Tableau sommaire des exigences plus contraignantes du projet de loi 64 par rapport à celles du Règlement général sur la protection des données

Le 12 juin 2020, à l'Assemblée nationale, le gouvernement du Québec a déposé le projet de loi 64, une *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, qui comporte des modifications importantes proposées à la *Loi sur la protection des renseignements personnels dans le secteur privé* (la « Loi du Québec »).

De nombreux nouveaux droits individuels et de nombreuses nouvelles exigences proposés par le projet de loi 64 sont semblables à ceux énoncés dans le *Règlement général sur la protection des données* (« RGPD »).

Souvent, toutefois, les exigences et d'autres dispositions du projet de loi 64 sont plus contraignantes, plus normatives ou simplement différentes du RGPD, notamment celles qui se rapportent à la responsabilisation, à la nouvelle « confidentialité par défaut », à un droit de « désactivation » étendu des fonctions d'identification, de localisation ou de profilage, aux circulations des données à l'extérieur du Québec, aux analyses d'impact, au consentement et aux exceptions au consentement, à la norme de protection des renseignements personnels, à la conservation des données, à la transparence, au processus décisionnel automatisé et aux multiples droits concernant les données. De plus, les variations de la terminologie employée pour les incidents de confidentialité en vertu du projet de loi 64 et les violations des données à caractère personnel du RGPD peuvent engendrer des différences au niveau des normes de notification, le seuil étant plus bas avec le projet de loi (un plus grand nombre d'incidents pouvant être signalés) par rapport au RGPD. De manière générale, contrairement au RGPD qui définit clairement les obligations légales des responsables du traitement et des sous-traitants, le projet de loi 64 n'est pas très explicite quant aux dispositions qui ne s'appliquent qu'aux responsables de la protection des renseignements personnels, ou à la fois à ces responsables et aux sous-traitants.

Par conséquent, si le projet de loi 64 est promulgué dans sa forme actuelle, les entreprises qui sont soumises à la Loi du Québec et qui ont mis en place des politiques, procédures et pratiques visant à se conformer au RGPD devront prendre une série de mesures accrues en vue de satisfaire les exigences du projet de loi 64 (dans la mesure où il est possible de faire, vu la sévérité de nombreuses dispositions du projet de loi).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Le tableau sommaire figurant dans le présent document présente les principales exigences proposées en vertu du projet de loi 64 (avec les renvois aux articles modifiés), et une brève description indiquant comment ces dispositions sont plus contraignantes, plus normatives ou simplement différentes des exigences du RGPD.

À des fins de clarté, le tableau sommaire ci-après ne présente pas les exigences ou les autres dispositions qui sont essentiellement semblables ou plus permissives que celles du RGPD, ou qui n'imposeraient pas un fardeau opérationnel à une organisation dont les politiques, procédures et pratiques sont en conformité avec le Règlement.

Pour les besoins de ce tableau, chaque fois que l'on mentionne dans le projet de loi 64 « toute personne qui exploite une entreprise », on considère qu'il s'agit du « responsable de la protection des renseignements personnels » (voir également Responsable de la protection des renseignements personnels/responsable du traitement ou sous-traitant).

Afin de faciliter la consultation, vous pouvez aller directement au sujet qui vous intéresse en utilisant la table des matières suivante :

Tableau sommaire 4

Dispositions du projet de loi 64 qui sont plus contraignantes ou plus normatives que celles du RGPD ou simplement différentes 4

Responsabilisation – Délégué à la protection des données/Responsable de la protection des renseignements personnels 4

Responsabilisation – Politiques et pratiques 5

Responsable de la protection des renseignements personnels/responsable du traitement ou sous-traitant 7

Protection des données dès la conception/confidentialité par défaut 8

Analyses d'impact 9

Consentement et autres autorisations légales pour le traitement 9

Limites de la collecte 12

Sécurité 13

Avis d'atteinte à la protection 14

Conservation des données 15

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Transparence	17
Prise de décision automatisée	19
Exactitude des données	19
Exigences relatives aux flux transfrontaliers de données	20
Droit d'accès	22
Droit à la portabilité des données	25
Droit de rectification	26
Droits à la limitation du traitement, droit d'opposition et droit à l'effacement (RGPD) c. droit à la cessation de la diffusion, à la réindexation ou à la désindexation (projet de loi du Québec)	27
Amendes, sanctions et droit aux dommages-intérêts	30

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

ACCESSPRIVACY BY OSLER

Tableau sommaire

Dispositions du projet de loi 64 qui sont plus contraignantes ou plus normatives que celles du RGPD ou simplement différentes

Responsabilisation – Délégué à la protection des données/Responsable de la protection des renseignements personnels

Responsabilité des cadres supérieurs en matière de protection des renseignements personnels

En vertu du projet de loi 64, la personne qui a « la plus haute autorité » (p. ex., le chef de la direction ou le président) est tenue d'exercer la fonction de « responsable » de la protection des renseignements personnels.

Au Québec, la législation actuelle stipule qu'un particulier qui ordonne ou autorise un acte ou une omission constituant une violation de la part du responsable de la protection des renseignements personnels au titre de cette loi est considéré comme partie à la violation et personnellement responsable des sanctions prescrites en vertu de la Loi. (Voir l'article 93, « Amendes, sanctions et droit aux dommages-intérêts ».)

