大成 DENTONS

Do you know what your neighbor is doing?

Dentons US and Canada Comparative Privacy Cheat Sheet

The digital revolution has created a whole host of new questions regarding privacy, consent, and data protection. Canada and the United States, though close allies and mutually dependent trade partners, have vastly different approaches to privacy law, some apparent and some less so. How can businesses operating between these two nations comply with the laws of each and keep pace with a rapidly evolving area of law? Dentons US and Canada Comparative Privacy Cheat Sheet provides a quick comparison of current and proposed privacy laws. Please note this document will be updated regularly to reflect the changing privacy landscape.

Disclosure:

This cheat sheet is not comprehensive and is meant as a general reference guide. Information may change as the privacy laws change in Canada and the US. This guide does not constitute legal or professional advice or opinion. If you have any questions, please reach out to Peter Stockburger or Kirsten Thompson for further guidance.

This document has been updated as of October 19, 2021.

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
General							
1. Coming into force and territoriality	The existing Act respecting the Protection of Personal Information in the Private Sector" has been amended by Bill 64, assented to September 22, 2021. The majority of the provisions will come into force two years after the date of royal assent, with a few provisions coming into force in one year (e.g., appointment of privacy officer, breach reporting, right to disclose personal information without knowledge or consent in context of a business transaction or research).	January 1, 2001	Not yet passed	January 1, 2020 (applies extra-territorially)	January 1, 2023 (applies extra-territorially)	January 1, 2023 (applies extra-territorially)	July 1, 2023 (applies extra-territorially)
2. Regulator/data protection authority	Commission d'accès à l'information du Québec (CAI)	Office of the Privacy Commissioner of Canada (OPC)	Office of the Privacy Commissioner of Canada (OPC) Tribunal	California Attorney General	California Attorney General California Privacy Protection Agency (CPPA)	Virginia Attorney General	Colorado Attorney General Colorado District Attorneys

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
3. Scope	Any "enterprise" (defined by Civil Code of Québec) which collects, holds, uses or communicates PI whether it keeps the information itself or through a third person. Applies to PI held by a professional order to extent provided for in Professional Code) and to that held by an authorized entity to the extent provided for in Election Act. Excludes public bodies (as defined in Act respecting Access to documents held by public bodies and the Protection of personal information.	Applies to every organization in respect of PI that it collects, uses or discloses PI in the course of its commercial activities in Canada (includes foreign organizations that have a "real and substantial" connection to Canada). Excludes government institutions to which the public sector Privacy Act applies. Excludes activities to which 'substantially similar" provincial private sector privacy legislation or health privacy legislation applies. Only covers employees of, or applicants for employment with, an organization that collects, uses or discloses PI in connection with the operation of a federal work, undertaking or business.	Applies to every organization in respect of PI that • the organization collects, uses or discloses in the course of commercial activities; or • is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business. The CPPA applies in respect of PI • that is collected, used or disclosed interprovincially or internationally by an organization; or • that is collected, used or disclosed by an organization within a province, to the extent that the organization is not exempt from the application of the CPPA under an order made under paragraph 119(2)(b) of the CPPA. CPPA applies to service providers, however they are exempt from its general obligations (except for safeguards requirements and breach reporting/notification).	Applies to covered "businesses", "service providers" and any non "third party". Two definitions of a "business": Definition #1: Any for-profit legal entity that: (a) collects California resident PI (or on the behalf of which such PI is collected); (b) that alone, or jointly with others, determines the purposes and means of processing PI; (c) does business in California; and (d) satisfies one of three thresholds: • Annual gross revenue in excess of $25m USD; or • Alone or in combination with others annually buys, receives for a commercial purpose, sells, or shares for a commercial purpose the PI of 50,000 or more California residents, households, or devices; or • Derives 50% or more of annual revenues from selling California resident PI. Definition #2: Any legal entity that controls or is controlled by a business that meets Definition #1, and shares common branding with the business. "Service provider" is separately defined. A non "third party" is separately defined.	Applies to covered "businesses", "service providers", and "contractors." Four definitions of a "business": Definition #1: Any for-profit legal entity that: (a) collects California resident PI (or on the behalf of which such PI is collected); (b) that alone, or jointly with others, determines the purposes and means of processing PI; (c) does business in California; and (d) satisfies one of three thresholds: • As of January 1 of the calendar year, had annual gross revenue in excess of $25m USD in the preceding calendar year; or • Alone or in combination with others annually buys or, sells, or shares the PI of 100,000 or more California residents or households; or • Derives 50% or more of annual revenues from selling or sharing California resident PI. Definition #2: Any legal entity that controls or is controlled by a business that meets Definition #1, and shares common branding with the business and with whom the business shares consumers' PI. Definition #3: A joint venture or partnership composing of "businesses" in which each business has at least a 40% interest. Definition #4: A person that does business in California, that is not covered by the definitions above, but that voluntarily certify to the CPPA that it is in compliance with, and agrees to be bound by the CPRA.	Applies to covered entities that: • Conduct business in Virginia; • Produce products or services that are targeted to Virginia residents; and • During a calendar year: (1) controls or processes the personal data of at least 100,000 Virginia residents; or (2) controls or processes the personal data of at least 25,000 Virginia residents and derives over 50% of gross revenue from the sale of personal data.	Applies to entities that: • Conduct business in Colorado or produces or delivers commercial products or services that are intentionally targeted to residents of Colorado; and • Satisfies one or both of the following thresholds: (1) controls or processes the personal data of 100,000 consumers or more during a calendar year; or (2) derives revenue or receives a discount on the price of goods or services from the sale of personal data and processes or controls the personal data of 25,000 consumers or more.[1]

