CI– 032M
C.P. – PL 64
Protection des renseignements personnels

Le 28 septembre, 2020

Mme Louisette Cameron
Édifice Pamphile-Le May
1035, rue des Parlementaires
3e étage
Québec (Québec) G1A 1A3

RE: Projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Chère Mme Cameron, chers membres de la Commission des institutions,

Les entreprises, les organisations et les citoyens doivent avoir la certitude que les produits et les services qui leur sont fournis et dont ils se servent sont sûrs, sécurisés, fiables et ne porteront pas atteinte à la vie privée. De plus, les risques en matière de cybersécurité sont plus élevés que jamais. Les consommateurs sont de plus en plus conscients des atteintes à la protection des données et des menaces qui pèsent sur leurs renseignements personnels. En conséquence, les consommateurs s'attendent à ce que les organisations prennent des mesures concrètes pour protéger leurs données.

La soumission de la Chambre de commerce du Canada portant sur le projet de loi n° 64 est composée de deux parties. La première partie évoque des principes généraux pour favoriser la protection des renseignements personnels tout en assurant un cadre législatif qui crée un environnement favorable aux entreprises et qui contribue à l'essor de l'économie québécoise. La deuxième partie comporte des recommandations plus précises afin de rencontrer les objectifs de protection des renseignements personnels et de maintenir un environnement économique favorable. Bien que la Chambre de commerce du Canada représente les entreprises au niveau national, elle compte de nombreux membres au Québec et elle travaille de concert avec et appuie fortement les perspectives de ses collègues à la Fédération des chambres de commerce du Québec.

La protection des renseignements personnels et des données est essentielle dans notre économie moderne - souvent appelée « économie numérique », où les Québécois et les Canadiens accèdent constamment à des services numériques dans le cadre de leur travail, pour rester en contact avec leurs amis et leur famille, se procurer des biens, effectuer des transactions financières, recevoir des soins de santé virtuels, apprendre en ligne, ou entreprendre des activités de loisirs. Les entreprises de toutes tailles et de tous les secteurs s'appuient également sur les technologies numériques pour pénétrer de nouveaux marchés et gérer efficacement leurs activités, surtout avec la nouvelle réalité du télétravail pour plusieurs travailleurs.

La collaboration continue entre l'industrie et les gouvernements sur les cadres de protection de la vie privée est essentielle pour garantir que nous disposions de solides protections de la vie privée et que nous soutenions en même temps l'innovation et la compétitivité. Si nous n'y parvenons pas, nous risquons de faire peser un lourd fardeau sur les entreprises, en particulier les PME, et de priver les consommateurs des dernières technologies et des nouveaux services novateurs, deux facteurs qui entraveraient la croissance économique et la prospérité du Québec.

Alors que le gouvernement du Québec et les parlementaires poursuivent l'étude projet de loi n° 64, trois principes clés sont essentiels à une approche qui augmenterait la protection des renseignements personnels tout en favorisant l'innovation et l'essor de l'économie québécoise:

Trouver l'équilibre entre protection des données et l'innovation

Comme soulevé par la FCCQ dans son mémoire, le Québec se présente comme un leader au Canada avec ce projet de loi et la Chambre de commerce du Canada salue ces efforts tout en soulevant l'enjeu important pour le Québec de ne pas s'isoler du reste du Canada ou de ses partenaires internationaux. Les cadres de protection des renseignements personnels doivent être interopérables les uns avec les autres afin que les entreprises puissent exercer leurs activités de façon transparente au-delà des frontières internationales et provinciales/territoriales, en plus de permettre au Québec de demeurer une destination de premier choix pour les investissements étrangers. Ces efforts d'interopérabilité des cadres législatifs et règlementaires contribuent à un environnement économique favorable pour les entreprises et les consommateurs.