Le RGPD n'impose pas de responsabilité semblable au chef de la direction ou au cadre supérieur qui est responsable du traitement (art. 37).

Approbation des politiques et pratiques

En vertu du projet de loi 64, le rôle du responsable comprend l'« approbation » des politiques et pratiques encadrant la gouvernance à l'égard des renseignements personnels (projet de loi 64, art. 3.2).

Dans le cas du RGPD, le délégué à la protection des données n'est pas explicitement tenu d'« approuver » les politiques et pratiques de gouvernance (art. 37-39).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Délégation des fonctions de « responsable »

En vertu du projet de loi 64, le responsable de la protection des renseignements personnels peut déléguer cette fonction en tout ou en partie à un « membre du personnel », mais il n'est pas précisé si ce membre du personnel doit être un employé du responsable (ou si un employé d'une société affiliée serait autorisé) (projet de loi 64, art. 3.1). Apparemment, toute personne à qui on délègue les fonctions de responsable serait exposée à la disposition de responsabilité personnelle dont il a été question précédemment.

Le RGPD autorise qu'un seul délégué soit nommé pour plusieurs organismes (ce qui n'est pas le cas pour le projet de loi 64, comme on l'a vu plus haut) (art. 37(3)).

Obligations du responsable à l'égard des demandes d'accès, de rectification et de désindexation

Le projet de loi 64 exige spécifiquement que le responsable participe directement au processus de réponse aux demandes d'accès, de rectification, de cessation de la diffusion ou de désindexation (projet de loi 64, art. 35).

Le RGPD n'impose pas qu'une personne en particulier soit chargée des réponses (mais voir l'article sur le délégué en général) (art. 37).

Responsabilisation – Politiques et pratiques

Norme de conformité

Le projet de loi 64 exige des organisations qu'elles mettent en œuvre des politiques et pratiques de gouvernance propres à « assurer » la protection des renseignements personnels (projet de loi 64, art. 3.2).

Le RGPD établit une norme moins contraignante en obligeant les organismes à prendre les mesures « appropriées » afin d'être conformes au Règlement (art. 12(1)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Contenu des politiques de gouvernance

Le projet de loi 64 stipule que les politiques et pratiques de gouvernance : i) prévoient l'encadrement applicable à la conservation et à la destruction des renseignements personnels; ii) prévoient les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements; iii) prévoient un processus de traitement des plaintes relatives à la protection de ceux-ci; et iv) sont proportionnées à la nature et à l'importance des activités de l'entreprise (projet de loi 64, art. 3.2).

Ces exigences normatives ne figurent pas explicitement dans le Règlement.

Approbation

Le projet de loi 64 exige que les politiques et pratiques de gouvernance soient approuvées par le responsable (projet de loi 64, art. 3.2).

Ce type d'approbation n'est pas prévu par le RGPD.

Respect d'un code de conduite/mécanisme de certification

Contrairement au RGPD, le projet de loi 64 ne prévoit pas l'application d'un code de conduite ou d'un mécanisme de certification approuvé comme élément pour démontrer le respect des obligations (art. 24, rec. 74.).

Osler, Hoskin & Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Responsable de la protection des renseignements personnels/responsable du traitement ou sous-traitant

Alors que de nombreuses dispositions du projet de loi 64 font mention de « toute personne qui exploite une entreprise » (notion qui englobe les responsables de la protection des renseignements personnels), un grand nombre d'entre elles font simplement référence à « une personne » ou « une personne ou un organisme », ce qui peut laisser supposer qu'elles s'appliquent à la fois aux responsables et aux sous-traitants. Voici des exemples :

- « personne qui recueille des renseignements personnels », en ce qui a trait aux droits d'accès individuels (art. 1.1, 8., 8.1 et 8.2);
- « personne qui détient des renseignements personnels pour le compte d'une personne qui exploite une entreprise » (art. 16) concernant les demandes d'accès ou de rectification;
- « personne ou organisme qui exerce un mandat ou exécute un contrat d'entreprise », relativement à l'exception au principe de consentement pour l'exécution d'un contrat (art. 18:3);
- « une personne ou un organisme qui souhaite utiliser ces renseignements à des fins d'étude » (art. 21); « une personne ou un organisme qui souhaite utiliser des renseignements personnels à des fins d'étude » (art. 21.0.1); et « une personne qui communique des renseignements personnels » (art. 21.0.2), en ce qui a trait à l'exception au principe de consentement pour les études, la recherche et les statistiques;
- « celui qui détient des renseignements faisant l'objet d'une demande » (art 36) d'accès ou de rectification;
- « personne qui détient le dossier » (art. 53), en rapport avec des désaccords au sujet de demande de rectification;
- « quiconque détient un renseignement » (art. 91), relativement aux infractions.