[1] Colo. Rev. St. § 6-1-304(1).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
Definitions							
4. Person / Consumer	All natural persons are protected, regardless of citizenship. However, the territorial application of the Bill is unclear. The definition has not changed from the current privacy law.	All natural persons are protected, regardless of citizenship.	All natural persons are protected, regardless of citizenship.	"Consumer" is defined as a California resident. Includes persons acting in a commercial or employment context, subject to certain exceptions.	"Consumer" is defined as a California resident. Includes persons acting in a commercial or employment context.	"Consumer" is defined as a Virginia resident acting in an "individual or household" context. Excludes persons acting in a "commercial or employment" context.	"Consumer" means an individual who is a Colorado resident acting in an individual or household context. This definition expressly excludes B2B (i.e., an individual acting in a commercial context), and any individual acting in an employment context, as a job applicant, or as a beneficiary of someone acting in an employment context.[2]
5. Personal data / information definition	Any information held by an enterprise that relates to a person. Divisions II and III of the Act do not apply to PI which by law is public. Nor do they apply to PI concerning the performance of duties within an enterprise by the person concerned (e.g., name, title and duties, as well as the address, email address and telephone number of the person's place of work.)	Any information about an identifiable individual, with the exception of "business contact information" used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession.	Any information about an identifiable individual, with the exception of "business contact information" used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession.	Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Excludes publicly available, deidentified, and aggregate information.	Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Excludes publicly available information, information that is "lawfully obtained," "truthful information that is a matter of public concern," deidentified, and aggregate information.	Any information that is linked or reasonably linkable to an identified or identifiable natural person. " Excludes de-identified data or publicly available information.	"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. Excludes de-identified data or publicly available information.[3] "Publicly available information" means information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public.[4] "De-identified" data means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data: • Takes reasonable measures to ensure that the data cannot be associated with an individual; • Publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and • Contractually obligates any recipients of the information to comply with the requirements of the above.[5]

[2] Co. Rev. St. § 1-1-1303(6).
[3] Colo. Rev. St. § 6-1-1303(17)(a)-(b).
[4] Colo. Rev. St. § 6-1-1303(17)(b).
[5] Colo. Rev. St. § 6-1-1303(11).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
6. Sensitive information definition	PI is sensitive if, due to its nature or the context of its use or communication, it entails a high level of reasonable expectation of privacy. Consent must be express for sensitive PI.	No definition but is contextual. The level of protection provided by security safeguards must be proportionate to the sensitivity of the information. The sensitivity of the PI is a factor to be taken into account in determining whether the purpose for which it is used collected and disclosed is appropriate.	No definition but is contextual. The level of protection provided by security safeguards must be proportionate to the sensitivity of the information. The sensitivity of the PI is a factor to be taken into account in determining whether the purpose for which it is used collected and disclosed is appropriate. An organization developing a privacy management program must take into account the volume and sensitivity of the PI under its control Note that the federal Privacy Commissioner recently published (non-binding) guidance taking a more list-based approach, stating that "certain types of information that will generally be considered sensitive and require a higher degree of protection. This includes health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious/ philosophical beliefs."	Not expressly addressed.	Defined as: • PI that reveals a consumer's social security, driver's license, state identification card, or passport number. • PI that reveals a consumer's account log-in, financial account, debit card, or credit card number in combination with a password. • PI that reveals a consumer's precise geolocation. • PI that reveals a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership. • PI that reveals the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication. • PI that reveals a consumer's genetic data. • The processing of biometric information for the purpose of uniquely identifying a consumer. • PI collected and analyzed concerning a consumer's health. • PI collected and analyzed concerning a consumer's sex life or sexual orientation.	Any personal data that includes: • Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status. • The processing of genetic or biometric data for the purpose of uniquely identifying a natural person. • The personal data collected from a known child. • Precise geolocation data.	"Sensitive data" means any data that: • Reveals racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; • Genetic or biometric data that may be processed for the purpose of uniquely identifying individual; or • Personal data from a known child.[6] A "child" means an individual under 13 years of age.[7]

