CI– 025M
C.P. – PL 64
Protection des renseignements personnels
VERSION RÉVISÉE

Soumission à la Commission des institutions de l'Assemblée nationale sur les modifications proposées au Projet de loi 64 modernisant des dispositions législatives en matière de protection des renseignements personnels

29 septembre 2020

Sommaire

En tant que porte-parole de la profession du marketing, l'Association canadienne du marketing (« ACM ») apprécie l'occasion qui lui est offerte de faire part de ses commentaires au gouvernement du Québec sur les modifications proposées par le Projet de loi 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.

Dans notre économie numérique moderne, les consommateurs attendent de plus en plus des organisations qu'elles fournissent les produits et services intuitifs qu'ils souhaitent et dont ils ont besoin. La Loi sur la protection des renseignements personnels dans le secteur privé (la Loi), aujourd'hui et à l'avenir, doit englober les nombreux avantages économiques et sociaux de l'utilisation des données pour les Québécois tout en protégeant leur vie privée. Il doit y avoir un mécanisme d'alignement du Québec sur les initiatives de réforme de la protection de la vie privée en cours dans tout le pays afin d'éviter une complexité inutile pour les consommateurs et les entreprises, et de prévenir les complications pour le commerce interprovincial et international, et les investissements étrangers directs au Québec.

Pendant que l'Assemblée nationale examine les dispositions du Projet de loi 64, l'ACM est heureuse de formuler les recommandations suivantes :

1. La loi du Québec sur la protection des renseignements personnels doit être souple, neutre sur le plan technologique et proportionnée aux objectifs à atteindre en matière de protection de la vie privée. La loi québécoise sur la protection de la vie privée devrait être fondée sur des principes souples face à l'évolution rapide des technologies, des modèles commerciaux et des attentes des consommateurs en matière de protection de la vie privée. Elle doit être proportionnée aux objectifs de protection de la vie privée, sans créer de complexité excessive pour les consommateurs, les entreprises et le gouvernement.

2. Il doit y avoir un mécanisme de coordination avec les autres cadres de protection de la vie privée au Canada afin d'éviter une complexité excessive pour les entreprises et les consommateurs, ainsi que des obstacles au commerce et aux investissements étrangers au Québec. Plus expressément, il devrait y avoir un alignement raisonnable avec les réformes prévues de la loi fédérale sur la protection de la vie privée et les documents électroniques (LPRPDE), car des différences importantes entre les deux lois auront un impact négatif sur les entreprises et les citoyens du Québec.

3. Les exigences relatives aux transferts de données transfrontaliers doivent inclure des alternatives prouvées et réalisables à l'adéquation, telles que des clauses contractuelles types.

4. La responsabilité de l'externalisation devrait être confiée à l'organisation principale, en obligeant les fournisseurs de services à respecter les exigences fixées par cette dernière.

5. Le type de consentement requis doit être basé sur une évaluation des facteurs pertinents, en réservant le consentement explicite pour le moment où il est vraiment significatif. La Loi devrait reconnaître le rôle important joué par le consentement implicite au service des consommateurs et des entreprises, ou elle pourrait sinon prévoir un consentement explicite pour des « objectifs légitimes », permettant aux organisations de justifier leurs objectifs légitimes par des évaluations internes et de les identifier auprès des individus.

6. Les mesures d'application devraient être revues et réduites afin d'encourager la conformité sans avoir un effet dissuasif sur les entreprises et les investissements au Québec. En particulier, l'application des amendes doit être basée sur des facteurs particuliers en utilisant une approche

proportionnée qui tient compte de la nature de la violation, de la taille et des activités de traitement des données de l'organisation qui a commis la violation.

7. Une transparence raisonnable devrait être exigée en ce qui concerne le profilage et les décisions fondées uniquement sur un traitement automatisé. Les réponses réglementaires devraient être correctives, en interdisant ou en limitant uniquement les activités pour lesquelles il existe des preuves évidentes de préjudice.

8. L'exception de consentement pour les renseignements dépersonnalisés devrait être élargie, à condition que certaines normes de dépersonnalisation soient respectées. La Loi devrait en outre autoriser la collecte, l'utilisation et la divulgation de renseignements dépersonnalisés sans consentement à toutes fins raisonnables, si certaines normes sont élaborées et respectées.

9. Les mesures d'autorégulation devraient être encouragées et incitées pour assurer l'efficacité de la réglementation. Les codes volontaires, les certifications et autres normes (telles que le Code de déontologie et des normes de pratique) jouent un rôle important en complétant la législation sur la protection de la vie privée. Le gouvernement devrait encourager les certifications et les codes autorégulés comme des outils de respect et de responsabilité des renseignements personnels, et devrait encourager davantage leur utilisation en en sélectionnant certains pour une reconnaissance formelle.

10. Le droit à la portabilité des données devrait être reporté jusqu'à ce que ses impacts plus larges soient compris. La portabilité des données crée de nouveaux risques sérieux liés à la fraude, à la vie privée et à la sécurité, et ses impacts plus larges sur l'économie et la concurrence ne sont pas bien compris**.** Elle ne devrait être réalisée que par une approche progressive qui permet la mise en œuvre de cadres sectoriels spécifiques.

Introduction et contexte

L'Association canadienne du marketing (« ACM ») apprécie l'occasion qui lui est offerte de faire part de ses commentaires au gouvernement du Québec sur les modifications proposées par le Projet de loi 64 à la Loi sur la protection des renseignements personnels dans le secteur privé du Québec.

L'AMC est la voix de la profession du marketing et représente plus de 50 entreprises, organisations à but non lucratif, organismes publics et établissements d'enseignement supérieur. Nous nous sommes engagés à aider les organisations à maintenir des normes élevées de conduite et de transparence grâce à notre Code de déontologie et des normes du pratique obligatoire et à nos ressources en matière de protection de la vie privée et des données pour les spécialistes du marketing et les consommateurs. En tant que leader reconnu et de longue date en matière d'autorégulation du marketing, nous nous efforçons de garantir un environnement où les consommateurs sont protégés et les entreprises peuvent prospérer.

La communauté marketing du Québec accorde une grande importance à ses clients, dont la loyauté et la confiance constituent le fondement du succès des entreprises. La plupart des organisations reconnaissent que de solides pratiques de protection de la vie privée et des données constituent un avantage concurrentiel et une stratégie de fidélisation des clients, et elles s'efforcent de protéger les renseignements personnels des individus qu'elles servent. La collaboration entre le gouvernement et l'industrie est essentielle pour garantir que le cadre de protection de la vie privée du Québec repose sur un équilibre entre l'acceptation des nombreux avantages économiques et sociaux de l'utilisation des données et la protection de la vie privée des individus.

Le Québec a été la première juridiction nord-américaine à adopter une loi sur la protection de la vie privée régissant les activités commerciales. La modernisation de la loi québécoise sur la protection de la vie privée est une étape importante pour garantir que le Québec continue à être un champion de la protection de la vie privée, en trouvant un équilibre entre les attentes des consommateurs en matière de protection de la vie privée et l'exploitation des données pour soutenir la croissance économique et l'innovation. Nous apprécions les efforts de réforme en cours à l'Assemblée nationale et nous croyons que le Québec a une opportunité importante de rechercher une solution pratique pour les consommateurs et les entreprises.

La coordination avec d'autres cadres de protection de la vie privée au Canada est essentielle pour assurer le succès des organisations opérant au Québec, pour le bien des citoyens québécois qui apprécient la gamme de produits et de services qui leur sont offerts. Il doit y avoir un mécanisme d'alignement sur les initiatives de réforme de la protection de la vie privée en cours dans tout le pays afin de garantir que les entreprises puissent opérer sans heurts au-delà des frontières internationales et provinciales, et de s'assurer que le Québec reste une destination attrayante pour les investissements étrangers directs. Si ces approches ne sont pas alignées, cela créera un ensemble disparate de législation sur la protection de la vie privée, ce qui entraînera une complexité et des obstacles inutiles pour les entreprises, et des perturbations pour les consommateurs. Elle réduira également l'attrait du Québec comme destination d'affaires pour les entreprises d'autres pays et provinces, ce qui aura un impact négatif sur l'économie et le choix des consommateurs québécois.

La communauté du marketing soutient de nombreuses améliorations proposées dans le Projet de loi 64, notamment de nouvelles exceptions de consentement pour la recherche et la vente de transactions commerciales, et l'exclusion des coordonnées commerciales de la définition des renseignements personnels. D'autres aspects du Projet de loi 64 doivent être examinés de plus près par l'Assemblée nationale afin de s'assurer que le cadre de protection de la vie privée du Québec atteint son double objectif de protection des consommateurs tout en soutenant l'innovation et la compétitivité

responsables, et d'éviter les problèmes qui se sont posés dans des juridictions régies par des lois de protection des données plus normatives, inspirées par l'UE.

Alors que l'Assemblée nationale examine les dispositions du Projet de loi 64, l'ACM est heureuse de formuler les recommandations suivantes.

Recommandations

1. La loi québécoise sur la protection de la vie privée doit être souple, neutre sur le plan technologique et proportionnée aux objectifs à atteindre en matière de protection de la vie privée.

Les données constituent la base de l'économie numérique. Elles permettent une meilleure prise de décision et le développement de nouvelles technologies importantes, comme l'intelligence artificielle (IA), un domaine dans lequel le Québec est un leader mondial.

La capacité des organisations à recueillir, utiliser et communiquer des renseignements personnels est essentielle pour offrir de la valeur aux consommateurs et pour assurer l'innovation et la compétitivité du Québec. Il est important que la loi québécoise sur la protection de la vie privée demeure adaptable à un environnement commercial en évolution et fonctionne selon des réalités opérationnelles et des risques propres au contexte. Cela est particulièrement important pour les petites et moyennes entreprises (PME) afin que la mise en conformité ne soit pas indûment onéreuse.

La loi québécoise sur la protection de la vie privée doit reposer sur des principes qui peuvent être appliqués de façon réfléchie à toutes les technologies et à tous les modèles commerciaux, afin qu'elle demeure pertinente. Le Projet de loi 64 fait un pas important pour s'éloigner des concepts statiques et dépassés tels que les « fichiers ». Un nouvel examen de la Loi devrait garantir qu'il ne reste aucune disposition particulière à une technologie qui ne résisterait pas à l'épreuve du temps.

Il est également important que la Loi tienne compte de l'évolution des attentes et des préférences des consommateurs**,** sans qu'il soit nécessaire d'introduire à plusieurs reprises des modifications législatives pour rester dans l'air du temps.