Il est impossible de déterminer avec certitude si ces dispositions veulent explicitement établir une distinction entre les responsables de la protection des renseignements personnels et les sous-traitants, et il n'est pas entièrement sûr non plus quelles dispositions du projet de loi 64 renfermant la mention « toute personne qui exploite une entreprise » s'appliquent aux sous-traitants.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Le RGPD est plus clair quant aux obligations des responsables du traitement par rapport aux sous-traitants, en fournissant les définitions de « responsables du traitement » (art. 4(7)) et de « sous-traitant » (art. 4(8)) et en énumérant les obligations spécifiques des sous-traitants (art. 28).

Protection des données dès la conception/confidentialité par défaut

Le projet de loi 64 renferme une exigence étendue et très contraignante selon laquelle un responsable de la protection des renseignements personnels qui recueille des renseignements personnels en « offrant un produit ou un service technologique doit s'assurer que, par défaut, les paramètres de ce produit ou de ce service assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée » (projet de loi 64, 9.1).

Le terme « confidentialité » n'est pas défini dans le projet de loi 64, mais son emploi dans d'autres dispositions du projet de loi laisse croire que cette notion se rapporte à la fois à la sécurité et à la protection des renseignements personnels. Cette disposition (art. 9.1) exige d'un responsable de la protection des renseignements personnels d'assurer, par défaut, le plus haut niveau de confidentialité.

La clause de « confidentialité par défaut » du projet de loi a une portée beaucoup plus étendue et est beaucoup plus contraignante que la notion de « confidentialité dès la conception » contenue dans le RGPD, qui impose aux responsables du traitement de mettre en œuvre « des mesures techniques et organisationnelles appropriées » qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (art. 25(1)).

De même, le RGPD exige également que les responsables du traitement mettent en œuvre les mesures techniques et organisationnelles « appropriées » pour garantir que, par défaut, « seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées » (art. 25(2)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Analyses d'impact

Le projet de loi 64 exige des responsables qu'ils procèdent à une évaluation des facteurs relatifs à la vie privée de « tout projet de système d'information ou de prestation électronique de services ». Ainsi, les responsables de la protection des renseignements personnels seraient tenus de mener des évaluations même lorsque les risques associés au traitement en question seraient faibles ou nominaux (projet de loi 64, art. 3.3).

Le RGPD exige la conduite d'une analyse d'impact relative à la protection des données d'une étendue beaucoup moins importante et dans beaucoup moins de circonstances, à savoir seulement lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (art. 35(1)).

Consentement et autres autorisations légales pour le traitement

Différences structurelles

Le projet de loi 64 établit la primauté du consentement en tant qu'autorisation par défaut pour le traitement des renseignements personnels.

Pour le RGPD, le consentement n'est pas une autorisation primaire ou par défaut pour le traitement des données à caractère personnel, et établit plus clairement d'autres fondements légaux et valides pour ce type de traitement (p. ex., nécessité contractuelle, respect d'obligations juridiques, intérêts vitaux, intérêt public, intérêts légitimes, droit de l'État membre) (RGPR, art. 6).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Consentement distinct

Parmi les exigences relatives au consentement, le projet de loi 64 stipule qu'il faut demander le consentement pour chacune des fins spécifiques, distinctement de toute autre information (projet de loi 64, art. 14).

Le RGPD n'exige pas explicitement de demander le consentement séparément.

Consentement explicite

Le projet de loi 64 exige un consentement explicite pour le traitement d'un « renseignement personnel sensible », qui est défini comme un renseignement qui « suscite un haut degré d'attente raisonnable en matière de vie privée » (projet de loi 64, art. 12).

Contrairement au RGPD, qui établit des catégories de données sensibles, le projet de loi impose une évaluation contextuelle au cas par cas, afin de déterminer si le consentement explicite sera nécessaire dans les circonstances.

Consentement tacite

Alors que le projet de loi 64 envisage le consentement explicite pour le traitement des renseignements personnels sensibles, il ne renferme pas de dispositions explicites concernant un consentement tacite ou présumé pour le traitement légal des renseignements personnels non sensibles. De plus, il n'est pas évident de voir comment une forme tacite de consentement pourrait avoir lieu, étant donné l'exigence selon laquelle un consentement doit être demandé à chacune des fins spécifiques, distinctement de toute autre information (selon l'article 14 du projet de loi).

Expiration du consentement

En vertu du projet de loi 64, le consentement n'est valide que pendant la période nécessaire pour atteindre la fin pour laquelle il avait été demandé (projet de loi 64, art. 14).

Les dispositions du RGPD relatives au consentement ne traitent pas expressément de la question de l'expiration ou d'autres aspects temporels liés au consentement.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Assistance

Le projet de loi 64 stipule que lorsque la personne le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé (projet de loi 64, art. 14).

Cela n'est pas prévu dans le Règlement.

Traitement autorisé sans consentement

Le projet de loi 64 autorise l'utilisation de renseignements personnels à une autre fin sans le consentement de la personne concernée dans les cas où celle-ci est « compatible » (« lien pertinent et direct ») avec les fins initiales (projet de loi 64, art. 17, art. 12).

Le RGPD est plus permissif en permettant de traiter ultérieurement les données à caractère personnel pour d'autres finalités qui ne sont pas « incompatibles » avec celles pour lesquelles les données ont été collectées initialement (rec. 50; art. 5(1)(b)), et une évaluation contextuelle est nécessaire afin de déterminer le degré de compatibilité dans les circonstances (art. 6(4)).