[6] Colo. Rev. St. § 6-1-1303(24).
[7] Colo. Rev. St. § 6-1-1303(4).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
Consent							
7. Consent requirements	Must be clear, free and informed and be given for specific purposes. It must be requested for each such purpose, in clear and simple language and, when requested in writing, it must be presented separately from any other information provided to the person concerned. On request, assist must be provided to help an individual understand the scope of the consent requested. Consent is valid only for the length of time needed to achieve the purposes for which it was requested. Individuals are free to withdraw their consent. Consent must be express for sensitive PI.	May be express or implied, each subject to specified requirements and limitations. May be withdrawn at any time on reasonable notice, unless withdrawing consent would frustrate performance of a legal obligation.	Presumption of express consent (onus or organization to demonstrate implied consent would be appropriate). Transfers to service providers do not require consent. Consent must be obtained before the time of the collection of the PI. Consent is valid only if certain information is provided at the time of collection: information regarding the purpose of the collection, the way in which the PI is to be collected, used or disclosed, any foreseeable consequences, the specific type of PI that is to be collected, used or disclosed and the names of any third parties to which the organization may disclose the PI. Individuals can withdraw their consent.	No express consent requirements, generally. Certain opt-in requirements for minor PI or new uses of PI. Some consent exceptions to the definition of "sale."	No express consent requirements, generally. Certain opt-in requirements for minor PI or new uses of PI. Some consent exceptions to the definition of "sale" or "share".	No express consent requirements, generally. Certain consent requirements depending on the nature of processing. Certain consent requirements for use of minor data.	
8. Exceptions from the requirement of consent OR other lawful bases of processing (excluding usual exceptions for emergencies, national security, etc.).	Consent not required when an exception applies: • PI is used for purposes consistent with those for which it was collected, • when its use is clearly for the benefit of the individual concerned, and • when it is de-identified and its use is necessary for study, research or statistical purposes.	Not required when exceptions apply (for example, in the case of a "business transaction").	Consent not required when an exception applies: • Carrying out a defined business activity (such as providing a product or service requested by the individual, securing an organization's information, systems or networks, or where it is virtually impossible to obtain the individual's consent due to the lack of a direct relationship with the individual). • Transfers of PI to service providers; • De-identification of PI and its use for internal research and development purposes.	Certain opt-in requirements for minor PI or for new uses of PI. Some consent exceptions to the definition of "sale."	Certain opt-in requirements for minor PI or for new uses of PI. Some consent exceptions to the definition of "sale" or "share". General processing requirement that restricts a business from collecting, using, retaining, and sharing PI only where reasonably necessary and proportionate to achieve the purposes for which the PI was collected or processed, or for another disclosed purpose that is compatible with the context in which the PI was collected, and not further processed in a manner that is incompatible with those purposes.	Certain consent requirements depending on the nature of processing. Certain consent requirements for use of minor data. Some consent exceptions for certain uses of data.	

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
Data Subject Rights							
9. Data subject right: Access	Yes, on written request and subject to certain exceptions (e.g., possibility of litigation, access may seriously harm a third person). • Request must be in writing with proof of identity • Response within 30 days • Free of charge (reasonable charge permitted in certain conditions • Obligation to provide assistance to requestor	Yes. On written request, on subject to certain exceptions, an organization must inform an individual of whether it has any PI about them, how it uses the information and whether it has disclosed the information, as well as make such information available. • Response within 30 days • Free of charge (unless certain conditions are met) • Obligation to provide assistance to requestor	Yes. On written request, on subject to certain exceptions, an organization must inform an individual of whether it has any PI about them, how it uses the information and whether it has disclosed the information, as well as make such information available. • Response within 30 days • Free of charge (unless certain conditions are met) • Obligation to provide assistance to requestor	Yes. Consumers may request categories and specific pieces of personal information. Business must verify request, and generally respond within 45 calendar days (subject to an extension). Other requirements around response obligations, and verification requirements.	Yes. Consumers may request categories and specific pieces of personal information. Business must verify request, and generally respond within 45 calendar days (subject to an extension). Other requirements around response obligations, and verification requirements.	Yes. Consumer may obtain a copy of personal data. Controller generally must respond within 45 days of receipt of request, subject to certain extensions. Verification standards included. Controller must provide right to appeal decision, subject to certain requirements.	General Right. A consumer has the right to confirm whether a controller is processing personal data concerning the consumer, and to access the consumer's personal data.[8]
10. Data subject right: Rectification (correction)	Yes, if the information is inaccurate or incomplete comment. Rectification rights same as for access.	Yes, if the information is inaccurate or incomplete. Rectification rights same as for access.	Yes, if the information is inaccurate or incomplete. Rectification rights same as for access.	No.	Yes Consumer may request that information be corrected. Business generally must respond within 45 days of receipt of request, subject to certain extensions. Verification standards included.	Yes Consumer may correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of processing. Controller generally must respond within 45 days of receipt of request, subject to certain extensions. Verification standards included. Controller must provide right to appeal decision, subject to certain requirements.	General Right. Consumer has the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.[9]
11. Data subject right: Cancellation (erasure or deletion)	No. However, where the purposes for which PI was collected or used are achieved, the person carrying on an enterprise must destroy or anonymize the information, subject to any preservation period provided for by law. Individuals have the right to: • require that such information cease to be disseminated; • de-indexing/re-indexing.	Not specifically. No explicit right to de-indexing.	As soon as feasible upon the receipt of the individual's written request, unless the disposal would result in the disposal of PI about another individual or requirements of the CPPA or a contract prevent it. The individual must be informed in writing of the refusal to dispose of their PI. The organization must also inform any service provider to whom it has transferred PI and obtain a confirmation that the information has been disposed of. No explicit right to de-indexing.	Yes, subject to certain exceptions. General 45 days to respond, subject to extension. Specific requirements for substance of response, confirmation responses.	Yes, subject to certain exceptions. General 45 days to respond, subject to extension. Specific requirements for substance of response, confirmation responses.	Yes. Consumer delete personal data provided by or obtained about the consumer. Controller generally must respond within 45 days of receipt of request, subject to certain extensions. Verification standards included. Controller must provide right to appeal decision, subject to certain requirements.	General Right. Consumers have a right to delete personal data concerning the consumer.[10]