Les progrès technologiques ont donné aux organisations la souplesse nécessaire pour proposer des offres pertinentes et utiles aux consommateurs. En conséquence, les consommateurs exigent une rapidité et une qualité d'information bien plus grandes que jamais pour utiliser les services fournis par les entreprises et pour prendre des décisions d'achat en connaissance de cause. Une forte majorité de consommateurs (76 %) est prête à partager des données personnelles afin de recevoir des avantages, à condition que les données soient correctement protégées[1]. De nombreux consommateurs, y compris les jeunes générations, reconnaissent que l'échange de données est de plus en plus fondamental pour accéder aux nombreux services bénéfiques avec lesquels ils interagissent quotidiennement.

Elle doit être proportionnée aux objectifs de protection de la vie privée, sans créer de complexité excessive pour les consommateurs, les entreprises et les pouvoirs publics. La législation sur la protection de la vie privée doit être fondée sur des principes solides qui permettent aux organisations de tenir compte du contexte. La Loi doit être suffisamment souple pour imposer des mesures proportionnées aux intérêts de la vie privée en jeu et à l'attente raisonnable de l'individu en matière de vie privée dans les circonstances.

[1] Foresight Factory, 2018: Data Privacy Study: What the Canadian Consumer Really Thinks

Une loi réformée devrait inclure une nouvelle clause exigeant que la loi soit interprétée de manière proportionnée, raisonnable dans les circonstances. Nous recommandons d'apporter les modifications suivantes à la Loi :

> *La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil.*
>
> *Ces règles particulières doivent être appliquées d'une manière qui reconnaît le droit à la vie privée des individus en vertu du Code civil et la nécessité pour les organisations de recueillir, détenir, utiliser ou communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait appropriées dans les circonstances.*

2. Il doit y avoir un mécanisme de coordination avec les autres cadres de protection de la vie privée au Canada afin d'éviter une complexité excessive pour les entreprises et les consommateurs, ainsi que des obstacles au commerce et aux investissements étrangers au Québec.

Il doit y avoir un mécanisme d'alignement sur les initiatives de réforme de la protection de la vie privée en cours dans tout le pays afin de garantir que les entreprises puissent opérer sans heurts au-delà des frontières internationales et provinciales, et de s'assurer que le Québec reste une destination attrayante pour les investissements étrangers directs. Si ces approches ne sont pas alignées, cela créera une disparité de législations sur la protection de la vie privée, ce qui entraînera une complexité et des obstacles inutiles pour les entreprises, et des perturbations pour les consommateurs. Il doit y avoir un mécanisme de coordination entre les gouvernements fédéral, provinciaux et territoriaux afin d'éviter la fragmentation préjudiciable des cadres de protection de la vie privée, y compris les effets négatifs des barrières commerciales interprovinciales.

Plus expressément, il devrait y avoir un alignement raisonnable avec les réformes prévues de la loi fédérale sur la protection des renseignements personnels et des documents électroniques (LPRPDE), car des différences importantes entre les deux lois auront un impact négatif sur les entreprises, les consommateurs québécois et le gouvernement.

De nombreuses caractéristiques de la législation canadienne actuelle sur la protection de la vie privée, bien qu'elles doivent faire l'objet d'une mise à jour réfléchie, ont résisté à l'épreuve du temps, assurant la protection de la vie privée sans charge réglementaire inutile. Des lois plus récentes et plus prescriptives dans d'autres juridictions, y compris le Règlement général sur la protection des données (RGPD), n'ont pas encore fait leurs preuves à bien des égards et ont créé un fardeau réglementaire stupéfiant pour le gouvernement et les entreprises. Un cadre de protection de la vie privée ne doit pas être si onéreux qu'il ne puisse être mis en œuvre efficacement et qu'il ne soit pas bien compris par les non-spécialistes.

En ce qui concerne l'état d'adéquation de le RGPD, la réduction des frictions dans les transferts de données est un objectif valable. Toutefois, en envisageant l'adoption de certains aspects du RGPD, nous demandons instamment à l'Assemblée nationale d'évaluer chacun d'eux en fonction de son mérite dans le contexte québécois, l'objectif étant d'obtenir des résultats compatibles en matière de protection de la vie privée par opposition à des exigences législatives compatibles. Si les cadres canadiens de protection de la vie privée sont mieux alignés, cela permettrait de soutenir une décision positive sur le statut d'adéquation du RGPD qui s'appliquerait de manière plus complète dans toutes les juridictions du Canada, ce qui faciliterait le commerce et la concurrence pour les entreprises québécoises.

La loi québécoise sur la protection de la vie privée devrait être compatible avec les juridictions qui ont une approche similaire, fondée sur des principes, en matière de protection de la vie privée. Il est plus important que jamais que la Loi soit agile face à l'évolution rapide des technologies et des modèles commerciaux, permettant aux organisations de déterminer la manière la plus efficace de remplir leurs obligations communes. Les nuances -- le respect du contexte, les attentes des individus et l'accent général sur le caractère raisonnable -- doivent être maintenues.

3. Les exigences relatives aux transferts transfrontaliers de données doivent comprendre des alternatives prouvées et réalisables à l'adéquation.

Dans le monde interconnecté d'aujourd'hui, l'externalisation efficace et fiable des opérations de traitement des données à l'extérieur du Québec est cruciale pour le fonctionnement des entreprises québécoises et leur capacité à bien servir les consommateurs.

Le Projet de loi 64 propose des restrictions considérables pour les organisations qui cherchent à partager des renseignements avec des tiers situés à l'extérieur du Québec, ce qui complique les conditions d'efficacité, de croissance et de commerce des entreprises.

En vertu de cette disposition, les entreprises québécoises ne peuvent transférer des renseignements personnels qu'aux « États » dont le cadre juridique offre une protection de la vie privée équivalente à celle du Québec, dans le cadre d'une évaluation complète des incidences sur la vie privée. Cette disposition est préoccupante à plusieurs égards importants :

- L'exigence d'équivalence créerait des difficultés importantes pour les entreprises québécoises, en particulier les PME, alors qu'elles sont concurrentielles dans l'économie mondiale., Ces entreprises seront confrontées à une complexité, à des retards et à des coûts excessifs lorsqu'elles effectueront des évaluations individuelles pour chaque juridiction à laquelle elles peuvent transférer des renseignements personnels. Les préoccupations soulevées à la suite de la récente décision « Shrems II » en Europe, qui exige que tout transfert transfrontalier de données soit évalué au cas par cas, soulignent l'impraticabilité de cette approche.

- Les organisations basées au Québec, y compris les multinationales, peuvent décider de réduire ou de modifier leurs activités au détriment de l'économie québécoise, de la saine concurrence et du choix des consommateurs. À l'heure actuelle, le Projet de loi ne précise pas si un « État » inclurait d'autres provinces, ce qui créerait encore plus de complexité pour les entreprises québécoises, ainsi que pour les consommateurs qu'elles servent dans tout le Canada.

- La détermination et l'examen en cours du statut d'adéquation d'autres juridictions nécessiteront une attention et des ressources importantes de la part du gouvernement provincial, comme nous l'avons vu dans le cadre du RGPD de l'UE.

- L'exigence d'adéquation risque de violer les dispositions d'importants accords commerciaux concernant les flux de données transfrontaliers, notamment l'Accord global et progressif pour le partenariat transpacifique (CPTPP) et l'Accord Canada-États-Unis-Mexique (CUSMA) L'absence d'une alternative à l'équivalence pourrait être interprétée comme restreignant indûment la circulation des données à des fins commerciales, ce qui est contraire à l'article 14.11 du PTPGP et à l'article 19.11 de l'ACEUM. L'exigence d'équivalence peut également être une exigence de facto pour les entreprises de maintenir des installations informatiques au Québec comme condition pour faire des affaires et peut violer les articles 14.13 et 19.12 du PTPGP et de l'ACEUM, respectivement.

Nous demandons instamment au gouvernement de ne pas maintenir l'exigence d'adéquation. Si l'exigence d'adéquation est maintenue malgré les obstacles qu'elle crée, il doit y avoir des mécanismes alternatifs en place pour le transfert de renseignements personnels vers des juridictions qui ne sont pas jugées équivalentes. Comme nous l'avons appris de l'expérience d'autres juridictions, il existe des mécanismes alternatifs bien établis et juridiquement exécutoires.

Le RGPD, par exemple, est beaucoup plus souple et prévoit diverses bases légales autres que l'adéquation pour les transferts de données vers d'autres États, notamment si cela est nécessaire à l'exécution d'un contrat, ou si des clauses contractuelles types, des codes de conduite ou des règles d'entreprise contraignantes sont en place.

Étant donné la nature des flux de données, les obligations contractuelles actuelle entre les organisations constituent une forme efficace de gouvernance responsable des données.

Enfin, la Loi doit préciser quand ses dispositions ont un effet extraterritorial. Elle devrait indiquer clairement que ses dispositions s'appliquent à l'intérieur de la province de Québec et ne s'appliquent qu'aux entités ou activités à l'extérieur du Québec lorsqu'il existe un « lien réel et substantiel » avec la juridiction, comme l'exige la LPRPDE.

Nous recommandons d'apporter les modifications suivantes à la Loi :

> *17. Avant de communiquer à l'extérieur du Québec un renseignement personnel, la personne exploitant une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée. Elle doit notamment tenir compte des éléments suivants :*
> (1) la confidentialité des renseignements,
> (2) les fins auxquelles elles doivent être utilisées,
> *(3) les mesures de protection qui lui seraient applicables, y compris les mesures contractuelles.*
>
> *Les renseignements peuvent être communiqués si l'évaluation établit qu'ils recevraient un niveau de protection comparable par des mesures législatives, contractuelles ou autres à celles prévues par la présente loi.*
>
> Il en va de même lorsque la personne exploitant une entreprise confie à une personne ou à un organisme hors Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver ces renseignements pour son compte.
>
> Le présent article ne s'applique pas à la communication de renseignements en vertu du paragraphe 7 du premier alinéa de l'article 18.

4 La responsabilité de l'externalisation devrait être confiée à l'organisation principale

Nous soutenons le cadre du Projet de loi 64 pour le partage des renseignements personnels avec les fournisseurs de services dans le contexte des relations d'externalisation. Ce cadre représente la meilleure pratique en ce sens qu'il ne nécessite pas de consentement supplémentaire.

Afin de garantir une chaîne de responsabilité claire et cohérente, il est important que la Loi précise que l'organisation principale (c'est-à-dire « une personne exploitant une entreprise ») est seule responsable du respect de la législation sur la protection de la vie privée, tandis que le rôle du prestataire de

services (c'est-à-dire « une personne ou un organisme exécutant un mandat ou exécutant un contrat d'entreprise ou de services ») est de suivre les exigences fixées par l'organisation principale.