De plus, le RGPD autorise expressément le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, qui ne sont pas considérées comme « incompatibles » avec les fins initiales (art. 5(1)(b)).

Osler, Hoskin & Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Autres exceptions au consentement

En ce qui a trait aux exceptions suivantes au consentement, le projet de loi peut imposer des restrictions plus contraignantes sur les organisations que le RGPD :

- Utilisation de renseignements personnels à des fins de recherche et de production de statistiques (art. 12 (3)). Le projet de loi 64 exige la dépersonnalisation (définie à l'article 12) pour toutes ces utilisations, alors que le Règlement ne prévoit pas la « pseudonymisation » dans tous les cas (art. 6(4)(e)).
- Contrairement au RGPD, le projet de loi 64 n'autorise pas le traitement ultérieur à des fins archivistiques dans l'intérêt public (art. 5(1)(b)).
- Le projet de loi 64 établit que le traitement ultérieur des données pour la prospection commerciale ou philanthropique n'est pas autorisé (art. 12). Ce qui n'est pas le cas avec le RGPD.
- L'exception prévue dans le projet de loi 64 au consentement pour l'exécution d'un contrat comprend des exigences visant à établir des mesures pour assurer la protection du caractère confidentiel des renseignements personnels (projet de loi 64, art. 18.3), qui semblent plus normatives que celles de l'exception analogue figurant dans le RGPD (art. 6(1)(b)).

Limites de la collecte

Le projet de loi 64 limite la collecte de renseignements personnels aux renseignements « nécessaires aux fins déterminées avant la collecte », et renferme des dispositions qui stipulent qu'il doit y avoir un « intérêt sérieux et légitime » dans cette collecte (art. 1.1, 4, 5).

Le Règlement est moins contraignant, en permettant la collecte et le traitement des données à caractère personnel pour des finalités « déterminées, explicites et légitimes » (p. ex., la finalité n'a pas à être « sérieuse ») (art. 5(1)(b)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

ACCESSPRIVACY BY OSLER

Sécurité

Mesures de protection plus contraignantes/non qualifiées

Le projet de loi 64 introduit des dispositions qui imposent une norme très élevée de protection des renseignements personnels, qui ne concordent pas avec les exigences en matière de protection non modifiées.

Plus précisément, en vertu du projet de loi, une organisation est tenue de « protéger les renseignements personnels qu'elle détient » (art. 3.1) et d'établir et mettre en œuvre des politiques et pratiques de gouvernance qui « assurent » la protection de ces renseignements (projet de loi 64, art. 3.2).

De plus, les organisations qui recueillent des renseignements personnels en « offrant un produit ou un service technologique doit s'assurer que, par défaut, les paramètres de ce produit ou de ce service assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée » (projet de loi 64, art. 9.1) [nous soulignons].

Les mesures de protection des renseignements personnels qui figurent aux articles 3.1, 3.2 et 9.1 sont incompatibles avec les exigences qualifiées énoncées à l'article 10 qui stipule que les organisations doivent mettre en œuvre des mesures de sécurité qui sont « raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support » (projet de loi 64, art. 10).

La norme de protection du Règlement est moins contraignante, car elle exige des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (art. 5(1)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Approbation des politiques et pratiques

En vertu du projet de loi 64, les politiques et pratiques du responsable de la protection des renseignements personnels doivent être approuvées par le responsable de la protection des renseignements personnels (projet de loi 64, art. 3.2).

Le Règlement ne renferme aucune exigence selon laquelle une personne employée ou engagée par un responsable du traitement doit approuver les politiques et pratiques en matière de protection des données.

Avis d'atteinte à la protection

Avis d'« incident de confidentialité »

Le projet de loi 64 renferme une obligation de notification à la Commission d'accès à l'information et aux personnes concernées pour des « incidents de confidentialité » qui présentent un risque qu'un « préjudice sérieux » soit causé (projet de loi 64, art. 3.5).

La définition d'« incident de confidentialité » en vertu du projet de loi est différente de celle de « violation de données à caractère personnel » énoncée dans le Règlement. Plus particulièrement, dans le projet de loi, on entend par « incident de confidentialité », toute communication « non autorisée par la loi » de renseignements personnels et (plus généralement) « toute autre atteinte à la protection d'un tel renseignement ». L'étendue de l'expression « toute autre atteinte » et les variations terminologiques peuvent au bout du compte faire en sorte qu'un plus grand nombre d'incidents de confidentialité fassent l'objet d'une notification en vertu du projet de loi par rapport au Règlement.