[8] Colo. Rev. St. 6-1-1306(1)(b).
[9] Colo. Rev. St. 6-1-1306(1)(c).
[10] Colo. Rev. St. 6-1-1306(1)(d).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
12. Data subject right: Portability	Yes. Right to: • obtain a copy of PI held by an enterprise in a structured commonly used technological format upon request • or have it communicated to an authorized person or body.	None.	Yes. Future regulations will provide a data mobility framework, to allow an organization, upon request, to disclose PI to another organization.	Yes. Business must provide information in a usable format.	Yes. Business must provide the information requested in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance.	Yes. Controller must provide information in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller "without hindrance," where the processing is carried out by automated means.	General Right. When exercising any right to access, the consumer has the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance. A consumer may exercise this right no more than two times per calendar year. The controller can withhold trade secrets.[11]
13. De-identification	PI is depersonalized when it no longer allows the direct identification of the person concerned. De-identified information remains subject to the privacy law. • Only "anonymized" information falls outside the privacy law. PI will be considered anonymized when it is at all times reasonable to expect in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly. Anonymization must be done in accordance with the industry best practices in accordance with industry best practices, and any criteria prescribed by regulation. There are penal provisions and fines for persons who make or attempt to make an identification of an individual based on de-identified information. Does not include information created or inferred from personal information collected from the individual.	No specific requirements. Anonymized information, not being PI, would fall outside of PIPEDA's scope.	No distinction between de-identification and anonymization. "De-identification" is defined as modifying PI - or creating information from PI - through technical processes so that the information is not personally identifiable and cannot, under reasonably foreseeable circumstances, be used, either alone or in combination with other information, to identify an individual. De-identified information remains subject to the CPPA. Consent is not required to de-identify PI. The technical and administrative procedures used to de-identify PI must be proportionate to the purposes for which the information is being de-identified and the sensitivity of the PI. Prohibition against using de-identified information, alone or in combination with other information, to identify an individual (except for the purpose of verifying the effectiveness of the security measures in place). Requirement to de-identify PI prior to sharing with counterpart in context of a business transaction (e.g., sale of a business, merger, etc).	Yes. Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: • Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. • Has implemented business processes that specifically prohibit reidentification of the information. • Has implemented business processes to prevent inadvertent release of deidentified information. • Makes no attempt to reidentify the information.	Yes. Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: • Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. • Has implemented business processes that specifically prohibit reidentification of the information. • Has implemented business processes to prevent inadvertent release of deidentified information. • Makes no attempt to reidentify the information.	Yes. Information that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.	"De-identified" data means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data: • Takes reasonable measures to ensure that the data cannot be associated with an individual; • Publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and • Contractually obligates any recipients of the information to comply with the requirements of the above.[12]

[11] Colo. Rev. St. Colo. Rev. St. 6-1-1306(2).
[12] Colo. Rev. St. § 6-1-1303(11).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
14. Automated decision making	Specific rules apply to decisions based exclusively on automated processing. Right to know about the PI, the reasons, factors and parameters used to make the decision and to have the information corrected Right to submit observations for review.	None.	"Automated decision system means any technology that assists or replaces the judgement of human decision-makers". If used, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the PI that was used to make the prediction, recommendation or decision was obtained. More general description required to be included in privacy policy.	Yes. Although no express rights, consumers are entitled to notice at or before the point of collection explaining how their personal information will be used. This may include disclosing how information would be used in automated processing.	Yes. Although no statutory express rights, consumers are entitled to notice at the point of collection, disclosing how personal information (including sensitive personal information) is processed and used, which may include by automated means. CPPA has authority to issue regulations governing access and opt-out rights with respect to the business's use of automated decision-making technology, including profiling and requiring business's response to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer. Consumers also have a right to limit the processing (which may include by automated means) of sensitive personal information.	Yes. Consumers have right to limit processing of profiling activities, which means by automated processing. Additional guidance may be forthcoming.	Consumers have the right to opt-out of the processing of personal data for profiling. "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.[13]

[13] Colo. Rev. St. § 6-1-1303(20).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
15. Other rights	Right to apply to the CAI for review of any disagreement.	Written complaint to the OPC.	Written complaint to the OPC.	Yes. Consumers have a right to opt-out of the "sale" of their personal information. "Sale" is defined broadly, and generally means sharing, disclosing or making available for monetary or other valuable consideration. Certain exceptions exist, including when involving "service providers" or non "third parties." Consumers also have the right to exercise rights under the CCPA free from discrimination, subject to certain exceptions.	Yes. Consumers have a right to opt-out of the "sale" or "share" of their personal information. "Sale" is defined broadly, and generally means sharing, disclosing or making available for monetary or other valuable consideration. "Share" is defined as, among other actions, sharing, disclosing, and/or making available personal information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged. Certain exceptions exist, including when involving "service providers" or non "contractors." Consumers also have a right to opt-out of the processing of sensitive personal information, subject to certain exceptions. Consumers also have a right to anti-discrimination in exercising their rights, subject to certain exceptions.	Yes. Consumers have the right to opt-out of the processing of their personal data for purposes of: (1) targeted advertising (which is separately defined); (2) the "sale" of personal data (which is separately defined); or (3) "profiling" (which is separately defined) in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.	General Right. Consumer may opt-out of the processing of personal data for purposes of: (i) targeted advertising; (ii) the sale of personal data; or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer. "Targeted advertising" means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests.[14] Targeted advertising does not include: (i) advertising to a consumer in response to the consumer's request for information or feedback; (ii) advertisements based on activities within a controller's own websites or online applications; (iii) advertisements based on the context of a consumer's current search query, visit to a website, or online application; or (iv) processing personal data solely for measuring or reporting advertising performance, reach, or frequency.[15] "Profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.[16] "Sale" means the exchange of personal data for monetary or other valuable consideration by a controller to a third party. This does not include: The disclosure of personal data to a processor that processes the personal data on behalf of a controller.

