Overview of Quebec's *Regulation respecting the anonymization of personal information*	
Title	*Regulation respecting the anonymization of personal information* (the "**Regulation**")
Date of Entry into Force	The Regulation came into force on May 30, 2024, with the exception of the record-keeping requirements (s. 9), which came into force on January 1, 2025.
Enabling Statute	*Act respecting the protection of personal information in the private sector* (the "**Quebec Privacy Act**"), per ss. 23 and 90(3.2): **23.** Where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy the information, or anonymize it to use it for serious and legitimate purposes, subject to any preservation period provided for by an Act. For the purposes of this Act, information concerning a natural person is anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly. Information anonymized under this Act must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation. […] **90(3.2).** The Government, after obtaining the advice of the Commission, may make regulations to […] for the purposes of section 23, determine the criteria and terms applicable to the anonymization of personal information;
Scope and Application	• Due to the language used in the enabling provisions at ss. 23 and 90(3.2) of the Quebec Privacy Act, there is some uncertainty as to the precise scope and application of the Regulation – i.e., whether the requirements apply whenever an organization anonymizes personal information or only when an organization anonymizes personal information as a means of satisfying its destruction obligations. • Based on previous commentary from the Quebec privacy regulatory authority, the Commission d'accès à l'information (the "**CAI**"), it is foreseeable that the CAI will take the position that the Regulation applies to the anonymization of personal information in every instance, despite that ss. 23 and 90(3.2) suggest a narrower scope. • Many organizations will find that several of the requirements in the Regulation are already met as part of their existing anonymization practices, whereas others (most notably the requirement to identify and document the purpose(s) for using

Overview of Quebec's *Regulation respecting the anonymization of personal information*	
	anonymized information) are unique to the Quebec Privacy Act and may require certain changes or enhancements to the organization's anonymization practices and/or documentation of same.
Penal and Regulatory Sanctions	• While there are no specific penalties or fines for failure to meet the requirements under the Regulation, an organization's non-compliance with the requirements increases the risk of the CAI concluding that the information has not been effectively anonymized and, as such, remains personal information that is subject to the full scope of the Quebec Privacy Act. On that basis, the CAI could determine that the organization used, communicated or retained personal information without lawful authority or otherwise in contravention of the Act and is subject to an administrative monetary penalty or penal fine (Quebec Privacy Act, ss. 90.1(2), 91(1)). • Separately, the use of anonymized information to identify or attempt to identify an individual is an offence (Quebec Privacy Act, s. 91(5)). • Such contraventions could give rise to significant administrative monetary penalties (the greater of $10 million or 2% of worldwide turnover for the preceding fiscal year) or penal fines (the greater of $25 million or 4% of worldwide turnover for the preceding fiscal year) (Quebec Privacy Act, ss. 90.12 and 91(1)). Fines are doubled for subsequent offences (Quebec Privacy Act, s. 92.1)).

Definition of "Anonymized" Information
• Under the Quebec Privacy Act, personal information is anonymized if it is "at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly" (Quebec Privacy Act, s. 23). • Personal information must be anonymized according to "generally accepted best practices" and according to criteria and terms determined by regulation (Quebec Privacy Act, s. 23). • Section 7 of the Regulation clarifies that it is not necessary to demonstrate that there is zero risk of re-identifying a person in order for information to be considered "anonymized"; rather, the residual risk of re-identification must be "very low". • The definition under the Quebec Privacy Act generally aligns with the GDPR and the proposed definition of "anonymize" in Canada's Bill C-27 (which would, if passed, substantially amend PIPEDA).

Anonymization Requirements	
Identify the Purpose(s) for Using Anonymized Information	• Before anonymizing personal information, the organization must identify the "serious and legitimate" purpose(s) for which it intends to use the anonymized information (Quebec Privacy Act, s. 23 and Regulation, s. 3). • This obligation is unique to the Quebec Privacy Act and has no known analog across Canadian or foreign privacy laws. Typically, there are no statutory restrictions on the use of information that has been anonymized, as it is no longer governed by privacy laws. • The term "serious and legitimate" is not defined under the Quebec Privacy Act. However, in the context of *collecting* personal information (Quebec Privacy Act, s. 4), the CAI has considered a purpose to be "serious and legitimate" when it is "legitimate, significant and real" and where the invasion of privacy is "proportionate to the objectives pursued," taking into account, among other things, the sensitivity of the information, the lawfulness of the purpose, and its compliance with law, justice and fairness (e.g., see PIPEDA Findings #2021-001, paras. 71-73; 1023158-S, paras. 96-107). • It is conceivable that the CAI will apply a similar standard when assessing the seriousness and legitimacy of an organization's purposes for *anonymizing* personal information, though key elements of this standard (e.g., sensitivity, impact on privacy) would be inapplicable to anonymized information. Conceptually (and consistent with privacy statutory regimes globally), information that has been anonymized is no longer personal information and its use has no impact on the privacy of the individuals whose personal information was used to generate the anonymous dataset.
Involve a "Person Qualified in the Field" to Supervise	• The organization must ensure that the anonymization process is supervised by a "person qualified in the field", which is not a defined concept in the Regulation or the Quebec Privacy Act (Regulation, s. 4).
Remove Direct Identifiers	• The organization must first remove all personal information that directly identifies individuals (i.e., direct identifiers, such as name, contact information, government ID numbers) from the dataset it wishes to anonymize (Regulation, s. 5).

Conduct Preliminary Re-identification Risk Analysis	• Once all direct identifiers are removed from the dataset, the organization must conduct a preliminary assessment of the risk of re-identification, considering, *inter alia*:
	  ○ the extent to which it remains possible to (i) connect datasets concerning the same person, (ii) isolate or distinguish an individual within the dataset or (iii) infer information about a unique individual from other available information; and
	  ○ the risk of public or other reasonably available information being used in combination with the de-identified information to identify an individual. (Regulation, s. 5)

Anonymization Requirements	
Implement Anonymization Techniques and Security Measures	• Based on the identified risks in the preliminary analysis, the organization must develop and implement anonymization techniques that are consistent with generally accepted best practices, as well as reasonable protection and security measures to reduce the risk of re-identification (Regulation, s. 6).
Conduct Post-Implementation Re-identification Risk Analysis	• Once the anonymization techniques and measures have been implemented, the organization must conduct another assessment of the risk of re-identification of the dataset to show that it is "at all times, reasonably foreseeable in the circumstances" that the information "irreversibly no longer allows the person to be identified directly or indirectly" (Regulation, s. 7). • The analysis must show that the residual risks of re-identification are "very low" (but not zero risk), taking into account the following elements: ○ the purposes and circumstances of anonymization; ○ the nature of the information; ○ the inability to (i) connect datasets concerning to the same person, (ii) isolate or distinguish an individual within the dataset or (iii) infer information about a unique individual from other available information; ○ the risk of public or other reasonably available information being used to identify the individual; and ○ the effort, resources, and expertise required to re-identify the individual. (Regulation, s. 7)
Periodically Update Re-identification Risk Analysis	• After the information is anonymized, the organization must periodically update the risk analysis to ensure the residual risk of re-identification remains "very low", taking into account technological advancements (Regulation, s. 8).
Maintain a Record	• The organization must record the following in a "register": ○ A description of the information that was anonymized; ○ The purposes for which the organization intends to use anonymized information; ○ The anonymization techniques and measures that were implemented; and ○ The date(s) on which the original risk analysis, and, as applicable, any periodic re-assessments, were completed. (Regulation, s. 9) • Neither the Regulation nor the Quebec Privacy Act specifies the retention period applicable to this register.