De plus, le critère d'avis utilisé par le projet de loi 64 (« risque qu'un préjudice sérieux soit causé ») semble très semblable à celui du RGPD (qui exige d'informer les personnes concernées lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un « risque élevé » pour les droits et libertés des personnes physiques). De plus, les variations de la terminologie employée dans le projet de loi 64 et le RGPD peuvent donner lieu à des différences sur le plan des normes/critères d'avis, le seuil étant plus bas avec le projet de loi 64 (ce qui accroît le nombre d'incidents pouvant être signalés) par rapport au RGPD.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Absence d'obligation de notification spécifique pour les responsables de la protection des renseignements personnels/responsables du traitement et les sous-traitants

Les obligations de notification en vertu du projet de loi 64 s'appliquent à « toute personne qui exploite une entreprise » et contrairement au Règlement, ne traitent pas explicitement des différentes obligations touchant les responsables et les sous-traitants/fournisseurs. Toutefois, les contrats de service doivent renfermer une exigence selon laquelle le fournisseur doit aviser « sans délai » le responsable « de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué » (article 18.3).

Contrairement au RGPD, le projet de loi stipule qu'il faut tenir compte de critères précis pour évaluer le « risque de préjudice » et renferme l'obligation de consulter le responsable de la protection des renseignements personnels au sein de l'entreprise (projet de loi 64, art. 3.7).

Exigences qui doivent figurer dans des règlements

Certains détails, comme le contenu des avis et les exigences en matière de tenue de dossier seront exposés dans les règlements associés, ce qui fait qu'il n'est pas encore possible de savoir si ceux-ci seront plus sévères que dans le RGPD. Article 33.

Conservation des données

Période de conservation minimale prescrite

Le projet de loi 64 exige des responsables de la protection des renseignements personnels de conserver les renseignements utilisés pour prendre une décision pendant au moins un an suivant celle-ci (projet de loi 64, art. 11).

Le RGPD ne prévoit pas de période de conservation minimale (ou normative) des renseignements personnels et exige seulement qu'elles soient conservées « pendant une durée n'excédant pas celle nécessaire » (rec. 9; art. 5(1)(e)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Limite de la période de conservation

Le projet de loi 64 autorise la conservation des renseignements personnels après que les fins initiales ont été accomplies « sous réserve d'un délai de conservation prévue par la loi » (projet de loi 64, art. 23).

Le RGPD offre plus de souplesse en autorisant les responsables du traitement de conserver les données à caractère personnel pour une série plus étendue de finalités au-delà des finalités initiales du traitement, en particulier celles qui sont compatibles à ces finalités, ainsi que d'autres finalités spécifiées (voir rec. 39; art. 5(1)(e)).

Anonymisation

Lorsqu'une organisation anonymise des renseignements personnels qui ne sont plus nécessaires, elle doit le faire selon les « meilleures pratiques généralement reconnues » (projet de loi 64, art. 23). Selon le projet de loi 64, un renseignement personnel est « anonymisé » lorsqu'il ne « permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne », ce qui est une définition absolue et contraignante (projet de loi 64, art. 23).

Le RGPD ne prescrit aucune norme d'anonymisation (pseudonymisation dans le Règlement), et la définition de ce terme semble moins stricte que celle donnée par le projet de loi, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes « de telle manière que la personne concernée ne soit pas ou plus identifiable » (rec. 26).

Transparence de la période de conservation

Le projet de loi 64 stipule que la personne concernée doit être informée, sur demande, de la durée de conservation des renseignements personnels par le responsable de la protection des renseignements personnels (projet de loi 64, art. 14).

Le Règlement montre plus de souplesse en exigeant que le responsable du traitement fournisse à la personne concernée, au moment où les données à caractère personnel sont obtenues, la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée (art. 13(2)(a)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Transparence

Publication des politiques

Le projet de loi 64 exige d'un responsable du traitement qu'il publie ses politiques de gouvernance interne sur son site Web ou, s'il n'a pas de site, par un autre moyen approprié (projet de loi 64, art. 3.2).

Le RGPD n'exige pas d'un responsable du traitement qu'il affiche publiquement ses politiques de gouvernance interne.

Politique en matière de confidentialité

Le projet de loi 64 exige qu'une personne (c.-à-d. un responsable du traitement ou sous-traitant) qui recueille par un moyen technologique des renseignements personnels publie une politique de confidentialité (et toute version modifiée de celle-ci) sur son site Web, en plus de la diffuser par tout moyen propre à atteindre les personnes concernées (projet de loi 64, art. 8.2). La portée exacte du contenu de cette politique et les situations où sa publication serait nécessaire ne sont pas clairement établies, vu le libellé de la disposition et l'absence dans le présent projet de loi d'une définition pour le terme « confidentialité ».

La portée du contenu pour des exigences semblables en matière de transparence est exprimée plus clairement dans le RGPD (art. 12-14).

Information sur les moyens par lesquels les renseignements sont recueillis

Le projet de loi 64 exige qu'une personne soit informée des moyens par lesquels les renseignements sont recueillis au moment de la collecte (projet de loi 64, art. 8).

Le RGPD ne requiert pas explicitement un tel avis au moment de la collecte, que ces données aient ou non été obtenues auprès des personnes concernées : se reporter aux art. 13-14.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Transparence et demandes d'accès

Dans le cadre des obligations d'un responsable du traitement de donner suite à une demande d'accès, le projet de loi 64 exige que, sur demande, une personne soit informée (i) des moyens par lesquels ses renseignements personnels sont recueillis et (i) des catégories de personnes qui ont accès à ses renseignements personnels au sein de l'entreprise (projet de loi 64, art. 8).