Les prestataires de services ont la responsabilité de protéger les renseignements personnels de manière adéquate, et ces responsabilités sont généralement définies dans le contrat. Du fait que l'organisation principale est le décideur ultime lorsqu'il s'agit d'engager un prestataire pour fournir un service, il est logique que l'organisation principale reste seule responsable du respect de la Loi.

Nous recommandons d'apporter les modifications suivantes à la Loi :

> *18.3(3) Aux fins de la présente loi, une personne ou un organisme exerçant un mandat ou exécutant un contrat d'entreprise ou de services pour le compte d'une personne exerçant une entreprise n'est pas considéré comme une personne exerçant une entreprise.*

5. Le type de consentement requis doit être basé sur une évaluation des facteurs pertinents, en réservant le consentement explicite pour le moment où il est vraiment significatif

Une confiance excessive dans le consentement explicite a contribué à la « lassitude du consentement » des consommateurs, qui sont moins enclins à examiner attentivement les avis de confidentialité, à prendre des décisions éclairées et à faire des choix. Il est mal adapté aux réalités des entreprises commerciales, au monde de plus en plus connecté dans lequel vivent les consommateurs et à l'évolution des attentes des consommateurs.

La demande de consentement explicite, le suivi du consentement et l'enregistrement du consentement pour des utilisations raisonnables et standard des données sont trop lourds pour les entreprises, sans avantage correspondant en matière de protection de la vie privée, et se traduisent souvent par une mauvaise expérience client.

Il est impératif que l'exigence d'un consentement exprès soit réservée aux choses qui comptent le plus, aux situations auxquelles on ne peut raisonnablement s'attendre et où les individus ont un choix valable.

Le Projet de loi 64 apporte plusieurs améliorations au modèle de consentement. La communauté du marketing soutient fortement les exceptions proposées à l'exigence de consentement pour :

- le transfert de renseignements personnels à un agent en vue de leur traitement,
- les utilisations secondaires et les analyses d'entreprise lorsque l'utilisation est conforme au consentement initial,
- lorsque l'utilisation est clairement dans le meilleur intérêt de l'individu, et
- dans le cas d'une transaction commerciale.

Nous soutenons également l'exclusion des coordonnées professionnelles de la définition des renseignements personnels qui déclenchent l'obligation de consentement.

Cependant, le libellé actuel du Projet de loi 64 concernant le consentement n'est pas clair. Le Projet de loi semble exiger le consentement dans presque toutes les circonstances où des renseignements personnels sont utilisés ou transférés à un tiers à la suite des articles 12 et 13. Le consentement doit être explicite lorsqu'il s'agit de renseignements personnels sensibles, ce qui semble impliquer qu'une autre forme de consentement peut être acceptable dans certaines circonstances impliquant des renseignements non sensibles.

Le Projet de loi stipule que le consentement doit être manifeste, libre, éclairé et « être donné à des fins spécifiques. Il est demandé à chacune de ces fins en termes simples et clairs, distinctement de tout autre renseignement communiqué à la personne concernée ». Ces exigences sont disproportionnées dans de nombreuses circonstances, et incompatibles avec le rôle important joué par le consentement implicite. En outre, il n'est pas clair si « séparément de tout autre renseignement fourni à la personne concernée » signifie en dehors du champ d'application d'une politique de protection de la vie privée.

Le Projet de loi 64 ne fait actuellement pas référence aux concepts de consentement explicite et implicite, contrairement à d'autres lois sur la protection de la vie privée au Canada, qui autorisent le consentement implicite dans certaines circonstances. La proposition de séparer le consentement à chaque fin des autres termes s'écarte considérablement des autres régimes de protection de la vie privée. La Loi devrait être modifiée pour reconnaître l'importance du consentement implicite, et devrait préciser que le consentement implicite est suffisant lorsqu'il est raisonnable dans les circonstances.

Une force de longue date des cadres canadiens de protection de la vie privée est que les organisations ont le choix opérationnel de demander un consentement explicite ou implicite. Cela garantit que la forme approprié de consentement dépend d'une évaluation de la sensibilité des informations et des attentes raisonnables de la personne, qui dépendront toutes deux du contexte.

En général, le consentement exprès (par exemple, l'option d'adhésion) doit être utilisé pour une collecte, une utilisation ou une divulgation qui implique généralement des renseignements sensibles, qui ne répond pas aux attentes raisonnables de l'individu ou qui crée un risque significatif de préjudice important. Le consentement implicite (par exemple, l'option de refus) doit être utilisé pour une collecte, une utilisation ou une divulgation qui implique généralement des renseignements non sensibles et des objectifs simples.

Nous demandons instamment au Québec d'adopter le même cadre pour le consentement implicite que celui sur lequel s'appuient le gouvernement fédéral et les autres provinces, tel que décrit dans les Lignes directrices pour l'obtention d'un consentement valable du Commissariat à la protection de la vie privée du Canada.

Nous recommandons d'apporter les modifications suivantes à la Loi :

14. Lorsque le consentement prévu à la présente loi est approprié, ce consentement doit être clair, libre et éclairé. Il doit être demandé dans un langage clair et simple

> Le consentement d'un mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale.
> .
> *Le consentement d'un mineur de 14 ans ou plus est donné par le mineur ou par le titulaire de l'autorité parentale.*

L'Assemblée nationale devrait prévoir des options supplémentaires au consentement explicite (par exemple, une exemption au consentement pour des « objectifs légitimes »). Le consentement explicite ne devrait pas être requis dans des situations où il n'est pas significatif ou approprié, comme dans le cas de renseignements personnels utilisées par des organisations à des fins légitimes qui prennent en compte les attentes raisonnables de l'individu dans les circonstances.

Les organisations qui se prévalent de cette exemption doivent faire preuve de transparence quant à leurs objectifs légitimes, en les précisant explicitement à l'avance et en les exposant dans une politique de confidentialité ou une autre méthode facilement accessible aux particuliers.

La Loi pourrait permettre l'élaboration de règlements pour préciser les objectifs légitimes autorisés ou les catégories d'objectifs légitimes et pour préciser quels renseignements doivent être explicitement spécifiées par les organisations avant que les renseignements ne soient utilisés.

Il est raisonnable d'attendre des organisations qui invoquent cette exemption qu'elles justifient leurs objectifs légitimes et les exposent clairement dans leurs politiques de protection de la vie privée et par la réalisation d'évaluations internes. L'évaluation devrait être basée sur le contexte et les circonstances spécifiques pour démontrer que le traitement est approprié et raisonnable.

6. Les mesures doivent être revues et réduites afin d'encourager la conformité sans avoir un effet dissuasif sur les entreprises et les investissements au Québec.

La grande majorité des organisations québécoises veulent protéger la vie privée de leurs clients. Elles ne veulent pas nuire à leur réputation et mettre en péril la confiance des consommateurs en utilisant à mauvais escient ou en traitant incorrectement les renseignements personnels. Nous sommes favorables à des mesures d'application renforcées pour offrir un recours efficace aux individus et pour sévir contre les acteurs malveillants. Toutefois, il est essentiel que ces mesures n'aient pas d'effet dissuasif sur les entreprises et leur capacité à bien servir les consommateurs.

Le Projet de loi 64 propose de nouvelles mesures d'application qui sont disproportionnées par rapport aux objectifs à atteindre en matière de protection de la vie privée et ne sont pas assorties de garanties procédurales suffisantes. Les sanctions doivent être suffisamment incitatives pour dissuader les entreprises qui pourraient autrement ne pas se conformer et doivent également être conçues pour éviter un environnement coûteux et litigieux, alors que des sanctions réduites pourraient être tout aussi efficaces.

Si des mesures d'application indûment strictes sont mises en place, certaines organisations jugeront nécessaire d'évaluer les risques, les coûts et les avantages de continuer à faire des affaires au Québec. Les mesures du Projet de loi 64 doivent être modifiées pour assurer une approche raisonnable de l'application de la Loi, avec un niveau de responsabilité qui incite à la conformité tout en favorisant un climat de collaboration et de confiance en matière de vie privée.

L'utilisation d'un pourcentage du chiffre d'affaires mondial pour calculer les éventuelles amendes[2] n'est pas recommandée, et si cette approche est retenue, il est important de réduire le montant maximum à un niveau plus raisonnable et proportionné. La fourchette proposée pour les amendes et les sanctions administratives pécuniaires entraînerait des amendes sans rapport avec l'impact réel de la plupart des infractions, et il est peu probable qu'elle puisse refléter correctement les circonstances de chaque cas. Cela rendrait les entreprises plus réticentes à entrer ou à demeurer sur le marché québécois, en particulier si le Québec ne représente qu'une petite partie de leur activité globale, par crainte d'être condamnées à une amende en pourcentage du chiffre d'affaires mondial.

Il doit y avoir des facteurs spécifiques à prendre en compte lors de l'application des amendes, en utilisant une approche proportionnée qui tient compte de la nature de la violation et de la taille et des activités de traitement des données de l'organisation qui a commis la violation. Les amendes devraient être

[2] Le Projet de loi 64 prévoit un régime pénal avec des amendes pouvant atteindre 25 000 000 $ (ou, si ce montant est supérieur, le montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice précédent), ce montant étant doublé pour les infractions suivantes. Le Projet de loi prévoit également des sanctions administratives pécuniaires (SAP) pour un large éventail d'infractions allant jusqu'à 10 000 000 $ (ou, si elles sont supérieures, 2 % du chiffre d'affaires mondial de l'exercice financier précédent). En outre, le Projet de loi propose un droit privé d'action avec responsabilité sans faute.

concentrées sur les cas les plus flagrants de préméditation et de négligence grave. Si la fourchette actuelle des sanctions administratives pécuniaires est maintenue, des garanties procédurales rigoureuses doivent être mises en place pour assurer l'équité.

Le Projet de loi 64 propose un nouveau droit privé d'action. Cela créerait des conditions qui favorisent les recours collectifs potentiellement opportunistes, en plus d'une exposition accrue des organisations aux réclamations liées à la vie privée, y compris les demandes de dommages-intérêts punitifs. Elle impose un niveau de responsabilité strict sans précédent en matière de respect de la vie privée, ce qui crée une charge disproportionnée pour les entreprises.

Le Projet de loi 64 établit une responsabilité à moins que l'événement sous-jacent n'ait été impossible à prévoir et à éviter. Le régime proposé ne prévoit aucun moyen de défense fondé sur la diligence raisonnable ou autre. Une organisation peut néanmoins engager sa responsabilité si elle agit de manière raisonnable et responsable, si elle informe à l'avance l'individu des risques possibles et si elle prend toutes les précautions possibles pour gérer les renseignements personnels de manière conforme.