Si les cadres législatifs en matière de vie privée et de protection des renseignements personnels manquent d'interopérabilité d'une juridiction à l'autre, cela crée des obstacles pour les entreprises. Ces difficultés pourraient également entraîner le départ d'entreprises d'un marché donné en plus d'entraîner le risque de diminutions des investissements étrangers. Cela crée des désagréments pour les consommateurs et réduit la résilience des entreprises. Par ailleurs, les limites ou les différences dans les règles relatives aux transferts transfrontaliers de données pourraient empêcher les entreprises et les citoyens du Québec d'utiliser de nombreux produits et services disponibles sur le marché, y compris l'infrastructure infonuagique, les solutions de commerce en ligne, les plates-formes de paiement en ligne, et les outils de marketing et de relations avec la clientèle. Un niveau accru d'interopérabilité avec les autres marchés avec lesquels transigent les entreprises du Québec maintiendrait la compétitivité et permettrait le rayonnement de l'économie du Québec.

Mettre l'accent sur les principes

Les règles de protection de la vie privée et des renseignements personnels doivent être fondées sur des principes et axées sur les résultats, plutôt que d'être prescriptives dans les moyens. Cela permettra au cadre de protection des renseignements personnels de s'adapter à l'évolution de l'environnement économique et de fonctionner dans le cadre des réalités opérationnelles et des risques spécifiques au contexte. Il sera également bénéfique à l'évolution des habitudes et des préférences des consommateurs sans qu'il soit nécessaire d'introduire à plusieurs reprises des modifications législatives en fonction des circonstances.

Neutralité sur le plan technologique

Se concentrer sur les résultats signifie également que les règles de protection des renseignements personnels restent neutres sur le plan technologique et sectoriel. Cette approche permet de soutenir les entreprises dans une gamme de secteurs ayant des modèles économiques différents. C'est particulièrement important compte tenu de l'évolution rapide des technologies en matière de services que les entreprises fournissent à leurs clients, et de la demande d'interconnectivité des Québécois.

Afin d'appuyer les parlementaires dans leur étude portant sur le projet de loi n° 64, les recommandations en deuxième partie sont humblement présentées.

Si vous avez des questions, n'hésitez pas à communiquer avec nous.

Veuillez agréer, chère Mme Cameron, chers membres de la Commission des institutions, l'expression de nos sentiments distingués.

Ulrike Bahr-Gadalia
Directrice principale - Économie numérique, technologie & innovation

&

Mark Agnew
Directeur principal, Politiques internationales

Part II – Specific Recommendations Related to Bill 64

The Quebec Privacy Private Sector Act, while a leading example when adopted in 1994, must now be modernized considering the current technological and international environment. Bill 64 presents an opportunity to modernize Quebec's privacy regime in several respects:

(i) strike a better balance between individuals' privacy rights and the commercial needs of organizations;
(ii) ensure interoperability with data protection laws across the world, including to facilitate data transfer with other jurisdictions; and
(iii) guarantee greater flexibility for digital and innovation-focused enterprises.

However, Bill 64 in its current form is not achieving these objectives as well as it could do. Instead, some provisions are stringent, lack nuance and are unique to Quebec. Our members have expressed concerns that Bill 64 would lead to uncoordinated privacy requirements between Quebec and other provinces, which would create operational challenges and adverse impacts on Quebecers.

Specific areas of concern include Bill 64's implications on equivalency and consent. These and selected other key areas of concerns are discussed below in more detail. However, to provide context for the broader extent of our concerns, here are several examples of the obligations imposed on enterprises by the Bill 64 that diverge significantly from certain international and domestic privacy laws:

- Requirement to establish, implement and publish governance policies and practices with no consideration of the relevance of these documents for individuals or the proprietary nature of their content to an organization;
- Imposing a new privacy officer role that would rest with CEOs by default regardless of the nature and/or amount of personal data processed;
- Mandating requirements for automated processing of personal information with no limitation depending on the effect and/or the nature of the decision concerned;
- Retention of personal information at least one year when used to make a decision instead of relying on the necessity of the personal information; and

- New sanctions seemingly more onerous than the GDPR and less proportional depending on the nature of the breach, with no procedural safeguards.