[14] Colo. Rev. St. § 6-1-1303(25).
[15] Colo. Rev. St. § 6-1-1303(25)(b).
[16] Colo. Rev. St. § 6-1-1303(20).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
							The disclosure of personal data to a third party for the purposes of providing a product or service requested by the consumer. • The disclosure or transfer of personal data to an affiliate of the controller. • The disclosure or transfer of a third party of personal data as an asset that is part of a merger, acquisition, etc. • The disclosure of personal data: (i) that a consumer directs the controller to disclose or intentionally discloses by using the controller to interact with a third party; or (ii) intentionally made available by a consumer to the general public via a channel of mass media.[17] Notice Requirements. A controller that engages in targeted advertising or the sale of personal data must provide a clear and conspicuous method to exercise the right to opt-out of the processing of personal data concerning the consumer. The method must be provided clearly and conspicuously in any privacy notice required to be provided to consumers, and readily accessible location outside of the privacy notice. Universal Opt-Out Mechanism. Between 7/1/23 and 7/1/24, it is optional to allow consumers to exercise their opt-out right by a user-selected universal opt-out mechanism that meets the technical specifications established by the Attorney General's office. This becomes mandatory on 7/1/24.[18]

[17] Colo. Rev. St. § 6-1-1303(23).
[18] Colo. Rev. St. § 6-1-1306(a)(IV).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
Children							
16. Special considerations for children	For a minor under 14 years of age, consent must be given by the person who has parental authority or the tutor (unless the information is clearly for the minor's benefit).	No specific rules, though must be able to give meaningful consent. The vulnerability of a population segment will be a factor in determining sensitivity of information, nature of consent required, etc.	No specific rules, though must be able to give meaningful consent. The vulnerability of a population segment will be a factor in determining sensitivity of information, nature of consent required, etc.	Yes. There are special rules around the "sale" of personal information of minors.	Yes. There are special rules for the sale or sharing of personal information of minors, and rules around processing.	Yes. There are special rules around the sale and sharing of personal information of minors, and rules around processing.	Data of a minor child is generally considered sensitive personal data, which is subject to additional restrictions.
Privacy Program							
17. Privacy Officer	Yes, the "person in charge of the protection of personal information". • Must establish and implement governance policies and conduct assessments of the privacy-related factors of any project or system involving PI. • Plays a role in reporting data breaches to the CAI. • Plays a role in access and rectification requests.	Required. An organization must designate one or more individuals to be responsible for matters related to its obligations. It must make the person's business contact information available.	Required. An organization must designate one or more individuals to be responsible for matters related to its obligations. It must provide the person's business contact information to any person who requests it.	No.	No.	No.	No.
18. Privacy Impact Assessments	Must be done for any information system project involving the collection, use, disclosure, retention or destruction of PI.	None specifically required.	Not specifically. Organizations must have a "privacy management program" that can be reviewed by the OPC.	No.	Yes. These may be required by the CPPA subject to future regulations.	Yes. Required in each of the following processing activities involving personal data: • The processing of personal data for purposes of targeted advertising. • The sale of personal data.	Triggering Requirement. A controller shall not conduct a processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities that involve personal data.[19]

[19] Colo. Rev. St. § 6-1-1309(1).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
						• The processing of personal data for profiling, where such profiling presents a reasonably foreseeable risk of (1) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (2) financial, physical, or reputational injury to consumers; (3) a physical or other intrusion upon the solitude or seclusion, or the private affairs or conserns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers. • The processing of sensitive data. • Any processing activities involving personal data that present a heightened risk of harm to consumers. The assessments conducted must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into the assessment by the controller.	"Processing that presents a heightened risk of harm to a consumer" includes: • Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial or physical injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers. • Selling personal data. • Processing sensitive data.[20] Substantive Requirements. The data protection assessment must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller must factor into the assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed. Availability. A controller must make the data protection assessment available to the Colorado AG upon request. Multiple Purposes. A single data protection assessment may address a comparable set of processing operations that include similar activities.

