, excessive or repetitive requests with explanation to requester • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must act respond or decline to act on the request within 45 days of request – may extend time to respond by 45 days if reasonably necessary (must inform consumer of reason) • If decline to act, must provide justification and appeal info. • **Appeal:** Consumer may appeal controller's inaction within a reasonable time. Decision (with reasoning) due within 60 days. • **Complaint to AG:** If appeal is denied, must provide mechanism for consumer to submit a complaint to the AG

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
Required privacy notice	❖ **Controller** must provide reasonably accessible and clear privacy notice that includes: • Controller's online contact information (e-mail or other) • Categories of personal data it processes • Purpose for processing personal data • How consumers may exercise their rights • What categories of personal data are shared 3rd parties • What categories of 3rd parties it shares personal data with	❖ **Controller** must provide reasonably accessible and clear privacy notice that includes: • Controller's online contact information (e-mail or other) • Categories of personal data it processes (using clear description) • Categories of sensitive data processed (using clear description) • Purpose for processing each category of personal data • Length of time it retains each category of personal data • How consumers may exercise their rights • What categories of personal data are shared 3rd parties • What categories of 3rd parties it shares personal data with • If controller sells personal data or processes personal data for targeted advertising, describe this and the opt-out mechanism ❖ **Material change: controller** must, before materially changing its policy for prospectively collected personal data: • Take reasonable measures to elect. notify affected individuals • Provide reasonable opportunity to withdraw consents
Deletion of protected data	❖ **By request**: as is explained above, controller must delete protected data for free within 45 days of authenticated consumer request Exceptions (specific to deletion requests): • If controller did not itself collect the data requested to be deleted, it may retain the data deletion request and minimum data necessary to ensure data remains deleted in its system • Controller may charge a reasonable fee or decline to act on manifestly unfounded, technically infeasible, excessive or repetitive requests with explanation to requester	❖ **By request**: as is explained above, controller must delete protected data for free within 45 days of authenticated consumer request Exceptions (specific to deletion requests): • If controller did not itself collect the data requested to be deleted, it may retain the data deletion request and minimum data necessary to ensure data remains deleted in its system **or** opt the consumer out of processing such personal data • Controller may charge a reasonable fee or decline to act on manifestly unfounded, excessive or repetitive requests with explanation to requester • Controller that is a private school (including college/university) may decline to delete personal data that would unreasonably interfere with provision education services (ex: student grades)

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
Data Security (*redlined LD 1977 no longer requires data security officers*)	❖ **Controller** must: • Establish and implement reasonable data security and integrity practices appropriate to the volume and nature of the data	❖ **Controller** and **processor** must • Establish & implement reasonable data security practices to protect against unauthorized access appropriate to volume and nature of the data; size and complexity of entity; nature and scope of collecting, processing or transferring activity; sensitivity of the data; current state-of-the art safeguards; and security costs • Identify & assess internal & external risks to its systems • Plan to receive/respond to reports of vulnerabilities • Prevent and mitigate identified reasonably foreseeable risks and vulnerabilities to personal data (ex: through software) • Train employees with access to personal data on data security • Implement procedures to detect / respond to security breaches ❖ **Controller** must **delete personal data** (when retention is no longer necessary for the collection/processing purpose. **Processor** must delete personal data or return it to controller at end of provision of services. Exceptions: (a) if have affirmative consent (opt-in) to retain data or (b) if required to retain data by law
Data Protection Assessments (*redlined LD 1977 transferred some of the bill's original algorithm assessment requirements into this section*)	❖ **Controller** must conduct/document **data protection assessment(s)** weighing benefits to controller, consumer and public of processing the data against the risks to consumers • **What activities must be assessed?** All activities presenting a heightened risk to consumers including: o Processing personal data for targeted advertising o Sale of personal data o Processing of sensitive data o Processing of personal data for profiling that presents a foreseeable risk of unfair treatment of consumers or of physical, reputational or financial injury to consumers • **When?** Not specified • **Copy to AG:** Must provide copy of assessment to AG on request (if relevant to an investigation). Assessment is not a public record for purposes of FOAA.	❖ **Controller** must conduct/document **data protection assessment(s)** weighing benefits to controller, consumer and public of processing the data against the risks to consumers. The assessment must ID categories of personal data collected and why and whether transferred to 3rd parties. • **What activities must be assessed?** All activities presenting a heightened risk to consumers including: o Processing personal data for targeted advertising o Sale of personal data o Processing of sensitive data o Processing of personal data for profiling that presents a foreseeable risk of unfair treatment of consumers or of physical, reputational or financial injury to consumers ▪ Profiling assessments require detailed descriptions of algorithm used, reasonably foreseeable uses of the algorithm, steps taken to mitigate harm, etc. (see p.28) • **When?** (a) before engaging in an activity that poses heightened risk and (b) must update assessment "as often as appropriate" • **Summary/AG:** Must make a summary of assessment publicly accessible and available to AG on request (redact private info.)