Collectively, these potential measures might adversely impact the competitiveness of Quebec-based enterprises, reduce the appetite of domestic and foreign enterprises to do business in the province of Quebec, diminish the products and services offered to Quebec consumers, and adversely impact innovation. While Bill 64 needs to ensure a balance between individuals and organizations, coordination with federal and provincial laws, as well as those of foreign jurisdictions is critical for consumers and businesses as noted in our comments below.

1.Cross border data flows and equivalency

Issue

The proposed amendments through Section 17 and 17.1 require an entity seeking to transfer personal information outside of Quebec to conduct a privacy assessment, including an assessment of the legal framework of the receiving State. If the receiving State does not have an equivalent legal framework protecting privacy, the personal information cannot be transferred. This exposes several considerations:

- Requiring equivalency creates a significant new hurdle for Quebec companies, particularly SMEs, thereby reducing consumer choice as well as the ability of Quebec businesses to compete and innovate.
- Requiring equivalency risks violating trade agreement provisions on cross-border data flows and not requiring local computing facilities as a condition of doing business.
- Requiring equivalency may also render Quebec businesses unable to leverage highly specialized or secure service providers in other jurisdictions, including cloud service providers that can assist in deploying data protections such as encryption.
- Depending on the sector, some organizations may not be able to comply with the equivalency requirement due to certain international regulations or obligations to share with regulators outside of Quebec (e.g., anti-money laundering regulations in other Canadian or international jurisdictions).
- Quebec should seek to align with federal legislation requiring businesses to use contractual or other means to provide a comparable level of protection to personal information that is transferred to service providers for processing.
- If the equivalency requirement is retained, alternative mechanisms must be introduced for transferring personal information outside Quebec to non-equivalent jurisdictions to align with international best practice. The GDPR has an adequacy process and alternative methods for transfers to States without adequacy, such as Standard Contractual Clauses.

Background

The proposed amendments to Section 17 and 17.1 requiring a privacy impact assessment are intended to require companies to exercise due diligence before transferring personal information out of Quebec. As drafted, the provisions create uncertainty for businesses. Companies will incur significant costs as they carry out individual assessments for every jurisdiction to which they may transfer personal information. The EU experience with regulator equivalency determinations suggests this method will provide very limited relief. The significant concerns raised following the recent “Schrems II” decision, mandating that every cross border data transfer be assessed on a case-by-case basis, underscores the

impracticality of this approach. If businesses operating in Quebec cannot easily engage in cross-border data transfers, investment, innovation and competition will likely decrease to the detriment of consumer choice and the quality of certain goods and services (e.g., engagement with world class service providers may be difficult to engage).

The proposed equivalency requirement has no alternative mechanism enabling the transfer of data if a company determines the jurisdiction outside Quebec does not provide equivalent privacy protections. Many businesses operating in Quebec rely on third-party outsourcing, including to other provinces. Data flows play a key role for businesses expanding into new markets. The absence of an alternative mechanism will hurt Quebec-based companies and may deter other companies from operating in the province. Bill-64 should include well-established alternative mechanisms for protecting personal information transferred to non-equivalent jurisdictions.

Furthermore, the proposed equivalency requirement may violate Canada's obligations on cross-border data transfers under the CPTPP and CUSMA trade agreements. The absence of an alternative to equivalency could be interpreted as unduly restricting the movement of data for a business purpose contrary to CPTPP Article 14.11 and CUSMA Article 19.11. The equivalency requirement may also be a de facto requirement for companies to maintain computing facilities within Quebec as a condition of doing business, which would violate Article 14.13 and 19.12 of the CPTPP and CUSMA, respectively.

Members have expressed concern that there is a lack of clarity on how many of the requirements would be applied on businesses based outside of Quebec. Further consultation between federal and provincial privacy regulators and stakeholders should be undertaken to ensure these impacts are understood and to avoid unintended adverse effects on organizations and Quebec individuals.

Recommended Change

Remove binding language from Section 17 and allow for contractual measures as an alternative to equivalency as a legal authority for transferring personal information out of Quebec. Additionally, remove provisions related to the Minister publishing an equivalency list.