[20] Colo. Rev. St. § 6-1-1309(2).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
19. Transparency obligations	Must inform the individual of the object of the "file", the use which will be made of the information, the categories of persons in the enterprise who will have access to it, the place where the file will be kept, and of the rights of access and rectification. Information must be in simple and clear terms and set out in particular: • the purposes for the collection (and name of 3rd party for whom the information is being collected, if applicable); • the means of collection; • the rights of access and rectification; • their right to withdraw their consent; • the possibility the information may be disclosed outside Québec; and • certain information and means relating to the use of a technology that includes functions allowing the identification, localization or profiling of individuals.	An organization must make readily available to individuals specific information about its policies and practices relating to the management of PI. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable. The information made available shall include: • the name or title, and the address, of the person accountable for the organization's policies and practices and to whom complaints or inquiries can be made; • the means of gaining access to PI held by the organization; • a description of the type of PI held by the organization, including a general account of its use; • a copy of any brochures or other information that explain the organization's policies, standards, or codes; and • what PI is made available to related organizations (e.g., subsidiaries).	An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfil its obligations. The organization must make the following information accessible: • a description of the type of PI under its control; • a general explanation of the uses of PI, including reliance on any applicable the exceptions to obtaining consent; • a general explanation of how it uses automated decision making systems to make predictions, recommendations or decisions that could have a significant impact on individuals; and • whether or not it engages in interprovincial or international transfers or disclosures of PI that may have a reasonably foreseeable impact on privacy • how to make a request for access or withdraw consent; • contact information of the individual to whom inquiries and complaints may be directed.	Yes. Notice must be provided at or before the point of collection of categories of PI to be collected, along with additional information. Consumers also have a right to request certain information. External notices, such as privacy policies, must also be updated with certain required information.	Yes. Notice must be provided at or before the point of collection of categories of PI to be collected, along with additional information. Sensitive PI is also included in these notices. Consumers also have a right to request certain information. External notices, such as privacy policies, must also be updated with certain required information.	Yes. Express notice and privacy policy requirements.	• Accessibility / Readability Requirements. Privacy notice must be "reasonably accessible", "clear" and "meaningful".[21] • Disclosure Requirements. The Privacy notice must list: (1) the categories of personal data collected or processed by the controller; (2) the purpose for processing personal data; (3) how consumers may exercise their rights, including the appeals process; (4) the categories of personal data that the controller shares with third parties, if any; and (5) the categories of third parties, if any, with whom the controller shares personal data.[22] • Sale / Targeting Advertising Disclosure. If the controller sells personal data to third parties or processes personal data for targeted advertising, the controller must "clearly and conspicuously" disclose such processing, as well as the manner in which a consumer may opt-out.[23] • Submission Process. The controller must establish and describe one or more secure and reliable means for consumers to submit a request to exercise their rights. The means selected must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication, and the ability of the controller to identify the consumer. Controllers shall not require a consumer to create a new account in order to exercise their rights, but may require the use of an existing account.[24]

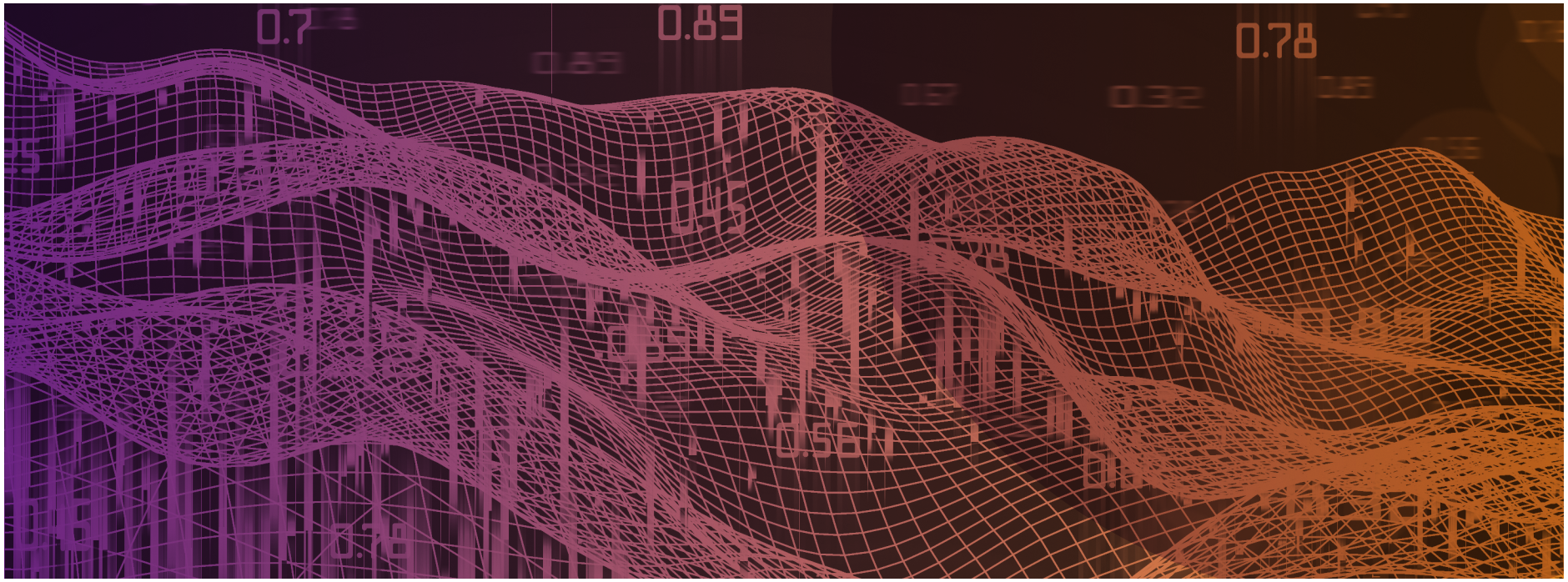
[21] Colo. Rev. St. § 6-1-1308(a).
[22] Colo. Rev. St. § 6-1-1308(a)(I)-(V).
[23] Colo. Rev. St. § 6-1-1308(b).
[24] Colo. Rev. St. § 6-1-1306(1).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
20. Security measures required	Must implement security measures that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.	An organization must protect PI through physical, organizational and technological security safeguards. The protection must be proportionate to the sensitivity of the information. Must protect against (among other things), loss or theft and unauthorized access, disclosure, copying, use or modification.	An organization must protect PI through physical, organizational and technological security safeguards. The protection must be proportionate to the sensitivity of the information. The organization must, in establishing its security safeguards, take into account the quantity, distribution, format and method of storage of the information. Must protect against (among other things), loss or theft and unauthorized access, disclosure, copying, use or modification. In the case of de-identified information, the measures applied to de-identify it must be proportionate to the purpose for which the information is de-identified and the sensitivity of the PI.	Yes. Private right of action in the event of a lack of "reasonable" security.	Yes. Private right of action in the event of a lack of "reasonable" security. Affirmative obligation to implement "reasonable" security.	Yes. Controller must establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data. The practices must be appropriate to the volume and nature of the personal data at issue.	Express Requirement. A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition. The data security practices must be appropriate to the volume, scope, and nature of the personal data processed and the nature of the business.[25]
Privacy Breaches							
21. Breach reporting	If the breach presents a risk of serious injury, it must be reported to the CAI.	If the breach of security safeguards presents a" real risk of significant harm" to the individual, a report must be given to the OPC.	If the breach of security safeguards presents a" real risk of significant harm" to the individual, a report must be given to the OPC.	No.	No.	No.	No. Subject to additional data breach laws.
22. Breach notification	If the breach presents a risk of serious injury, a notification to concerned individuals must be made. However, a person whose PI is concerned by the incident. need not be notified so long as doing so could hamper an investigation conducted by a person or body responsible by law for the prevention, detection or repression of crime or statutory offences (s. 3.5).	Unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual's PI under the organization's control if it is reasonable in the circumstances to believe. that the breach creates a real risk of significant harm to the individual. Must also notify 3rd parties if it believes that the other organization may be able to reduce the risk of harm or mitigate that harm.	Unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual's PI under the organization's control if it is reasonable in the circumstances to believe. that the breach creates a real risk of significant harm to the individual. Must also notify 3rd parties if it believes that the other organization may be able to reduce the risk of harm or mitigate that harm.	No. Subject to additional data breach laws.	No. Subject to additional data breach laws.	No. Subject to additional data breach laws.	No. Subject to additional data breach laws.