Si le droit privé d'action est finalement appliqué, il ne doit être mis en œuvre qu'en dernier recours, une fois qu'il est clair que le recours aux amendes et aux sanctions administratives pécuniaires n'est pas suffisant. Il doit de plus permettre tous les moyens de défense raisonnables en droit, y compris l'exercice d'une diligence raisonnable.

7. Une transparence raisonnable devrait être exigée en ce qui concerne le profilage et les décisions fondées uniquement sur un traitement automatisé

Lorsqu'une organisation utilise des renseignements personnels pour prendre une décision fondée exclusivement sur un traitement automatisé, le Projet de loi 64 propose d'accorder aux individus le droit d'être informés au moment, ou avant, qu'une décision ne soit prise, y compris le droit d'être informés des éléments de renseignements personnels utilisés, des raisons et des principaux facteurs qui ont mené à la décision et le droit de faire corriger les renseignements les concernant. L'organisation serait également tenue d'autoriser la personne à présenter des observations en vue du réexamen de la décision.

Pour aider les individus à mieux comprendre comment les décisions sont prises à leur sujet, nous soutenons l'obligation pour les organisations de partager les sommaires (dans leurs politiques de confidentialité) avec les individus sur l'utilisation de la prise de décision automatisée, les facteurs impliqués dans la décision, et lorsque la décision a un impact. Ils ne doivent pas être tenus de révéler des informations, des algorithmes ou des procédures commerciaux de nature confidentielle ou exclusive.

Si les individus concernés soumettent des observations à l'organisation pour examen, celle-ci doit avoir le pouvoir discrétionnaire de déterminer si elle doit ou non modifier sa décision en dernier ressort. Ces décisions sont très nuancées, et un droit d'opposition à des décisions fondées uniquement sur un traitement automatisé serait très problématique.

Telle qu'elle est rédigée, l'obligation de notification est trop large, car elle serait applicable dans toutes les circonstances impliquant des décisions fondées sur un traitement automatisé, quelle que soit l'importance de l'impact de la décision sur l'individu.

Il est loin d'être clair que toutes les formes de prise de décision automatisée sont problématiques ou justifient une réponse réglementaire. En fait, la « prise de décision automatisée » comprend une série d'activités légitimes, telles qu'un site Web refusant de servir un contenu protégé par le droit d'auteur à un utilisateur résidant dans une juridiction où le fournisseur du site Web ne détient pas les droits pour rendre ce contenu disponible. Les données devenant de plus en plus complexes, l'utilisation de l'automatisation

est essentielle et bénéfique. Un nombre croissant de décisions automatisées utiles sont prises chaque jour, ce qui se traduit par des services avantageux pour les consommateurs, tels que les « robots conversationnels » qui fournissent aux consommateurs des conseils pertinents et personnalisés.

Les individus exigent des services plus rapides, plus faciles et plus intuitifs, et l'automatisation est essentielle à la réalisation de cette promesse. Il existe des cas où la prise de décision automatisée est liée à la prestation effective d'un service qu'un consommateur peut souhaiter ou dont il a besoin. Il doit être entendu que si un consommateur s'oppose à la prise de décision automatisée, il ne pourra pas accéder au service.

Le Projet de loi 64 exigerait également que les organisations qui recueillent des renseignements personnels au moyen d'une technologie ayant la capacité d'identifier, de localiser ou d'établir le profil d'un individu informent celui-ci de cette technologie et des moyens disponibles, le cas échéant, pour désactiver cette technologie.

Dans le cas du marketing, le profilage vise à fournir à un individu une expérience plus pertinente, par exemple si un produit ou un service est offert sur la base des préférences et des habitudes antérieures de l'individu.

De nombreuses organisations créent un profil ou utilisent un processus décisionnel automatisé afin de cibler leurs efforts de marketing, notamment par l'utilisation d'outils et de logiciels analytiques tiers, tels que les cookies, les pixels et les balises. Cela aide les organisations à fournir aux consommateurs les produits et services pertinents qu'ils souhaitent ou dont ils ont besoin.

Nous mettons en garde contre le modèle du RGPD, qui impose des restrictions aux décisions uniquement automatisées qui produisent des « effets légaux **ou** d'importance similaire », car il existe une incertitude importante pour les organisations dans l'évaluation des « effets d'importance similaire », ce qui freine l'innovation et entraîne une confusion dans l'industrie.

La transparence sera le facteur le plus important. Les organisations doivent être transparentes dans leurs politiques de protection de la vie privée quant à leur utilisation d'outils et de logiciels analytiques tiers pour suivre, identifier et cibler les individus afin de leur servir une publicité pertinente. Dans la mesure du possible, ils devraient également orienter les individus vers le mécanisme d'option de refus accessible via la plateforme du fournisseur de services.

8. L'exception de consentement pour les renseignements dépersonnalisés devrait être élargie, à condition que certaines normes de dépersonnalisation soient respectées

La dépersonnalisation et l'anonymisation sont parmi les mécanismes de protection de la vie privée les plus efficaces dont disposent les organisations pour s'engager dans l'analyse des données et l'innovation dans l'économie numérique.

Le Projet de loi 64 stipule que les renseignements personnels recueillis dans un but précis peuvent être utilisés, sans consentement, à des fins secondaires d'étude ou de recherche ou pour la production de statistiques, si les renseignements sont dépersonnalisés.

Comme l'exemption de consentement ne s'applique qu'à l'utilisation au sein de l'entreprise, les objectifs d'étude, de recherche et de production de statistiques peuvent être interprétés comme des analyses d'entreprise ou d'affaires. Cela devrait être clarifié dans la Loi.

Étant donné l'importance cruciale de la dépersonnalisation pour une innovation responsable, et afin d'éliminer toute incertitude juridique, la Loi devrait être modifiée pour permettre la collecte, l'utilisation et la divulgation de renseignements dépersonnalisés sans consentement à toutes fins raisonnables, si certaines normes sont respectées.

Pour garantir des conditions équitables et assurer la clarté, il est important que les organisations disposent d'un ensemble de normes communes leur permettant de démontrer qu'elles ont pris toutes les mesures raisonnables au moment de dépersonnaliser les renseignements personnels et atténuer le risque de réidentification. La norme de dépersonnalisation et de surveillance continue doit être adaptée au contexte, qui est plus pertinent que le « type » de données.

La Loi devrait reconnaître les normes officielles de l'industrie et inclure des points de référence pour les procédures techniques et administratives, la surveillance, ainsi que les évaluations des risques et les protocoles. La Loi devrait clarifier les paramètres de responsabilité concernant les transferts ultérieurs de données dépersonnalisées, et devrait souligner la nécessité de mettre en place des dispositions contractuelles entre les organisations pour traiter la réidentification.

À mesure que la technologie évolue, les exigences pour la réidentification devront également évoluer. Nous proposons que le gouvernement travaille avec l'industrie pour développer ces normes, ce qui pourrait aboutir à une certification formelle impliquant un tiers accréditeur approuvé par le Gouvernement du Québec (voir la recommandation 9 ci-dessous).

9. Les mesures d'autorégulation devraient être encouragées et incitées pour assurer l'efficacité de la réglementation

Tous les secteurs ont un rôle à jouer pour protéger la vie privée des Québécois. Un modèle de corégulation dans lequel la réglementation gouvernementale et l'autorégulation de l'industrie travaillent en tandem est important pour garantir l'efficacité de la réglementation. Il n'existe pas d'approche unique en matière de respect de la vie privée; tout dépend de chaque secteur et des types de renseignements collectés, utilisés et partagés. Aujourd'hui et à l'avenir, les codes, certifications et autres normes joueront un rôle important pour compléter la législation sur la protection de la vie privée.

Tous les régimes devraient être volontaires, en reconnaissant les différents degrés d'opérations de traitement des données parmi les organisations et en veillant à ce que les organisations disposant de ressources limitées ne soient pas indûment touchées. Les normes pourraient être soit autorégulées, soit officiellement reconnues par le gouvernement, comme indiqué ci-dessous :

A. **Normes auto-réglementées et codes :** Les normes et codes auto-réglementés devraient être mentionnés dans la Loi comme des outils pouvant aider les organisations à assurer la conformité et à démontrer leur responsabilité en cas d'enquête de la Commission d'accès à l'information du Québec. L'industrie devrait être encouragée à élaborer et à suivre ces normes et codes.

   Les codes de pratique auto-réglementés de l'industrie et des professionnels sont des outils pratiques et efficaces pour orienter le respect de la vie privée. Par exemple, le Code de déontologie et des normes de pratiqueest un code complet qui établit et encourage des normes élevées pour la conduite du marketing et renforce les connaissances des responsables du marketing en matière d'exigences de conformité. La section J du Code traite de la protection de la vie privée. Le Code est revu et mis à jour chaque année. En adhérant à l'AMC et en renouvelant leur adhésion chaque année, tous les membres de l'AMC s'engagent à respecter le Code.

Ces instruments fonctionnent dans un environnement juridique qui comprend la législation et la réglementation en matière de consommation, de concurrence, de santé et de sécurité, de travail et d'environnement, ainsi que le droit des contrats et de la responsabilité civile. Par exemple, si une organisation prétend être en conformité avec un code mais ne l'est pas, elle peut être soumise à la Loi sur la concurrence pour publicité trompeuse. La non-adhésion a également un impact sur la réputation.

La Commission d'accès à l'information du Québec devrait enquêter et procéder à des vérifications uniquement lorsque des plaintes n'ont pas été résolues à l'interne ou lorsqu'un processus interne adéquat de traitement des plaintes n'a pas été établi. Lorsqu'une organisation ne peut pas démontrer sa conformité, elle risque de tomber sous le coup des règles générales de conformité appliquées par la Commission.

B. **Certifications et codes officiellement reconnus :** Le cadre québécois de protection de la vie privée serait amélioré davantage si la Loi permettait la reconnaissance officielle de certaines certifications et de certains codes fondés sur l'approbation du gouvernement du Québec ou de la Commission d'accès à l'information du Québec, sous la surveillance d'organismes d'accréditation tiers sélectionnés.

La Loi ne doit pas prescrire une liste de domaines justifiant des normes, mais plutôt un cadre permettant aux organismes existants d'élaborer des programmes d'agrément en réponse aux besoins du marché. Elles peuvent être en rapport avec certaines dispositions de la Loi uniquement ou avec une évaluation générale de la vie privée (par exemple pour un secteur ou une industrie).