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
Processor duties and prohibitions	❖ **Processor** must: • Assist controller with responding to consumer requests • Assist controller with meeting data-security obligations • Notify controller of any security breach in processor's system • Assist controller with data protection assessments • Act only under contract with controller requiring it to: o Ensure each person processing personal data is subject to a duty of confidentiality o Delete or return personal data at end of services o Cooperate with controller assessments and/or share independent assessments of its own services o Require all subcontractors (if any) via written contract to comply with processor's obligations related to personal data ❖ **Processor** may not: • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1973)	❖ **Processor** must: • Assist controller with responding to consumer requests • Assist controller with meeting data-security obligations • Notify controller of any security breach in processor's system • Assist controller with data protection assessments • Act only under contract with controller requiring it to: o Only process data as directed by controller, to extent necessary to provide service requested by the controller o Not commingle personal data from >1 controller o Ensure each person processing personal data is subject to a duty of confidentiality o Delete or return personal data at end of services o Cooperate with controller assessments and/or share independent assessments of its own services o After allowing controller to object, engage subcontractors and require all subcontractors via written contract to comply with processor's obligations related to personal data ❖ **Processor** may not: • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1977)
Regulation of de-identified data; and pseudonymous data	❖ **Controller** in possession of **de-identified data** must: • Take reasonable measures to prevent re-identifying the data and publicly commit to not attempting to re-identify the data • Contractually obligate recipients of the data to comply with law and monitor compliance with those contractual commitments ❖ **Controller** in **possession** of **pseudonymous data** (personal data that can't be attributed to a specific individual w/out the use of additional info.that is kept separately from the pseudonymous data): • Need not respond to consumer requests about the data if the data is kept separately with appropriate technical measures to ensure the personal data can't be attributed to an individual	❖ **Controller** in possession of **de-identified data** must: • Take technical measures to prevent re-identifying the data and publicly commit to not attempting to re-identify the data • Contractually obligate recipients of the data to comply with law and monitor compliance with those contractual commitments *LD 1977 does not address pseudonymous data*
Geofence prohibitions	n/a	❖ **No person may create a geofence** (virtual boundary within 1750 feet of facility) to identify, track, collect data from or send notices to consumers regarding the consumer's CHD around: • A mental health, reproductive or sexual health facility