[25] Colo. Rev. St. § 6-1-1308(5).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
Data Transfers							
23. Transfer to foreign jurisdictions	Before communicating personal information outside Québec, a person carrying on an enterprise must conduct an assessment of privacy-related factors, taking into account: (1) the sensitivity of the information; (2) the purposes for which it is to be used; (3) the protection measures, including contractual ones, that would apply to it; and (4) the legal framework applicable in the State in which the information would be communicated, including the data protection principles applicable in the foreign State. The information may be communicated if the assessment establishes that it would receive adequate protection in compliance with generally accepted data protection principles. The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment. The same applies where the person carrying on an enterprise entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on its behalf. Exceptions to the above for emergencies.	A transfer (whether within or outside Canada) is a use for which no additional consent is required. The organization must ensure, by contract or other means, that the receiving party provides a comparable level of protection for the PI.	Transfer to service providers can be done without the individual's knowledge or consent. The organization must ensure, by a contract, that the service provider provides substantially the same protection for the PI.	No restrictions subject to notice and other requirements.	No restrictions subject to notice and other requirements.	No restrictions subject to notice and other requirements.	No. subject to notice and other requirements.

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
Data Retention							
24. Retention of information	No retention times established (though other applicable laws may have them). PI may be retained for such time as is necessary for the purposes identified or to allow the individual concerned to exhaust the recourses provided by law. Must ensure that any file held on an individual is up to date and accurate when used by an enterprise to make a decision in relation to the individual concerned. The information used to make such a decision is kept for at least one year.	No retention times established by PIPEDA (though other applicable laws may have them). Unless otherwise provided by law, information may be retained for as long as required to fulfill the purposes for which the information was collected, used or disclosed, or to fulfill legal requirements. An organization that uses PI to make a decision about an individual must retain the information for a sufficient period of time to permit the individual to make a request for access.	No retention times established by CPPA (though other applicable laws may have them). Unless otherwise provided by law, information may be retained for as long as required to fulfill the purposes for which the information was collected, used or disclosed, or to fulfill legal requirements. An organization that uses PI to make a decision about an individual must retain the information for a sufficient period of time to permit the individual to make a request for access.	Yes. Certain limited data retention requirements around data subject requests.	Yes. A business's retention of PI shall be reasonably necessary and proportionate to achieve the purposes for which the PI was collected or processed, or for another disclosed purpose that is compatible with the context in which the PI was collected, and not further processed in a manner that is incompatible with those purposes. Additional retention requirements relate to data subject requests.	Yes. Personal data may not be retained except as what's otherwise adequate, relevant, and limited to what is necessary in relation to the specific purposes for which the data was collected.	Collection Limitation. Controller shall limit the collection of personal data to only that which is adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed.[26]