S'inspirant du modèle britannique, les propositions soumises pour approbation pourraient identifier les opérations de traitement de données couvertes, les catégories d'organisations auxquelles elles s'adressent et les problèmes de protection de la vie privée qu'elles entendent aborder. Les propositions doivent faire l'objet d'une consultation adéquate et être classées en fonction des critères de recevabilité habituels. Lorsqu'une organisation est jugée conforme à une certification ou à un code par un tiers accréditeur, elle est considérée comme satisfaisant aux exigences pendant une période déterminée (par exemple, trois ans), après quoi son adhésion doit être renouvelée. Cette approche devrait être développée grâce à une collaboration entre les gouvernements provincial et fédéral. Le Conseil canadien des normes dispose d'un processus d'élaboration et d'examen approfondi des normes d'accréditation; son rôle devrait être mis à profit et maximisé.

La Commission d'accès à l'information du Québec pourrait avoir l'obligation générale de tenir compte du respect des codes et des certifications officiellement reconnus lorsqu'elle décide de mener ou non une enquête. Le respect des règles devrait également être un facteur de détermination de la diligence raisonnable dans le cadre d'une enquête ou d'une amende. La Commission ne devrait pas avoir le pouvoir d'examiner périodiquement l'adhésion d'une organisation à un régime, et cela relèverait à juste titre de l'organisme d'accréditation tiers. L'organisme d'accréditation pourrait avoir l'obligation de signaler à la Commission les cas où la conformité d'une organisation est révoquée pour non-conformité.

10. Le droit à la portabilité des données devrait être reporté jusqu'à ce que ses impacts plus larges soient compris.

Le droit proposé à la portabilité des données fournirait un droit explicite pour les individus de demander que leurs renseignements personnels soient transférés d'une organisation à une autre dans un format numérique standardisé, lorsqu'un tel format existe.

L'objectif premier de la portabilité des données est double : permettre un meilleur contrôle individuel des données et encourager la concurrence sur le marché. Bien que la portabilité des données vise à renforcer le contrôle et le choix des consommateurs, elle crée de nouveaux risques sérieux pour les consommateurs en ce qui concerne la cybersécurité, la vie privée et la confidentialité. De plus, ses répercussions plus larges sur l'économie, l'innovation et la concurrence ne sont pas bien comprises. Des recherches supplémentaires doivent être menées pour comprendre ses effets.

Il est important de reporter la mise en œuvre du droit de portabilité des données proposé dans le Projet de loi 64 dans l'attente d'une étude plus approfondie de ses répercussions sur la vie privée. Les secteurs industriels peuvent jouer un rôle central dans l'identification de considérations techniques ou concurrentielles particulières.

Pour s'assurer que ce nouveau droit ne crée pas de conséquences involontaires qui entraveraient le bien-être économique du Québec, d'autres organismes, comme le Bureau fédéral de la concurrence, devraient être invités à collaborer de façon significative à la recherche et au développement de ce concept dans un contexte québécois. C'est plus qu'une question de vie privée, et la réforme correspondante d'autres lois peut s'avérer nécessaire.

Si le droit à la portabilité des données est finalement appliqué, il exigera :

A. **Une approche progressive qui permet l'élaboration et la mise en œuvre de cadres sectoriels spécifiques :** Nous avons appris du modèle RGPD, qui crée un droit de portabilité des données de grande envergure mais n'apporte que peu de clarté sur la mise en œuvre, qu'une approche plus pratique est essentielle.

   Des cadres sectoriels spécifiques devraient être élaborés en consultation avec l'industrie pour refléter les aspects pratiques et risques actuels dans chaque industrie concernée, et pourraient être mis en œuvre par voie réglementaire. Ces cadres doivent tenir compte d'importantes questions économiques, techniques, d'authentification, de sécurité et opérationnelles. D'autres régulateurs que la Commission d'accès à l'information du Québec devraient être impliqués dans l'application de ces cadres, la Commission supervisant uniquement les questions liées au respect de la vie privée.

B. **Limites sur l'étendue des données portées :** Fournir de données directement à un individu est une extension du droit d'accès actuel en vertu de la Loi québécoise sur la protection des renseignements personnels, laquelle, dans sa forme actuelle, contribue grandement à soutenir le contrôle des consommateurs. Les individus disposent déjà d'un droit d'accès aux renseignements personnels qu'une organisation détient à leur sujet, pour contester leur exactitude et leur exhaustivité, et pour faire modifier ces renseignements comme il convient. Les transferts d'une organisation à l'autre doivent être effectués à la demande de l'individu. Le droit à la portabilité des données doit être considéré séparément du droit d'accès, et la portée des données ne doit pas nécessairement inclure tout ce qui est accordé dans le cadre d'une demande d'accès typique.

Les données portées doivent être limitées aux renseignements personnels fournis par l'individu. D'autres types de données doivent généralement être exclus, comme les données qui peuvent être propriétaires ou qui ne sont pas considérées comme des renseignements personnels. Nous soutenons l'intention déclarée du gouvernement que le droit de portabilité des données proposé ne couvre pas les renseignements qui ont été créés, dérivés, calculés ou déduits des données fournies par l'individu.

Les cadres sectoriels ont la capacité de fournir des éclaircissements sur la portée des données appropriées à l'objectif de la portabilité des données, y compris les données limitées liées aux transactions commerciales. En ce qui concerne les données à haut risque ou plus sensibles, il est conseillé de limiter les champs de données qui peuvent être portés et de renforcer les exigences d'authentification.

Pour éviter toute perturbation inutile des pratiques commerciales courantes, le droit à la portabilité des données ne doit pas imposer automatiquement à une organisation l'obligation de supprimer les données portées. Les organisations doivent être autorisées à suivre des politiques et des procédures standard en matière de rétention.

En termes de format, les données portées doivent être limitées aux données numériques dans des formats technologiquement neutres, en d'autres termes, un format numérique standardisé, lorsqu'un tel format existe, et non aux enregistrements physiques auxquels les droits d'accès normaux peuvent s'appliquer. La Loi doit permettre l'émergence de solutions dans chaque secteur, et leur évolution au fil du temps. Au fur et à mesure des progrès, l'étendue des données portées pourrait évoluer en conséquence.

Ces règles ne doivent pas créer d'obstacles indus pour les PME, car cela porterait atteinte à l'objectif initial d'une plus grande concurrence.

C. **Mesures visant à protéger contre les violations de données et la fraude, et à garantir une responsabilité équitable :** Lorsque les organisations sont obligées de répondre aux demandes d'individus concernant leurs propres données, une authentification forte doit être mise en place pour se prémunir contre les demandes frauduleuses. La mobilité d'organisation à organisation doit être conditionnelle à la demande faite par l'individu (et pas seulement l'organisation tierce), et à la mise en place d'un cadre sectoriel adéquat. Les demandes groupées de tiers doivent être interdites. En particulier, la Loi doit garantir que les organisations ne peuvent pas automatiser les demandes, ou tenter d'enterrer le consentement pour le partage ou l'obtention de renseignements portés dans les contrats.

L'introduction d'un droit à la portabilité des données attirera des fournisseurs tiers qui doivent être correctement évalués, en particulier s'ils opèrent au niveau international et peuvent potentiellement échapper à l'application de la Loi. Les parties qui reçoivent des renseignements portés doivent être responsables envers les consommateurs et doivent être prêtes à protéger de manière adéquate les renseignements personnels. Les organisations doivent prendre des mesures adéquates pour éviter les violations de données, et pour assurer le niveau approprié d'authentification des données (possiblement lié à la sensibilité des données) et de cryptage.

Une exclusion de responsabilité doit être mise en place lorsqu'un organisme est mandaté par un consommateur pour transférer des données à un tiers. Les responsabilités de l'organisation d'origine doivent se limiter à confirmer que la demande émane bien de l'individu concerné (c'est-à-dire qu'elle n'est pas frauduleuse) et à transférer les données en toute sécurité. L'organisation d'origine ne doit pas être tenue responsable si l'organisation destinataire ne respecte pas ses obligations de sauvegarde et autres exigences dans un cadre sectoriel, conduisant à une

utilisation abusive des données. Enfin, la Loi devrait définir les bases sur lesquelles une organisation peut s'opposer à une demande de portabilité des données.

Pour toute question ou commentaire concernant cette soumission, veuillez contacter :

Sara Clodman
Vice-présidente de l'ACM,
Affaires publiques et leadership éclairé
sclodman@theCMA.ca

Fiona Wilson
Directrice des relations gouvernementales
fwilson@theCMA.ca

À propos de l'ACM

L'ACM est la voix de la profession du marketing au Canada. Nous servons plus de 50 entreprises, organisations à but non lucratif, organismes publics et établissements d'enseignement supérieur au Québec, et contribuons à l'excellence professionnelle des spécialistes du marketing du Québec par le biais de nos événements et de nos programmes de perfectionnement professionnel, y compris les marques les plus prestigieuses du Canada. Notre communauté comprend des agences de création, de médias et de relations publiques, des sociétés de recherche, des sociétés de conseil en gestion, des entreprises technologiques et d'autres fournisseurs de la communauté marketing. Nous soutenons les activités liées à la réflexion, au développement professionnel, à la protection des consommateurs et au succès commercial. Nous sommes le principal défenseur de la commercialisation auprès des gouvernements, des régulateurs et des autres parties prenantes. Notre désignation de spécialiste du marketing agréé (SMA) garantit que les professionnels du marketing sont hautement qualifiés et à jour des meilleures pratiques. Nous défendons les normes d'autorégulation, notamment le Code de déontologie et de normes de pratiques de l'Association canadienne du marketing.

Feedback to the National Assembly's Committee on Institutions on proposed amendments to Quebec's private sector privacy law (Bill 64)

September 28, 2020

Executive Summary

As the voice of the marketing profession, the Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Government of Quebec on Bill 64's proposed amendments to Quebec's Act respecting the protection of personal information in the private sector.

In our modern digital economy, consumers increasingly expect organizations to deliver the intuitive products and services they want and need. Quebec's privacy law, now and into the future, must embrace the enormous social and economic benefits of data use for Quebecers while protecting their privacy. There must be a mechanism for Quebec's alignment on privacy reform initiatives underway across the country to avoid unnecessary complexity for consumers and business, and to prevent complications for interprovincial and international trade, and foreign direct investment in Quebec.

As the National Assembly considers the provisions of Bill 64, the CMA is pleased to provide the following recommendations:

1. Quebec's privacy law must be flexible, technology-neutral and proportionate to the privacy objectives to be achieved. Quebec's privacy law should be based on principles that are flexible in the face of rapidly evolving technologies, business models and consumer privacy expectations. It should be commensurate to the privacy goals at hand, without creating undue complexity for consumers, businesses and government.