2.Outsourcing

Issue

Bill-64 does not currently clarify that in an outsourcing or similar agency relationship, the service provider does not hold the same privacy accountabilities as the principal (i.e., "a person carrying out an enterprise"). Unless this is clarified, there may be undue and unreasonable privacy expectations on the service provider (e.g., providing rights of access) that truly belong to the principal.

Background

Article 18.3 implicitly recognizes the distinct roles and responsibilities that various organizations play in the data ecosystem. Accountability rests with the organization that ultimately controls what personal information is collected, how it is used and for what purposes, with whom it is shared, and how it is processed. Bill-64 implicitly limits the obligations of the agent who provides services to the person carrying on an enterprise (referred to as "a person or body carrying out a mandate or performing a contract of enterprise or for services") to the obligations found in article 18.3.

Recommended Change

To avoid any confusion about the responsibilities of the parties, we recommend adding the following provision to Bill-64:

> "*18.3(3) For the purpose of this Act, a person or body carrying out a mandate or performing a contract of enterprise or for services on behalf of a person carrying out an enterprise is not deemed to be a person carrying out an enterprise*."

3.Consent (alternatives to consent, exceptions to consent)

Issue

Bill 64 introduces several changes to the consent framework for personal information. These clarifications reduce the burden on business processes and better reflect the expectations of consumers. Unfortunately, the Bill also introduces other impractical consent obligations that will have the unintended consequence of creating "consent-fatigue" in consumers and reduce the real value of consent as a privacy safeguard.

Business supports the proposed exceptions to the consent requirement for a) transferring personal information to an agent for processing (s. 18.3), b) secondary uses and enterprise analytics where the use is consistent with the original consent (s. 12(1)), c) when the use is clearly in the individual's best interest (s. 12(2)), d) a business transaction (s.18.4) , and also the exclusion of business contact information from the definition of personal information that will trigger the consent obligation (s.1). However, consideration should be given to additional exceptions to consent or legal authorities for processing personal data, as is (1) proposed by ISED in their PIPEDA amendments paper[1], and (2) in the GDPR where consent is one of six lawful and valid bases for processing of personal data.

Bill-64 should also clarify that implied consent is sufficient where it is reasonable in the circumstances, including the sensitivity of the information.

Background

The language around the use of appropriate forms of consent in Bill-64 is ambiguous. For example, the Bill appears to require express consent in virtually all instances where personal information is used or transferred to a third party as a result of ss. 12 and 13. Section 14 states that consent must be clear, free, informed, given for specific purposes and must be requested for each such purpose, in clear and simple language and separately from any other information provided to the person concerned. These requirements may be disproportionate in many circumstances. The broad scope of the language is inconsistent with the important role played by implied consent. The limited alternatives or common exceptions to consent create an unnecessary burden on business.

Instead, it would be preferable to be less prescriptive and not require opt-in consent for all secondary purposes and to permit implied consent in some circumstances, particularly when the personal information at question is less sensitive. This approach permits a contextual analysis of how secondary purposes should be treated and strikes an appropriate balance between the privacy rights

[1] https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

of the individual and the needs of businesses to collect, use, and disclose information for purposes that a reasonable person would find appropriate in the circumstances.

Recommended Changes

> *14. When explicit consent is appropriate under this Act, such consent 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 separately from any other information provided to the person concerned~~. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested.*
>
> *The consent of a minor under 14 years of age is given by the person having parental authority.*
> *.*
> *The consent of a minor 14 years of age or over is given by the minor or by the person having parental authority.*
>
> *~~Consent is valid only for the time necessary to achieve the purposes for which it was requested.~~*
> *~~Consent not given in accordance with this Act is without effect.~~*

4.Exception to consent for employment personal information

Issue

Bill-64 lacks an exception to the consent requirement for employee personal information. Such an exception would allow employers to collect, use and disclose personal information that is necessary for establishing, managing or terminating an employment relationship, without requiring the employee's consent.