Aucune exigence n'est prévue en vertu du RGPD pour fournir le type d'information précitée par suite d'une demande d'accès.

Exigences en matière de transparence à l'égard des technologies d'identification, d'emplacements ou de profilage

Le projet de loi 64 énonce une exigence générale selon laquelle, si les renseignements personnels de la personne concernée sont recueillis en ayant recours à une technologie qui comprend des fonctions permettant de « l'identifier, de la localiser ou d'effectuer un profilage de celle-ci », le responsable du traitement doit au préalable l'informer du recours à une telle technologie et des moyens offerts pour désactiver les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage (projet de loi 64, art. 8.1).

Bien que, en vertu du RGPD, le responsable du traitement doit faire preuve de transparence relativement à l'existence du processus décisionnel automatisé, y compris le profilage, et fournir des renseignements utiles sur la logique du processus (voir l'alinéa 13, 2(f)), un droit de « désactivation » fort étendu ressemble au droit d'opposition du RGPD, mais va plus loin (art. 21).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Prise de décision automatisée

Le projet de loi 64 exige que les responsables du traitement qui utilisent des renseignements personnels afin de rendre une décision « fondée exclusivement sur un traitement automatisé de ceux-ci » en informent la personne concernée. Cette obligation d'avis, telle qu'elle est rédigée, serait applicable dans toutes les circonstances mettant en cause des décisions fondées sur un traitement automatisé, peu importe la pertinence des répercussions de la décision sur la personne concernée.

Les dispositions du RGPD quant à la prise de décision automatisée sont moins contraignantes, puisque les responsables du traitement sont soumis à des obligations de transparence ayant une portée générale (contrairement à l'obligation d'avis prévue dans le projet de loi 64) (alinéa 13(2)(f)), et le droit d'une personne à s'opposer à la décision s'applique seulement si la décision produit « des effets juridiques la concernant ou l'affectant de manière significative » (par. 22(1)).

Exactitude des données

Le projet de loi 64 établit une exigence non qualifiée pour les responsables du traitement qui doivent veiller à ce que les renseignements personnels soient à jour et exacts lorsqu'ils sont utilisés pour une prise de décision (c.-à-d. qu'il n'existe aucune limite de temps ou circonstance pour la mise à jour des renseignements personnels) (projet de loi 64, art. 11).

Aux termes du RGPD, l'exigence de conservation est qualifiée, les renseignements personnels ne sont tenus à jour que « si nécessaire » (rec. 39; alinéa 5(1)(d)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Exigences relatives aux flux transfrontaliers de données

Portée des obligations

Le projet de loi 64 prévoit des dispositions très restrictives et onéreuses concernant le flux transfrontalier de données, qui s'appliquent à la communication de renseignements personnels entre des responsables du traitement et le transfert vers des sous-traitants tiers.

Les règles sur le transfert transfrontalier du projet de loi 64 s'appliquent à toutes les communications de renseignements personnels à l'extérieur du Québec (y compris les communications vers d'autres provinces et territoires au Canada (projet de loi 64, article 17), contrairement au RGPD qui restreint seulement les communications vers des pays ou territoires en dehors de l'Espace économique européen (EEE) (RGPD, art. 45).

Évaluation des facteurs relatifs à la vie privée

Le projet de loi 64 prévoit qu'avant de communiquer à l'extérieur du Québec un renseignement personnel, le responsable de la protection des renseignements personnels doit procéder à une évaluation des facteurs relatifs à la vie privée et la communication ne peut être effectuée que si :

(i) le responsable de la protection des renseignements personnels détermine que le renseignement bénéficierait dans l'autre territoire d'une protection équivalente à celle prévue à la présente loi;

(ii) elle fait l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation et des risques identifiés dans le cadre de cette évaluation.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Protection équivalente dans d'autres territoires

Le projet de loi 64 prévoit la publication par le ministre d'une liste d'États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection, bien qu'il ne soit pas certain si une évaluation des facteurs relatifs à la vie privée ou une entente écrite qui tient compte des risques (comme il est décrit plus haut) devra être obtenue pour la communication de renseignements personnels dans les États figurant sur cette liste (projet de loi 64, art. 17.1).

Absence d'autorité légitime pour les flux transfrontaliers de données lorsqu'il n'y a pas de protection équivalente

Dans la forme actuelle de l'article 17 du projet de loi 64, il serait interdit aux responsables du traitement de communiquer des renseignements personnels à l'extérieur du Québec si le régime juridique applicable dans l'État en question n'offre pas une protection équivalant à celle prévue dans le projet de loi 64, même si la personne concernée a consenti explicitement à la communication, ou si le responsable de la protection a conclu une entente écrite qui oblige le destinataire à protéger les renseignements personnels de manière conforme aux dispositions du projet de loi 64.