2. There must be a mechanism for alignment with other privacy frameworks across Canada to prevent undue complexity for businesses and consumers, and barriers to trade and foreign investment in Quebec. In particular, there should be reasonable alignment with anticipated reforms to the federal Personal Information Protection and Electronic Documents Act (PIPEDA), as significant differences between the two laws will negatively impact Quebec's businesses and citizens.

3. Requirements for cross-border data transfers must include proven, workable alternatives to adequacy, such as standard contractual clauses.

4. **Accountability for outsourcing should be placed on the principal organization**, mandating service providers to follow the requirements set out by the principal organization.

5. The type of consent required must be based on an assessment of relevant factors, reserving express consent for when it is truly meaningful. The law should recognize the important role that implied consent plays in serving consumers and business.Alternatively the law could provide for express consent for "legitimate purposes", enabling organizations to justify their legitimate purposes through internal assessments, and identify them to individuals.

6. Enforcement measures should be reviewed and reduced to incentivize compliance without having a chilling impact on business and investment in Quebec. In particular, the application of fines must be based on specific factors using a proportionate approach that considers the nature of the violation, and the size and data processing activities of the organization that committed the violation.

7. Reasonable transparency should be required around profiling and decisions based on solely automated processing. Regulatory responses should be remedial, prohibiting or restricting only those activities where there is clear evidence of harm.

8. The consent exception for de-identified information should be broadened, provided certain standards for de-identification are met. The Act should further permit the collection, use and disclosure of de-identified information without consent for all reasonable purposes, if certain standards are developed and met.

9. Self-regulatory measures should be encouraged and incentivized to ensure regulatory efficiency. Voluntary codes, certifications and other standards (such as the Canadian Marketing Code of Ethics and Standards) play an important role in supplementing privacy legislation. The government should **e**ncourage self-regulated certifications and codes as tools for privacy compliance and accountability, and should further incentivize their use by selecting some for formal recognition.

10. The right to data portability should be postponed until its wider impacts are understood. Data portability creates serious new risks related to fraud, privacy and security, and its wider impacts on the economy and competition are not well-understood**.** It should only be achieved through a phased-in approach that allows for the implementation of sector-specific frameworks.

Introduction and Context

The Canadian Marketing Association (CMA) appreciates the opportunity to provide feedback to the Government of Quebec on Bill 64's proposed amendments to Quebec's Act respecting the protection of personal information in the private sector.

The CMA is the voice of the marketing profession, representing more than 50 corporate, not-for-profit, public, and post-secondary members across Quebec. We are committed to helping organizations maintain high standards of conduct and transparency through our mandatory Canadian Marketing Code of Ethics and Standards, and our privacy and data protection resources for marketers and consumers. As the recognized and longstanding leader in marketing self-regulation, we strive to ensure an environment where consumers are protected and businesses can thrive.

Quebec's marketing community highly values its customers, whose loyalty and trust provides the foundation for business success. Most organizations recognize that strong privacy and data protection practices serve as a competitive advantage and customer retention strategy, and they work hard to protect the privacy interests of the individuals they serve. Government and industry collaboration is essential to ensure Quebec's privacy framework is based on a balance between embracing the enormous social and economic benefits of data use while protecting the privacy of individuals.

Quebec was the first North American jurisdiction to enact privacy legislation governing commercial activities. The modernization of Quebec's privacy law is an important step to ensure that Quebec continues to be a champion of privacy protection, striking a balance between consumers' privacy expectations and leveraging data to support economic growth and innovation. We appreciate current reform efforts underway by the National Assembly, and believe Quebec has a significant opportunity to pursue a solution that is practical for both consumers and businesses.

Alignment with other privacy frameworks across Canada is critical to ensuring the success of organizations operating in Quebec, for the betterment of Quebec citizens who value the range of products and services that are available to them. There must be a mechanism for alignment on privacy reform initiatives underway across the country to ensure businesses can operate seamlessly across international and provincial borders, and to ensure Quebec remains an attractive foreign direct investment destination. If these approaches are not aligned, it will create a patchwork of privacy legislation, resulting in unnecessary complexity and barriers for businesses, and disruptions for consumers. It will also reduce Quebec's attractiveness as a business destination for companies in other countries and provinces, negatively impacting Quebec's economy and consumer choice.

The marketing community supports many improvements proposed in Bill 64, including new consent exceptions for research and sale of business transactions, and an exclusion of business contact information from the definition of personal information. Other areas of the Bill require a closer look by the National Assembly to ensure Quebec's privacy framework achieves its dual goal of protecting consumers while supporting responsible innovation and competitiveness, and to avoid the issues that have arisen in jurisdictions governed by more prescriptive, EU-inspired data protection laws.

As the National Assembly considers the provisions laid out in Bill 64, the CMA is pleased to provide the following recommendations:

Recommendations

1. Quebec's privacy law must be flexible, technology-neutral and proportionate to the privacy objectives to be achieved

Data underpins the digital economy. It informs better decision-making and enables the development of important new technologies, like artificial intelligence (AI), for which Quebec is a world leader.

The ability of organizations to collect, use and disclose personal information is key to providing value to consumers, and to ensuring Quebec's innovation and competitiveness. It is important that Quebec's privacy law remain adaptive to a changing business environment and function within operational realities and context-specific risks. This is especially important for Small and Medium Enterprises (SMEs) so that compliance is not unduly onerous.

Quebec's privacy law must be based on principles that can be thoughtfully applied to all technologies and business models, in order for it to remain relevant. Bill 64 takes an important step away from static and outdated concepts such as "files". A further review of the law should ensure there are no remaining technology-specific provisions that would not stand the test of time.

It is also important that the law provide for the evolving expectations and preferences of consumers**,** without the need to repeatedly introduce legislative amendments to keep up with the times.

Technological advancements have provided organizations with the agility to offer relevant, useful offerings to consumers. As a result, consumers demand much greater speed and quality of information than ever before to use services provided by companies, and to make informed purchase decisions. A strong majority of consumers (76%) are willing to share personal data in order to receive benefits, as long as the data is properly protected[1]. Many consumers, including younger generations, recognize that data exchange is increasingly fundamental to accessing many of the beneficial services they interact with daily.

Quebec's privacy law should be commensurate to the privacy goals at hand, without creating undue complexity for government, business and consumers. Privacy law should be based on sound principles that allow organizations to account for context. The law should be flexible enough to impose measures proportionate to the privacy interests involved and the individual's reasonable expectation of privacy in the circumstances.

A reformed law should include a new purpose clause requiring the law be interpreted in a proportionate manner, reasonable to the circumstances. We recommend the following changes to the Act:

> *The object of this Act is to establish, for the exercise of the rights conferred by articles 35 to 40 of the Civil Code concerning the protection of personal information, particular rules with respect to personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code.*
>
> *Those particular rules are to be applied in a manner that recognizes the right of privacy of individuals under the Civil Code and the need of organizations to collect, hold, use or communicate personal information for purposes that a reasonable person would consider appropriate in the circumstances.*

[1] Foresight Factory, 2018: Data Privacy Study: What the Canadian Consumer Really Thinks

2. There must be a mechanism for alignment with other privacy frameworks across Canada to prevent undue complexity for businesses and consumers, and barriers to trade and foreign investment in Quebec.

Privacy reform initiatives underway across the country must be consistent to ensure that businesses can operate seamlessly across international and provincial borders, in addition to enabling Quebec to remain an attractive destination for direct foreign investment. If these approaches are not aligned, it will create unnecessary complexity and barriers for businesses, disrupting the services and innovative technologies consumers want and need. There must be a mechanism for alignment between the federal, provincial and territorial governments in order to prevent the damaging fragmentation of privacy frameworks, including the negative impacts of interprovincial trade barriers.

In particular, it is critical for the National Assembly to ensure reasonable alignment with anticipated reforms to the federal Personal Information Protection and Electronic Documents Act (PIPEDA), as significant differences between the two laws will cause complexity for businesses, consumers and government.

Quebec's privacy law should be compatible with jurisdictions that have a similar, principles-based approach to privacy. It is more important than ever for the law to be nimble in the face of rapidly evolving technologies and business models, allowing organizations to determine the most effective way to meet their common obligations. The nuances – the respect for context, individuals' expectations and overall emphasis on reasonableness, should remain.

Many features of existing Canadian privacy laws, although due for a thoughtful upgrade, have stood the test of time, providing privacy protection without unnecessary regulatory burden. Newer and more prescriptive laws in other jurisdictions, including the GDPR, remain unproven in many respects, and have created a staggering regulatory burden for both government and business. A privacy framework should not be so onerous that it cannot be effectively implemented and is not well understood by non-specialists.

With regards to GDPR adequacy status, reducing friction in data transfers is a worthwhile objective. However, in considering the adoption of certain aspects of GDPR, we urge the National Assembly to evaluate each based on its merit in the Quebec context, with the goal being compatible privacy outcomes as opposed to compatible legislative requirements. If Canadian privacy frameworks are more aligned, it would support a positive decision on GDPR adequacy status that would apply more comprehensively across Canada's jurisdictions, making it easier for Quebec businesses to trade and compete.

3. Requirements for cross-border data transfers must include proven, workable alternatives to adequacy

In today's interconnected world, the efficient and reliable outsourcing of data processing operations outside of Quebec is crucial to the functioning of Quebec's businesses and their ability to serve consumers well.

Bill 64 proposes considerable restrictions on organizations seeking to share information with third parties located outside of Quebec, complicating conditions for business efficiency, growth and trade.

Under this provision, Quebec companies can transfer personal information only to those "States" whose legal frameworks have privacy protections equivalent to Quebec's, as part of a comprehensive privacy impact assessment. This provision is concerning in several significant respects:

- The requirement for equivalency would create significant difficulties for Quebec companies, particularly SMEs, as they compete in the global economy. Companies will face undue complexity, delays and costs as they carry out individual assessments for every jurisdiction to which they may transfer personal information. The concerns raised following the recent "Shrems II" decision in Europe, mandating that every cross-border data transfer be assessed on a case-by-case basis, underscore the impracticality of this approach.

- Quebec-based organizations, including multinationals, may decide to scale back or alter their operations to the detriment of Quebec's economy, healthy competition and consumer choice.At present, the Bill does not clarify whether a "State" would include other provinces, which would create even more complexity for Quebec businesses, as well as the consumers they serve across Canada.

- The ongoing determination and review of the adequacy status of other jurisdictions will require significant attention and resources by the provincial government, as we have seen under the EU's GDPR.

- The adequacy requirement risks violating the provisions in important trade agreements with regards to cross-border data flows, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Canada-United States-Mexico Agreement (CUSMA). 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 and may violate Article 14.13 and 19.12 of the CPTPP and CUSMA, respectively.