Background:

Bill 64 does not include an employee consent exception. This is problematic since the consent model is ill-suited to employer/employee relationships. It is difficult to think of an employee's consent in dealing with their employer as being "free," since an employee could well believe, rightly or wrongly, that their employment would be jeopardized by a refusal to consent. If an employee refused their employer's collecting, using or disclosing of their personal information for normal employment purposes, this could prevent the employer from continuing its activities and fulfilling its legal obligations. Such an observation is not a novel one and has been made, in particular, by the Federal Court of Appeal.[2]

Under PIPA (BC) and PIPA (Alberta), employers may, without the consent of their employees, collect, use and disclose personal information that is necessary for establishing, managing or terminating an employment relationship.[3] Employers have the duty to inform employees, in advance, that their personal information will be or might be collected, used or disclosed for such purposes.[4] Under

---

2 See *Wansink v. TELUS Communications Inc.*, 2007 FCA 21.

3 *PIPEDA*, sect. 7.3; PIPA (BC) sects. 13, 16 and 19; PIPA (Alberta), sects. 15, 18, 21.

4 *PIPEDA*, sect. 7.3; PIPA (BC) subsects. 13(3), 16(3) and 19(3); PIPA (Alberta), paras. 15(1)(c), 18(c) and 21(c).

PIPEDA, a change to adopt a similar exception to consent for employment purposes was made in a recent amendment following a legislative review.

In the EU, it is accepted that consent cannot be "freely" given by employees, since there is an imbalance of power in their relationship with their employers.[5] An employer may process their employees' personal data using a non-consent basis in GDPR, such as where the processing is necessary either for the performance of the employment contract, to comply with the employer's legal obligations, or in the context of its "legitimate interests."[6]

Recommended Change

The following exemption should be added to Bill-64:

> Any person may collect, use and disclose personal information without the consent of the individual if
>
> > (a) the collection, use or disclosure is necessary to establish, manage or terminate an employment relationship between the person, enterprise or business and the individual; and
> > (b) the person, enterprise or business has informed the individual that the personal information will be or may be collected, used or disclosed for those purposes.

5.De-identified information:

Background

Section 23 of the amendments notes that personal information is de-identified, when it is "irreversibly no longer allows the person to be identified directly or indirectly". This is a very high standard to meet and does not appropriately take in account the manner in which personal information can currently be de-identified and protected, through the use of technology (example, through the use of tokens, hashing, etc.). These types of technological tools allow for only parties with the tool to de-identify to do so. The parties that do not have access to the tools cannot re-identify the data, and thus the personal information remains only accessible to the initial party that collected the data prior to de-identification. It is our view that simply because the party with the "key" may re-identify the data (usually due to contractual obligations) should not categorize the entire data set as data that can be re-identified.

Recommended Change

It is critical to ensure that we avoid having different definitions across Canada at the federal and provincial levels for de-identified given the consumer risks and operational complexities it can present. Quebec should seek to coordinate with ongoing initiatives federally and provincially.

6.Enforcement

Issue

---

[5] Article 29 Date of Protection Working Party, Guidelines on consent under regulation 2016/679, November 2017, online: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051>, (revised and adopted April 10, 2018, under the GDPR).

[6] GDPR, art. 6: see *supra* Part 2(a) of this article.

Bill-64 creates sweeping new penalties and rights of action that are disproportionate and lack appropriate procedural safeguards. These measures must be modified to balance the protection of privacy with reasonable levels of liability. The significant penalties are complicated by the ambiguities in Bill 64's provisions and obligation to apply some requirements to all situations regardless of level of risk. For instance, the equivalency requirement creates great uncertainty for organizations (e.g., if a State deemed equivalent is later determined by the Quebec government to not be equivalent).

Background

The enforcement measures proposed by Bill-64 include fines of up to $25,000,000, or, if greater, the amount corresponding to 4 per cent of worldwide turnover for the preceding fiscal year (s. 91). For subsequent offence, the fines would be doubled. The Bill also sets out administrative monetary penalties (AMPs) of up to $10,000,000 or 2% of worldwide turnover for preceding fiscal year if greater (s. 90.12). In addition, the Bill proposes an onerous private right of action (PRA) with no-fault liability.