Dans le RGPD, les restrictions concernant le transfert de données vers un pays tiers sont beaucoup plus souples, car les diverses bases juridiques autres que l'adéquation pour le responsable de la protection de transférer les renseignements personnels à l'extérieur de l'UE, notamment le consentement explicite, les clauses types, les obligations contractuelles, les codes de conduite et les règles d'entreprise contraignantes (RGPD, art. 49).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

ACCESSPRIVACY BY OSLER

Droit d'accès

Notification de droits

Le projet de loi 64 prévoit qu'une personne (soit un responsable du traitement ou un sous-traitant) qui recueille les renseignements personnels doit informer la personne concernée des droits d'accès et de rectification prévus par la loi (projet de loi 64, art. 8).

Les dispositions relatives au droit d'accès du RGPD s'appliquent seulement aux responsables du traitement et stipulent que, au moment où les données à caractère personnel sont obtenues auprès d'une personne concernée, le responsable du traitement fournit l'information sur l'existence du droit de demander l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci ou une limitation du traitement relatif à la personne concernée (alinéa 13(2)(b)).

Portée du droit

En vertu du projet de loi 64, chaque personne (soit un responsable du traitement ou un sous-traitant) qui détient un renseignement personnel sur autrui doit en confirmer l'existence à la personne concernée et lui permettre d'en obtenir une copie (projet de loi 64, art. 27).

Le RGPD prévoit qu'un responsable du traitement (mais non un sous-traitant) doit fournir à la personne concernée la confirmation que des données à caractère personnel la concernant sont traitées et l'accès auxdites données ainsi que les informations prescrites (par. 15(1)).

En vertu du projet de loi 64, une demande d'accès pourra être formulée par une personne qui indique qu'elle est la personne concernée, son représentant, son héritier ou successeur et autre personne précisée : se reporter au projet de loi 64, art. 30. Le RGPD ne comporte aucune disposition équivalente et n'accorde un accès qu'à la personne concernée.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Forme de réponse

Le projet de loi 64 prévoit que, par suite d'une demande, un renseignement personnel informatisé doit être communiqué sous la forme d'une « transcription écrite et intelligible » (projet de loi 64, art. 27). Si la personne concernée est une personne handicapée, des « mesures d'accommodement raisonnables » doivent être prises par suite d'une demande (projet de loi 64, art. 27).

En vertu du RGPD, l'information doit être fournie sous « une forme électronique d'usage courant » lorsqu'une demande est présentée par voie électronique (par. 15(3)).

Délai de réponse

Le projet de loi 64 exige que le responsable réponde à une demande d'accès « avec diligence » et au plus tard dans les 30 jours (projet de loi 64, art. 32). Aucune disposition n'est prévue pour prolonger cette période.

(Le RGPD prévoit une réponse « dans les meilleurs délais » et, dans tous les cas, dans un délai d'un mois : se reporter au par. 12(3)).

Le RGPD autorise, à l'égard de droits semblables, une prolongation de deux mois au besoin, compte tenu de la complexité et du nombre de demandes (par. 12(3)).

Personne qui exerce la fonction de responsable

Se reporter à la rubrique sur la personne qui exerce la fonction de responsable pour les autres obligations relatives aux droits de demander l'accès aux données et aux exigences en matière de délai.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Refus

En vertu du projet de loi 64, il faut motiver tout refus d'acquiescer à une demande et indiquer la disposition de la loi sur laquelle ce refus s'appuie, les recours qui s'offrent au requérant, le délai dans lequel ils peuvent être exercés, en plus de prêter assistance, à la demande du requérant, pour l'aider à comprendre le refus (projet de loi 64, art. 34).

En vertu du RGPD, lorsqu'un responsable du traitement entend refuser de répondre à une demande, le responsable du traitement est seulement tenu, d'une façon moins prescriptive, de motiver sa réponse lorsqu'il n'a pas l'intention de donner suite aux demandes d'accès (rec. 59).

Personnes décédées

En vertu du projet de loi 64, une personne pourrait avoir accès aux renseignements personnels d'une personne décédée si elle est le conjoint ou le proche parent de la personne décédée et si la connaissance de ce renseignement est susceptible d'aider le requérant dans son processus de deuil et que la personne décédée n'a pas consigné par écrit son refus d'accorder ce droit d'accès (art. 40.1).

En règle générale, les données des personnes décédées sortent du champ d'application du RGPD (sauf dans la mesure où elles se rapportant également à une personne vivante).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

ACCESSPRIVACY BY OSLER

Droit à la portabilité des données

Les dispositions du projet de loi 64 qui énoncent la portée du droit d'accès s'appliquent généralement au droit à la portabilité des données. Les différences énoncées entre le projet de loi 64 et le RGPD sont notables, puisque le contexte québécois offre un droit à la portabilité beaucoup plus étendu, comparativement au RGPD (art. 20) :