We urge the government not to maintain the adequacy requirement. If the adequacy requirement is retained despite the obstacles it creates, there must be alternative mechanisms in place for the transfer of personal information to jurisdictions that are not deemed equivalent. As we have learned from the experience of other jurisdictions, there are well-established and legally enforceable alternative mechanisms available.

The GDPR, for example, is far more flexible and provides for various lawful bases other than adequacy for data transfers to other States, including for contractual necessity, or if standard contractual clauses, codes of conduct, or binding corporate rules are in place.

Given the nature of data flows, current contractual obligations between organizations are an effective form of responsible data governance. If standardized contractual clauses are considered, they must allow for some flexibility to account for the varying nature and scope of the organizations and activities involved.

Finally, the Act must clarify when its provisions have extra-territorial effect. It should clearly state that its provisions apply within the province of Quebec and only apply to entities or activities outside of Quebec where there is a "real and substantial connection" to the jurisdiction, similar to the requirement under PIPEDA.

We recommend the following changes to the Act:

> *17. Before communicating personal information outside Québec, a person carrying on an enterprise must conduct an assessment of privacy-related factors ~~must~~, in particular: ~~take into account~~*
> *(1) the sensitivity of the information;*
> *(2) the purposes for which it is to be used; and*
> *(3) the protection measures that would apply to it, including contractual measures.; ~~and~~*

~~(4) the legal framework applicable in the State in which the information would be communicated, including the legal framework's degree of equivalency with the personal information protection principles applicable in Québec~~.

The information may be communicated if the assessment establishes that it would receive a comparable level of protection through legislative, contractual or other measures ~~equivalent~~ to that afforded under this Act. ~~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.

This section does not apply to a communication of information under subparagraph 7 of the first paragraph of section 18.

~~17.1. The Minister shall publish in the Gazette officielle du Québec a list of States whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Québec.~~

4. Accountability for outsourcing should be placed on the principal organization

We support Bill 64's framework for sharing personal information with service providers in the context of outsourcing relationships. It represents best practice by not requiring additional consent.

To ensure a clear and consistent accountability chain, it is important that the Act clarify that the principal organization (i.e. "a person carrying out an enterprise") is solely responsible for ensuring compliance with privacy law, while the role of the service provider (i.e. "a person or body carrying out a mandate or performing a contract of enterprise or for services") is to follow the requirements set out by the principal organization.

Service providers have a responsibility for protecting personal information adequately, and these responsibilities are generally defined in the contract. Since the principal organization is the ultimate decision-maker when hiring a provider to provide a service, it makes senses that the principal organization remains solely responsible for complying with the Act.

We recommend the following change to the Act:

> *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.*

5. The type of consent required must be based on an assessment of relevant factors, reserving express consent for when it is truly meaningful

An overreliance on express consent has contributed to "consent fatigue" for consumers, causing individuals to be less likely to carefully review privacy notices, make informed decisions and exercise choices. It is ill-suited to the realities of commercial enterprises, to the increasingly connected world in which consumers live and to evolving consumer expectations.

Requesting express consent, tracking consent and keeping records of consent for reasonable and standard data uses is overly burdensome for businesses, without a corresponding privacy protection benefit, and often results in poor customer experience.

It is imperative that the requirement for express consent be reserved for the things that matter most; for situations that may not reasonably be expected, and where individuals have a meaningful choice.

Bill 64 introduces several improvements to the consent model. The marketing community strongly supports the proposed exceptions to the consent requirement for:

- transferring personal information to an agent for processing,
- secondary uses and enterprise analytics where the use is consistent with the original consent,
- when the use is clearly in the individual's best interest, and
- in the case of a business transaction.

We also support the exclusion of business contact information from the definition of personal information that will trigger the consent obligation.

However, the current language around consent in Bill 64 is unclear. The Bill appears to require consent in almost all circumstances where personal information is used or transferred to a third party as a result of ss. 12 and 13. Consent must be express when it involves sensitive personal information, which seems to imply that another form of consent may be acceptable in some circumstances involving non-sensitive information.

The Bill 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 are disproportionate in many circumstances, and inconsistent with the important role played by implied consent. Furthermore, it is unclear whether "separately from any other information provided to the person concerned" means outside the scope of a privacy policy.

Bill 64 does not currently refer to the concepts of express and implied consent, in contrast to other privacy laws across Canada, which authorize implied consent under certain circumstances. The proposal to separate consent for each purpose from other terms significantly departs from other privacy regimes. The Act should be amended to recognize the importance of implied consent, and should clarify that implied consent is sufficient where it is reasonable in the circumstances.

A longstanding strength of Canadian privacy frameworks is that organizations have the operational choice of whether to seek express or implicit consent. This ensures the appropriate form of consent is dependant on an assessment of the sensitivity of the information and the reasonable expectations of the individual, both of which will depend on context.

In general, express consent (e.g. opt-in) should be used for a collection, use or disclosure that generally involves sensitive information, is outside the reasonable expectations of the individual, or creates a meaningful risk of significant harm. Implied consent (e.g. opt-out) should be used for a collection, use or disclosure which generally involves non-sensitive information and straightforward purpose(s).

We urge Quebec to adopt the same framework for implied consent that the federal government and other provinces rely on, as outlined in the Office of the Privacy Commissioner of Canada's Guidelines for Obtaining Meaningful Consent.

We recommend the following changes to the Act:

> *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.*~~

The National Assembly should also incorporate additional alternatives to express consent (e.g. an exemption to consent for "legitimate purposes"). Express consent should not be required in situations where it is not meaningful or appropriate, such as in the case of personal information being used by organizations for legitimate purposes that take into account the reasonable expectations of the individual under the circumstances.

Organizations relying on this exemption must be transparent about their legitimate purposes, explicitly specifying them in advance and outlining them in a privacy policy or other method that is readily available to individuals.

The Act could allow for the formation of Regulations to specify allowable legitimate purposes or classes of legitimate purposes and to specify what information needs to be explicitly specified by organizations before the information is used.

It is reasonable to expect organizations relying on this exemption to justify their legitimate purposes and outline them clearly in their privacy policies and through the performance of internal assessments. The assessment would need to be based on the specific context and circumstances to demonstrate that processing is appropriate and reasonable.

6. Enforcement measures must be reviewed and reduced to incentivize compliance without having a chilling impact on business and investment in Quebec

The vast majority of Quebec organizations want to protect the privacy of their customers. They do not want to damage their reputations and jeopardize consumer trust by misusing or mistreating personal information. We support enhanced enforcement measures to provide effective recourse for individuals and to crack down on bad actors. However, it is critical that these measures not have a chilling effect on businesses and their ability to serve consumers well.

Bill 64 proposes new enforcement measures that are disproportionate to the privacy goals to be achieved and lack sufficient procedural safeguards. Penalties must provide sufficient incentive to deter businesses that might not otherwise comply, and must also be designed to avoid a costly and litigious environment, when reduced penalties could be just as effective.

If unduly strict enforcement measures are put in place, some organizations will find it necessary to assess the risks, costs and benefits of continuing to do business in Quebec. The measures in Bill 64

must be modified to ensure a reasonable approach to enforcement, with a level of liability that incentivizes compliance while fostering a collaborative and trusting privacy landscape.

The use of a percentage of worldwide turnover to calculate possible fines[2] is not advisable, and if this approach is set in place, it is important to reduce the maximum amount to a more reasonable and proportionate level. The proposed range for fines and AMPs would lead to fines out of touch with the actual impact of most offences, and is not likely to be able to appropriately reflect the circumstances of each case. It would make companies more reluctant to enter or remain in the Quebec market, particularly if Quebec accounts for only a small portion of their overall business, for fear of being fined as a percentage of worldwide turnover.

There must be specific factors to consider when applying fines, using a proportionate approach that considers the nature of the violation and the size and data processing activities of the organization that committed the violation. Fines should be focussed on the most egregious cases with intent and gross negligence. If the current range for AMPs is maintained, rigorous procedural safeguards must be put in place to ensure fairness.

The Bill proposes a new private right of action. This would create conditions that promote potentially opportunistic class actions, in addition to increased exposure by organizations to privacy-related claims, including claims for punitive damages. It imposes a strict level of liability for privacy that is unprecedented, creating a disproportionate burden on businesses.

Bill 64 attaches liability unless the underlying event was impossible to foresee and impossible to avoid. There is no due diligence defence or other defence set out in the proposed regime. An organization could still incur liability if it acted reasonably and responsibly, provided notice of possible risks to the individual in advance and took all possible precautions to manage personal information in a compliant manner.

If the private right of action is ultimately pursued, it must be implemented only as a last resort, once it is clear that the use of fines and AMPs is not sufficient. In addition, it must allow for all reasonable defences at law, including the exercise of due diligence.

7. Reasonable transparency should be required around profiling and decisions based on solely automated processing

When an organization uses personal information to render a decision based exclusively on automated processing, Bill 64 proposes to grant individuals the right to be informed at or before a decision is made, including to be provided with information regarding the elements of personal information used, the reasons and principal factors leading to the decision and the right to have their information corrected. The organization would also be required to allow the person to submit observations for review of the decision.

To assist individuals in better understanding how decisions are made about them, we support a requirement for organizations to share summary information (in their privacy policies) with individuals about the use of automated decision-making, the factors involved in the decision, and where the decision is impactful. They must not be required to reveal any confidential or proprietary commercial information, algorithms or procedures.

[2] Bill 64 includes a penal regime with fines of up to $25,000,000 (or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year), doubling this for subsequent offences. The Bill also sets out administrative monetary penalties (AMPs) for a broad range of offences of up to $10,000,000 (or, if greater, 2% of worldwide turnover for the preceding fiscal year). In addition, the Bill proposes a private right of action with no-fault liability.

If concerned individuals submit observations to the organization for review, an organization must have the discretion to determine whether or not to ultimately change its decision. These decisions are highly nuanced, and a right to object to decisions based solely on automated processing would be highly problematic.

As drafted, the notice requirement is too broad, as it would be applicable in all circumstances involving decisions based on automated processing, regardless of materiality of the impact of the decision on the individual.

It is far from clear that all forms of automated decision-making are problematic or warrant a regulatory response. In fact, "automated decision-making" includes a range of legitimate activities, such as a website declining to serve copyright-protected content to a user resident in a jurisdiction where the website provider does not hold the rights to make that content available. As data becomes more complex, the use of automation is critical and beneficial. There are a growing number of helpful automated decisions being made each day, resulting in beneficial services for consumers, such as chatbots that provide consumers with relevant and personalized advice.