Business is very concerned that the maximum range for fines and AMPs are excessive and will result in fines and AMPs being sought that are disproportionate to the circumstances of specific cases. Companies may be reluctant to enter the Quebec market (which may be a small portion of their overall business) if it could result in fines and AMPs calculated on the entity's worldwide turnover. If the maximum quantum for AMPs is maintained, rigorous procedural safeguards will be necessary for AMPs processes.

The proposal to introduce a PRA is flawed. The current drafting imposes no-fault liability. Liability attaches unless the underlying event was impossible to foresee and avoid. There is no due diligence defence or other defence set out in the proposed regime. An entity that acted reasonably and responsibly, taking all possible precautions to manage personal information in a secure and compliant manner could still incur liability. This is a real possibility in an era of rapidly evolving technology threats. This strict level of liability for privacy is unprecedented and creates an unreasonable burden for businesses operating in Quebec.

Recommended Changes

The enforcement and penalty provisions should be re-considered and re-drafted. It is recommended that:

- The use of a percentage of worldwide turnover to calculate possible fines and AMPs be eliminated.
- The maximum fixed figure for fines and AMPs should be reviewed and reduced.
- The PRA should not be implemented until it is clear that the use of fines and AMPs is not sufficient and the enforcement benefit of implementing PRAs outweighs the impact on businesses.
- Any PRA should allow for all reasonable defences at law, including the exercise of due diligence.
- Given the unprecedented levels of fines there needs to be a procedural mechanisms to ensure fairness (e.g. right to understand allegations, right to retain counsel, impartial hearings, right to challenge findings).

7.Data portability

Issue

Although data portability provides certain advantages to both consumers and businesses, it comes with inherent risks to consumer protection, privacy and confidentiality, and cybersecurity.

Background

Over and above the existing right for individuals to ask for access to the personal information that businesses hold about them, data portability allows individuals to obtain their personal information and to transfer it with their informed consent between organizations. Data portability can enhance individual autonomy, privacy and consumer choice if implemented properly. However, there are many practical challenges. If these challenges are not addressed in a detailed manner, the impacts on individuals can include reduced security, increased risk of fraud and a negative customer experience. A robust architecture to support data portability is necessary and may vary between different sectors. The government should pursue a phased approach to data portability as infrastructure and frameworks develop.

Data portability right should be limited in scope and include clear rules around requests for transfers and related accountabilities. Furthermore, data covered by the right should be limited to personal information held by the organization in digital format that the individual has provided to the organization and certain data (e.g. transactions) created through interaction with products and services. The right should not apply to other forms of data that may be proprietary, including derived or enriched data, de-identified information or data that is not conducive to data portability.

Careful thought has to be given to avoiding data breaches and facilitating fraud, the appropriate level of authentication for data (possibly linked to the sensitivity of the data) and to ensure adherence to appropriate information security standards. The appropriate format for individuals to receive their data should also be determined and should align with national, international or sector standards. The Act should set out the bases on which an organization can object to a request for data portability.

Recommended Change

Bill 64's data portability provisions should include an ability for individuals to request and receive their personal information in a digital format from an organization within a reasonable timeframe. Additionally, individuals should be allowed to ask for an organization to transfer data to a third party, provided both entities are subject to a sector-specific framework. There also need to be clear guardrails in place to provide exclusions for proprietary information, as well as data that has been anonymized, de-identified, or derived.

In the development of follow-on sector specific frameworks, there needs to be a close collaboration between industry and regulators that will: identify any specific technical or competitive considerations; ensure security standards and privacy controls are in place; specify how authenticate consent; define the scope of personal information within the request as well as exclusions; and identify accountabilities across the stages of the data transfer cycle.

The right itself should be introduced in a coordinated manner to maximize any benefits and limit confusion and unnecessary complexity. This needs to be augmented by greater convergence of the definitions that will ultimately also provide enhanced flexibility and reduced risks for consumers. Key to achieving this convergence will strong collaboration between industry and government.

