DENTONS

Service provider management checklist for an accountable organization

Grow | Protect | Operate | Finance

- *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5 ("**PIPEDA**")
- *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 ("**ARPPIPS**")
- *Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* ("**CPPA**")
- Commission d'accès à information ("CAI") *Notice of Consultation: Guidelines on the Criteria for Valid Consent* ("**Draft Consent Guidelines**")

#	Risk assessment description	Considerations under Canadian data privacy laws
1.	**Sensitivity of the information and the nature of consent**	To the extent that a service provider is instructed to collect personal information from individuals on behalf of an organization, consider how and when consent should be obtained from the individual in the context of the sensitivity of information being collected: ☐ Implied consent ☐ Express consent **PIPEDA:** in determining the form of consent to use,organizations must take into account the sensitivity of the information. Organizations must generally obtain express consent when the information being collected, used or disclosed is sensitive. **ARPPIPS:** states that consent need only be express when sensitive information (a) will be used for a secondary purpose (s. 12); or where the personal information will be communicated to a third party unless ARPPIPS otherwise provides for such communication (e.g., exception to consent) (s. 13). The Draft Consent Guidelines go further and state that "[t]he use or disclosure of sensitive information must be authorized by express consent" (para. 31). **CPPA:** Express consent must be obtained prior to collecting, using, or disclosing sensitive personal information.

2.	**Appropriate contractual protections**	In each service provider agreement, consider: ☐ Specifying standard of care and obligations with respect to the treatment of personal information. ☐ Address any results of due diligence findings. ☐ Any specific legal requirements, particularly in the context of cross border sharing of personal information. ☐ Oversight of security measures and audit rights. ☐ Training and education for all service provider employees with access to personal information. ☐ Return or destruction of personal information and certification of compliance. ☐ Privacy provisions in contracts setting out requirements for compliance including binding the service provider to the policies and protocols of the organization and requiring the organization to be notified in the event of a breach. ☐ Cooperation clause for data subject access requests where information will be in the possession of the service provider. ☐ Requirement for service providers to track and record information disposal requests, all breaches of security safeguards. ☐ Data residency requirements (service provider to keep personal information in certain jurisdiction(s) and is prohibited from transferring it elsewhere without prior written permission).

© 2023 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.

3.	**Physical and information security requirements**	☐ Completion of a security questionnaire (best practice). ☐ Limit service provider's ability to disclose or transfer personal information to third parties without customer's prior written consent. Disclosures should be subject to confidentiality obligations. ☐ Security breach procedures in the event of a breach of security safeguard (or "confidentiality incident" in Quebec). Clarify who will notify/report breaches. ☐ Assistance in the completion of a data transfer impact assessment (required in Quebec for the transfer of personal information outside of Québec). **CPPA:** as currently drafted, every organization must implement and maintain a privacy management program. Unlike PIPEDA, the CPPA would require service providers to, as soon as feasible, notify the controlling organization if "any breach of security safeguards has occurred that involves personal information". **ARPPIPS:** imposes notification obligations on "enterprises", which includes both controllers and service providers (s. 3.5).
4.	**Collection of children's information**	Children's personal information is likely to be designated as sensitive personal information (guidance from the OPC states that children's information is always sensitive, although PIPEDA does not expressly state this) thereby requiring express consent. The CPPA specifically designates the information of minors to be sensitive information and require express consent of a parent or guardian. ARPPIPS requires express consent of a parent or guardian. ☐ Consider how express consent will be obtained from a parent or guardian. ☐ Consider age-gating sites if children's personal information is not intentionally being collected, used or disclosed. **CPPA:** as currently drafted, contains enhanced rights of disposal with respect to children's information- consider whether technical solutions can be implemented to ensure that personal information from children can be easily segmented and retrieved. **NOTE:** in a letter published on October 3, 2023, the Minister of ISED proposed amendments to the CPPA that would further enhance children's privacy.

© 2023 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.

5.	**Automated decision making**	☐ Is automated decision making being used to make decisions about Quebec residents? If so, ARPPIPS requires that any decisions being made by automatic decision making be disclosed, with an individual having a right to learn more about how that decision was made. **CPPA:** as currently drafted, an organization using an automated decision system must provide an explanation of the system's prediction, recommendation or decision regarding an individual, the circumstances in which such an explanation must be provided are limited to those where there could be a significant impact on the individual. Service providers providing these technologies must provide this relevant information. ☐ Include contractual assurances and protections (representation and warranty) that the service provider will not use information for any other purpose (including for AI purposes) and would require written permission to do so.

Contact us

To learn more about how Dentons can help you and your business, please reach out to **Kirsten Thompson** and **Danielle Dudelzak.**

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

Danielle Dudelzak
Associate, Calgary
+1 403 268 6312
danielle.dudelzak@dentons.com

© 2023 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.