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
Remedies for violations Action by government entity	❖ **Attorney General** may bring action under Unfair Trade Practices Act (UTPA) against a controller or processer to obtain UTPA remedies: • Injunctive relief to enforce compliance with law/rules • Civil penalties (up to $10,000 for intentional UTPA violations or violations of a UTPA injunction) • Restitution (on behalf of State residents is implied); and • Investigation costs and costs of the suit	❖ **Attorney General, DA or Municipal Counsel** may bring an action against a controller or processor under LD 1977 (or the UTPA) for: • Injunctive relief to enforce compliance with law/rules • Damages or civil penalties (presumably in the amounts below under the private action provision) on behalf of State residents; • Restitution on behalf of State residents; and • Reasonable attorney's fees and litigation costs
Right to cure before action by government entity	❖ **Right to cure:** • During first 18 months after law takes effect: **AG must** first provide notice of violation and **30-day right to** cure if AG determines a cure is possible; may not initiate action if controller or processor asserts in writing the alleged violations have been cured and no future violations will occur • After 1st 18 months: **AG discretion** to give **30-day** opportunity to cure. Factors to consider: number of violations; size and complexity of defendant and nature of its processing activities; likelihood of injury to public, safety of persons or property; whether violation was caused by human or technical error	❖ **Right to cure:** • For all time periods: **AG discretion** to give **60-day** opportunity to cure. Factors to consider: number of violations; size and complexity of defendant and nature of its processing activities; likelihood of injury to public, safety of persons or property; whether violation was caused by human or technical error
Private actions	❖ **No private right of action**	❖ **Private action** by individual injured by violation of law/rules against entity committing violation for: • At least a $5,000 civil penalty per individual, per violation (adjust for inflation) or actual damages, whichever is greater • Punitive damages (no limit/amount stated) • Injunctive and declaratory relief • Reasonable attorney's fees and litigation costs ❖ Pre-dispute **arbitration agreements** are unenforceable
Rulemaking	❖ **No AG power** to make rules interpreting LD 1973	❖ **AG may** make (major substantive?) rules interpreting LD 1977 *Note: UTPA rules provision in 5 M.R.S. §207(2) is unclear whether those are major substantive rules. If want to follow UTPA, should ask AG about this.*
Exceptions to liability	❖ **Exceptions to liability** for all enforcement actions: • Controller not liable if processor or 3rd party violates LD 1973 absent knowledge that processor would violate the law • Processor or 3rd party not liable for controller's violations	*Same as LD 1973*

Comparison of Sponsors' Redlined Versions of LD 1973 and LD 1977 – Differences highlighted

	Redlined LD 1973 (Keim)	**Redlined LD 1977 (O'Neil)** – *structure much closer to LD 1973/CTDPA*
Repeal of other laws	❖ **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. **See handout showing law to be repealed*	*Redlined LD 1977 instead makes ISPs exempt from the legislation (and thus still subject to 35-A M.R.S. §9301)*
Attorney General Report	❖ By Feb. 1, 2027 (19 months after effective date) – AG report to JUD: • Number of right to cure notices issued & nature of violations ci • Number of violations cured within the 30-day cure period • Any other matter AG deems relevant [*Per sponsor: JUD can then report out bill to adjust law*]	n/a
Effective Date	❖ **Effective date:** July 1, 2025 • [*sponsor open to more delayed effective date for small businesses*]	❖ **Effective date:** 180 days after adjournment (most of bill) Exception: • 1 year later: data protection assessment requirement effective
	Miscellaneous	
Definition of targeted advertising	**21. Targeted advertising.** "Targeted advertising" means displaying advertisements to a consumer when the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated publicly accessible websites or online applications to predict that consumer's preferences or interests. "Targeted advertising" **does not include**: A. Advertisements based on activities within a controller's own publicly accessible websites or online applications; B. Advertisements based on the context of a consumer's current search query, visit to a publicly accessible website or online application; C. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or D. Processing personal data solely to measure or report advertising frequency, performance or reach.	**18. Targeted advertising.** "Targeted advertising" means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics or interests associated with the individual or a device identified by a unique identifier. "Targeted advertising" **does not include** A. Advertisements based on activities within a controller's own publicly accessible websites or online applications, provided that the processing necessary to generate such advertisements does not include sensitive data; B. [Ads] based on the context of a consumer's current search query, visit to a publicly accessible website or online application, in which the [ad] appears and does not vary based on who is viewing the [ad]; C. [Ads] directed to a consumer or consumer's device in response to the consumer's specific request for information or feedback; or D. Processing personal strictly necessary for the sole purpose of measuring or reporting advertising frequency, performance or reach.
Special business types		*Redlined LD 1977 no longer contains special rules for small businesses, data brokers, large data holders, and high-impact social media companies*