8.Security / Confidentiality by default

Issue

Bill-64 contains measures that are intended to maximize the security and privacy of personal information, often known as security by default and privacy by default, in sections such as 3.1, 3.2 and 9.1. However, these measures are inconsistently expressed and may have negative impacts on consumers if applied without regard to the circumstances, risks or sensitivity of the personal information.

Background

Bill 64 requires organizations to "protect personal information held by a person" (s. 3.1), and establish and implement governance policies and practices that "ensure" the protection of such information. (s. 3.2). The information security standards in sections 3.1, 3.2 and 9.1 are inconsistent with the qualified requirements set out in section 10 of the Act which provides that organizations 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." (s. 10).

PIPEDA, PIPA AB and PIPA BC qualify the information security safeguarding obligations on organizations by obligating organizations to implement safeguarding measures that are "reasonable" and "appropriate" in the circumstances. (PIPEDA, Principle 4.1; PIPA AB s. 34; PIPA BC, s. 34). Similarly, the GDPR's standard for safeguarding requires "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." (Art.5(1)). Bill 64 should follow a similar approach.

Business strongly supports a flexible approach to the security requirement, so that the level of security and related costs and processes are proportionate to the sensitivity of the personal information and context of the relationship.

Bill 64 also requires organizations that collect personal information when "offering a technological product or service must ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned." (s. 9.1). This "confidentiality by default" clause is far broader in scope and significantly more stringent than the "privacy by design" concept under the GDPR, which requires the data controller to implement "appropriate technical and organizational measures" for implementing data protection principles in an effective manner, taking into account the nature, scope, context, risks and purposes of processing. (Art. 25(1)). Similarly, GDPR requires data controllers to implement "appropriate" technical and organizational measures to ensure that by default, "only personal data which are necessary for each specific purpose of the processing are processed" (Art. 25(2)).

Business supports a flexible approach to the confidentiality requirement, so that the level of confidentiality and related costs and processes are proportionate to the sensitivity of the personal information and context of the relationship. A strict application of the confidentiality requirement could lead to poor consumer experiences. Many devices and services are programmed to be "smart" to anticipate the consumer's needs accessing information necessary to provide the services the consumer expects. Consequently, the confidentiality provision could require all services and devices to be pre-set to maximum confidentiality at the outset, requiring time-consuming programming by consumers to make the services and devices operate as the consumer intends.

Another example of where the highest level of confidentiality may apply is the selection of an individual's password whereby the entry of the password is masked, encrypted and not visible to

anyone other than the user; to apply this standard to all other online applications (e.g., an online survey that does not include sensitive personal information), is not practical.

Recommended Change
Modify Bill 64 Section 9.1 to align with the concepts of “privacy by design” that are well understood both domestically and globally, which take into account the nature, scope, context, risks and purposes of processing.

9. Privacy Impact Assessment Requirements for Projects

Issue

Section 3.3 requires a privacy impact assessment to be undertaken at the outset of all projects involving the collection, use, communication, keeping or destruction of personal information.

Background
Bill 64 requirements relating to Privacy Impact Assessments exceed that of GDPR, which are mandatory only whenever a processing operation is likely to result in a high risk to the rights and freedoms of individuals. Bill 64 requires an impact assessment for “any information system project or electronic service delivery project involving the collection, use, communication, keeping or destruction of personal information” but does not have a risk threshold to exempt projects with low or minimal risk. The requirement for a privacy impact assessment in such a broad manner will impose a significant administrative burden on companies to execute. This burden would be acutely felt by small and medium size enterprises that lack the resources to undertake this task thoroughly and comprehensively, but would also affect large organizations that manage thousands of projects annually, many with minimal risk. The legislation currently has no lower limit for what would trigger an assessment.

Recommended Change

In order to avoid systematic DPIAs for all product launches in Québec, we advise considering introduction of a threshold for conducting such assessment such as the risk of serious injury in relation to the right to the respect of reputation or privacy of the individuals.