Individuals are demanding faster, easier and more intuitive services and automation is central to the delivery of this promise. There are cases where automated decision-making is linked to the actual provision of a service that a consumer may want or need. There must be an understanding that if a consumer objects to the automated decision-making, they would not be able to access the service altogether.

Bill 64 would also require organizations that collect personal information using technology that has the ability to identify, locate or profile an individual to inform the individual of such technology and the means available, if any, to deactivate such technology.

In the case of marketing, profiling is intended to provide an individual with a more relevant experience, such as if a product or service is offered based on an individual's previous preferences and habits. Many organizations create a profile or use automated decision-making in order to target their marketing efforts, including through the use of third-party analytic tools and software, such as cookies, pixels and beacons.

We caution against the GDPR model, which places restrictions on solely automated decisions that produce "legal **or** similarly significant effects,", as there is significant uncertainty by organizations in assessing "similarly significant effects," stifling innovation and resulting in industry confusion.

Transparency will be the most important factor. Organizations should be transparent in their privacy policies about their use of third-party analytic tools and software to track, identify and target individuals in order to serve them relevant advertising. Where possible, they should also refer individuals to the opt-out mechanism accessible through the service provider's platform.

8. The consent exception for de-identified information should be broadened, provided certain standards for de-identification are met

De-identification and anonymization are among the most effective privacy-protective mechanisms available for organizations to engage in data analytics and innovation in the digital economy.

Bill 64 states that personal information collected for one purpose may be used, without consent, for the secondary purposes of study or research or for the production of statistics, if the information is de-identified.

As the consent exemption applies only to use within the enterprise, the purposes of study, research and the production of statistics may be construed as enterprise or business analytics. This should be clarified in the Act.

Given the critical importance of de-identification to responsible innovation, and in order to remove any legal uncertainty, the Act should be amended to further permit the collection, use and disclosure of de-identified information without consent for all reasonable purposes, if certain standards are met.

To ensure a level playing field and provide clarity, it is important for organizations to have a set of common standards by which they can demonstrate whether they took all reasonable steps at the time to de-identify personal information and mitigate the risk of re-identification. The standard of de-identification and ongoing monitoring should fit the context, which is more relevant than the "type" of data.

The Act should acknowledge formal industry standards, and include benchmarks for technical and administrative procedures, monitoring, and risk assessments and protocols. The Act should clarify parameters of accountability around the onward transfers of de-identified data, and should emphasize the need for contractual provisions between organizations to be in place to address re-identification.

As technology evolves, the requirements for de-identification will need to evolve too. We propose that the government work with industry to develop these standards , which could result in a formal certification involving a third-party accreditor approved by the Government of Quebec (see recommendation 9 below).

9. Self-regulatory measures should be encouraged and incentivized to ensure regulatory efficiency

All sectors have a role to play to protect the privacy of Quebecers. A co-regulatory model in which government regulation and industry self-regulation work in tandem is important to ensure regulatory efficiency. There is no one-size-fits all approach to privacy compliance; much depends on each sector and the types of information being collected, used and shared. Now and into the future, codes, certifications and other standards will play an important role in supplementing privacy legislation.

All schemes should be voluntary, recognizing the varying degrees of data processing operations among organizations, and ensuring organizations with limited resources are not unduly impacted. Standards could be either self-regulated or formally recognized by government, as outlined below:

A. **Self-regulated standards and codes:** Self-regulated standards and codes should be referenced in the Act as tools that can help organizations ensure compliance, and help demonstrate accountability in the event of an investigation by the Commission d'accès à l'information du Québec. Industry should be encouraged to develop and follow these standards and codes.

   Industry and professional self-regulated codes of practice are practical and efficient tools to steer privacy compliance. For example, the Canadian Marketing Code of Ethics and Standards is a comprehensive code that establishes and promotes high standards for the conduct of marketing and strengthens marketers' knowledge of compliance requirements. Section J of the Code addresses the protection of personal privacy. The Code is reviewed and updated annually. Upon joining the CMA and upon membership renewal each year, all CMA members agree to comply with the Code.

   These instruments operate in a legal environment that includes consumer, competition, health and safety, labour and environmental legislation and regulations, and contract and tort law. For example, if an organization purported to be in compliance with a code but was not, it could be

subject to the Competition Act for misleading advertising. Failure to adhere also has a reputational impact.

The Commission d'accès à l'information du Quebec should investigate and audit only where complaints arise that have not been resolved internally, or where an adequate internal complaints process has not been established. When an organization could not demonstrate compliance, it would risk falling under general compliance rules enforced by the Commission.

B. **Formally recognized certifications and codes:** Quebec's privacy framework would be further enhanced if the Act allowed for the formally recognition some certifications and codes based on approval by the Government of Quebec or the Commission d'accès à l'information du Quebec, with oversight from select third-party accrediting bodies.

The Act must not prescribe a list of areas that warrant standards but rather a framework to allow existing bodies to develop schemes for approval in response to market needs. They could be in relation to certain provisions of the Act only or a broad assessment of privacy (for example for a sector or industry).

Borrowing from the UK model, proposals submitted for approval could identify the data processing operations covered, the categories of organizations that they apply to, and the privacy issues that they intend to address. Proposals must be informed by adequate consultation and be ranked against standard admissibility criteria. Once an organization is deemed to be in compliance with a certification or code by a third-party accreditor, it would be considered to meet the requirements for a set time period (e.g., three years), after which its adherence would need to be renewed. This approach should be developed through collaboration between the provincial and federal governments. The Standards Council of Canada has a thorough development and review process for accreditation standards; its role should be leveraged and maximized.

The Commission d'accès à l'information du Quebec could have a general obligation to consider adherence to formally recognized codes and certifications in making decisions about whether to investigate. Compliance should also be a factor in determining due diligence in the context of an investigation or fine. The Commission should not have authority to periodically review an organization's adherence to a scheme, and this would properly fall with the third-party accrediting body. The accrediting body could have a duty to report incidences to the Commission where an organization's compliance is revoked for non-compliance.

10. The right to data portability should be postponed until its wider impacts are understood

The proposed right to data portability would provide an explicit right for individuals to direct that their personal information be moved from one organization to another in a standardized digital format, where such a format exists.

The primary objective of data portability is two-pronged: to provide greater individual control over data and to encourage competition in the marketplace. Although data portability is intended to enhance consumer control and choice, it creates serious new risks for consumers with regards to cybersecurity, privacy and confidentiality. In addition, its wider impacts on the economy, innovation and competition are not well-understood. More research must be done to understand its effects.

It is important to postpone the implementation of the data portability right proposed in Bill 64 pending further study of its non-privacy impacts. Industry sectors can play a pivotal role in identifying specific technical or competitive considerations.

To ensure that this new right does not create unintended consequences that hamper Quebec's economic well-being, other bodies, such as the federal Competition Bureau, should be invited to collaborate in a significant way in the research and development of this concept in a Quebec context. This is more than a privacy issue, and the corresponding reform of other statutes may be necessary.

If the right to data portability is ultimately pursued, it will require:

A. **A phased-in approach that allows for the development and implementation of sector-specific frameworks:** We have learned from the GDPR model, which creates a sweeping data portability right but provides little clarity on implementation, that a more practical approach is essential.

   Sector-specific frameworks would need to be developed in consultation with industry to reflect the current practicalities and risks in each affected industry, and could be implemented through regulation. These frameworks must consider important economic, technical, authentication, security and operational issues. Other regulators beyond the Commission d'accès à l'information du Quebec should be involved in the enforcement of such frameworks, with the Commission overseeing issues related only to privacy compliance.

B. **Limits on the scope of ported data:** Providing data directly to an individual is an extension of the current right to access under Quebec's privacy law, which in its current form goes a long way to support consumer control. Individuals already have a right to access the personal information that an organization holds about them, to challenge its accuracy and completeness, and to have that information amended as appropriate. Organization-to-organization transfers must be done at the request of the individual. The right to data portability must be considered separately from the right to access, and the scope of data should not necessarily include all that is afforded under a typical access request.

   Ported data must be limited to personal information provided by the individual. Other types of data should generally be excluded, such as data that may be proprietary or not considered personal information. We support the government's stated intent that the proposed data portability right not cover information that was created, derived, calculated or inferred from data provided by the individual.

   Sector frameworks have the capacity to provide clarity on the scope of data appropriate for the objective of data portability, including limited data related to commercial transactions. With respect to higher risk or more sensitive data, it is advisable to limit the data fields that can be ported and strengthen authentication requirements.

   To avoid unnecessary disruption to standard business practices, the right to data portability must not automatically place an onus on an organization to delete ported data. Organizations must be permitted to follow standard policies and procedures around retention.

   In terms of format, ported data must be limited to digital data in technology neutral formats, in other words, a standardized digital format, where such a format exists, and not physical records to which normal access rights may apply. The Act must allow for solutions to emerge in each sector, and to evolve over time. As advancements occur, the scope of ported data could evolve accordingly.

   These rules must not create undue barriers for SMEs, as this would undermine the original intent of greater competition.

C. **Measures to protect against data breaches and fraud, and to ensure fair accountability:** Appropriate data security and authentication requirements must be in place to prevent data breaches and guard against fraudulent requests (possibly linked to the sensitivity of the data).

Portability must be conditional on the request being made by the individual (and not just the third-party organization), and on having an adequate sector-specific framework in place. Bulk or automated requests from third parties must be prohibited, and consent for the sharing or obtaining of ported information should not be buried in contracts.

An exclusion of liability must be in place when an organization is mandated by a consumer to port data to a third party. The responsibilities of the originating organization must be limited to confirming that the request is from the individual (i.e. not fraudulent) and to safely transferring the data. The originating organization must not be held responsible if the recipient organization falls short of its safeguarding obligations and other requirements under a sector-specific framework, leading to misuse of the data. Finally, the law should set out the bases on which an organization can object to a request for data portability.

For questions or comments regarding this submission, please contact:

Sara Clodman
VP, Public Affairs and Thought Leadership
sclodman@theCMA.ca

Fiona Wilson
Director, Government Relations
fwilson@theCMA.ca

About the CMA

The CMA is the voice of the marketing profession, representing more than 50 corporate, not-for-profit, public, and post-secondary members across Quebec, and contributing to the professional excellence of Quebec marketers through our events and professional development programs. Our community includes creative, media, and PR agencies, research firms, management consulting firms, technology companies and other suppliers to the marketing community. We support activities related to thought-leadership, professional development, consumer protection, and commercial success. We act as the primary advocate for marketing with governments, regulators and other stakeholders. Our Chartered Marketer (CM) designation ensures that marketing professionals are highly qualified and up to date with best practices. We champion self-regulatory standards, including the mandatory Canadian Marketing Code of Ethics and Standards.