[26] Colo. Rev. St. § 6-1-1308(3).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
Enforcement/Penalties							
25. Statutory penalties	Bill 64 contains provisions for administrative monetary penalties and penal sanctions. The maximum penal sanction for natural persons $100,000, while the initial maximum penal sanction for businesses is $25,000,000 or 4% of their worldwide turnover as of the last financial exercise, if the latter is greater. These penal sanctions can be doubled in the case of a repeat offender. The maximum amount of administrative monetary penalty is $50,000 for a natural person and, for all other persons, $10,000,000 or 2% of their worldwide turnover, if the latter is greater.	None directly. OPC may go to court and obtain up to $10,000 (summary conviction) or $100,000 (indictable offence), when an individual obstructs the investigation of a complaint or an audit or fails to comply with breach notification provision.	OPC may enter into compliance agreements with the organization. OPC can make a recommendation for a penalty if it finds, after an inquiry, that an organization does not comply with the CPPA. Due diligence defense available. The Tribunal considers OPC penalty, taking into account: • the nature and scope of the contravention; • whether the organization has voluntarily paid compensation to a person affected by the contravention; • the organization's history of compliance with the CPPA; and • any other relevant factor. The organization can be guilty of an indictable offence for contravention of certain sections the CPPA or interfering with the OPC's investigation, inquiry or audit. For indictable offence, could be liable to a maximal fine of $25M or 5% or the organization's gross global revenue for the preceding financial year. For summary conviction could be liable to a fine not exceeding the higher of $20M or 4% or the organization's gross global revenue for the preceding financial year.	Yes. In a private right of action, plaintiffs may seek the award of actual damages or a statutory damage of $750 per consumer. In an enforcement action, the California AG may impose penalties between $2,500 to $7,500 for violations.	Yes. In a private right of action, plaintiffs may seek the award of actual damages or a statutory damage of $750 per consumer. In an enforcement action, the CPPA may impose penalties between $2,500 to $7,500 for violations.	Yes. Virginia AG may initiate an action to seek civil penalties of up to $7,500 for each violation.	The Colorado Attorney General and District Attorneys have exclusive authority to enforce the CPA.[27] Prior to bringing an enforcement action, the Attorney General or District Attorney must issue a notice of violation to the controller if a cure is possible. If the controller fails to cure the violation within 60 days, an action may be brought. This cure period requirement expires on 1/1/25.[28]
26. Private right of action	No.	No.	Individual has a private right of action against an organization for damages for loss or injury if the OPC has made a finding of contravention which is not appealed or the Tribunal has made such a finding or the organization has been convicted of an offence.	Yes. Limited to instances where certain PI is subject to a data breach resulting from the business failing to maintain "reasonable" security around that data. Class liability, and potential to seek actual damages or up to $750 per consumer.	Yes. Limited to instances where certain PI is subject to a data breach resulting from the business failing to maintain "reasonable" security around that data. Class liability, and potential to seek actual damages or up to $750 per consumer.	No.	No.[29]

[27] Colo. Rev. St. § 6-1-1311(1)(a).
[28] Colo. Rev. St. § 6-1-1311(1)(d).
[29] Colo. Rev. St. § 6-1-1311(1)(b).

	Québec (Bill 64 - assented to Sept 22, 2021)*	Canada - PIPEDA (current)	Canada - Proposed PIPEDA changes (Bill C-11 - now defunct, with new Bill pending)**	California - CCPA	California - CPRA***	Virginia - CDPA****	Colorado Privacy Act
27. Other remedies	Additional remedies available from the CAI. Remedies available from the courts (which include class action). Punitive damages available where infringement is intentional or results from a gross fault.	Additional remedies available from the OPC. Remedies available from the courts (which include class action).	Additional remedies available from the OPC.	Yes. The California AG may seek the imposition penalties between $2,500 and $7,500 per violation.	Yes. The California AG may seek civil enforcement. The CPPA may seek the imposition penalties between $2,500 and $7,500 per violation.	Yes. Virginia AG may seek injunctive relief, and may recover reasonable expenses incurred in investigating and preparing the case, including attorney fees, in any action initiated under the CDPA.	The Colorado Attorney General and/or District Attorneys may seek penalties and/or injunctive relief.

* This column reflects the changes that have been introduced by Bill 64 but are not yet in effect. The majority of the provisions will come into force two years after the date of royal assent, with a few provisions coming into force in one year (e.g., appointment of privacy officer, breach reporting, right to disclose personal information without knowledge or consent in context of a business transaction or research).
**It is widely expected than any new Bill introduced will look very similar to the changes proposed by Bill C-11.
***CPRA is still undergoing regulatory review, and may be subject to additional changes as reflected in adopted regulations and/or legislative amendments.
****The CDPA may undergo regulatory changes between now and when it takes effect on Jan. 1, 2023.

For further information please contact:

Kirsten Thompson
Toronto
D +1 416 863 4362
kirsten.thompson@dentons.com

Kirsten Thompson is a partner at Dentons in Toronto and leads the Transformative Technologies and Data Strategy group, which focuses on privacy, cybersecurity and data management. Kirsten's practice has a particular concentration in data-driven industries and disruptive technologies, and she is a leading practitioner in areas such as Fintech, digital identity, Open Data/Open Banking, vehicle telematics and connected devices and infrastructure, Big Data/data analytics applications and enterprise data strategy.

Peter Stockburger
San Diego
D +1 619 595 8018
peter.stockburger@dentons.com

Peter Stockburger is a partner at Dentons in San Diego and is a member of the Firm's global Employment and Data Privacy & Cybersecurity Groups. His practice focuses on the unique intersection between cybersecurity, data privacy, employment law and complex litigation. Peter regularly advises clients on a range of cutting-edge legal issues, including global data privacy compliance, cybersecurity resiliency and preparedness, trade secrets, and privacy and security litigation. Peter is a frequent speaker and author in the areas of privacy, cybersecurity, and employment law, including with groups such as the NATO Cooperative Cyber Defence Centre of Excellence in Tallin, Estonia and the US Cyber Institute at West Point.

CSBrand-60801-BD-Targeting-Guide_14 — 25/10/2021