- Le droit à la portabilité des données prévu dans le projet de loi 64 s'applique à la réception, dans tous les cas, de renseignements informatisés, à moins que cela ne soulève des difficultés pratiques sérieuses (projet de loi 64, art. 27). Le RGPD limite le droit à la portabilité des données aux constances suivantes :
    - la personne concernée a « fourni » (les autorités de contrôle en font une interprétation large de sorte à inclure les données « observées », mais compte non tenu des données inférées ou obtenues) des renseignements personnels en premier lieu;
    - les données sont automatisées (c.-à-d. aucun document papier);
    - la base juridique pour le traitement est le consentement ou l'exécution d'un contrat ou les étapes préparatoires à un contrat.
- Le RGPD n'accorde un droit à la portabilité des données qu'à la personne concernée. Le projet de loi 64 autorise un plus large éventail de personnes à soumettre des demandes, dont les représentants, les héritiers et les successeurs (se reporter au projet de loi 64, art. 30).
- Le projet de loi 64 accorde un droit à la portabilité pour les données concernant une personne décédée (projet de loi 64, art. 40.1). En règle générale, les données des personnes décédées sortent du champ d'application du RGPD (sauf dans la mesure où elles se rapportant également à une personne vivante).
- Contrairement au projet de loi 64, en vertu du RGPD, il y a une exception au droit à la portabilité si une demande est manifestement infondée ou excessive, notamment en raison de son caractère répétitif, le responsable du traitement pourra refuser de donner suite à la demande ou exiger le paiement de frais raisonnable (par. 12(5)).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Droit de rectification

Portée du droit

Le projet de loi 64 autorise un large éventail de personnes à soumettre des demandes de rectification, dont les représentants, les héritiers et les successeurs (projet de loi 64, art. 30). Le RGPD n'accorde un droit de rectification qu'à la personne concernée (art. 16).

Le projet de loi 64 accorde un droit de rectification pour les données concernant une personne décédée (projet de loi 64, art. 30). En règle générale, les données des personnes décédées sortent du champ d'application du RGPD (sauf dans la mesure où elles se rapportant également à une personne vivante).

Le projet de loi 64 accorde un droit de rectification à l'égard de données équivoques ou si la conservation ou la collecte n'est pas autorisée par la loi, de même que les renseignements inexacts et incomplets (projet de loi 64, art. 28). Le droit de rectification prévu dans le RGPD est limité aux données inexactes et incomplètes (art. 16).

Contrairement au RGPD, le droit de rectifier un renseignement personnel incomplet prévu dans le projet de loi 64 n'est pas limité à la finalité du traitement. Pour cette raison, le projet de loi 64 exige de façon plus générale des sous-traitants qu'ils prennent des mesures pour rectifier les renseignements personnels, peu importe la finalité du traitement, tandis que le RGPD stipule que la finalité doit être prise en compte (art. 16).

Fardeau de la preuve

Advenant un désaccord, le projet de loi 64 exige que la personne qui détient le dossier prouve que le fichier n'a pas à être rectifié, à moins que le renseignement en cause ne lui ait été communiqué par la personne concernée ou avec son accord (projet de loi 64, art. 53).

Le RGPD ne mentionne pas expressément le fardeau de la preuve du responsable du traitement (bien que, conformément au principe de responsabilité, un responsable de traitement doit être en mesure de démontrer sa conformité au principe d'exactitude).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Personne qui exerce la fonction de responsable et délai

Se reporter à la rubrique sur le droit d'accès pour connaître les obligations relatives aux demandes et les exigences en matière de délai.

Exceptions

Le projet de loi 64 ne prévoit aucune exception au droit de rectification, contrairement au RGPD et aux lois nationales des États membres.

Rejet

Contrairement au RGPD, le projet de loi 64 exige que le responsable :

- indique la disposition de la loi sur laquelle ce refus s'appuie;
- précise le délai dans lequel il peut exercer des recours;
- prête assistance au requérant, à sa demande, pour l'aider à comprendre le refus (projet de loi 64, art. 34).

Droits à la limitation du traitement, droit d'opposition et droit à l'effacement (RGPD) c. droit à la cessation de la diffusion, à la réindexation ou à la désindexation (projet de loi du Québec)

Portée du droit

Le projet de loi 64 confère le droit de faire **cesser la diffusion du renseignement ou de désindexer** tout hyperlien associé (projet de loi 64, art. 28.1), si cette diffusion contrevient à la loi ou à une ordonnance judiciaire, lorsque certaines conditions s'appliquent. Le RGPD ne confère pas de tels droits, mais accorde un **droit à la limitation du traitement** (**art. 18**) et un **droit d'opposition** (**art. 21**) ainsi qu'un **droit à l'effacement ou « droit à l'oubli »** (**art. 17**), qui pourraient offrir le même résultat.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Comparaison de la portée des droits :

- Le droit d'exiger la cessation de la diffusion ou la désindexation dans le projet de loi 64 émane de circonstances différentes des droits à la limitation du traitement, à l'opposition et à l'effacement prévus dans le RGPD. En vertu du projet de loi 64, une personne pourrait exiger la cessation de la diffusion ou la désindexation d'hyperliens lorsque :
    - la diffusion de ce renseignement cause à la personne concernée un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée;
    - ce préjudice est manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement;
    - la cessation de la diffusion, la réindexation ou la désindexation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice (projet de loi 64, art. 28.1).
- À l'opposé, en vertu du RGPD :
    - une **personne pourrait exiger une limitation au traitement** dans certains cas mettant en cause l'exactitude contestée, l'exercice ou la défense de droits en justice ou lorsque le responsable du traitement vérifie s'il faut mettre fin au traitement, auquel cas les données peuvent être conservées, mais non utilisées : se reporter à l'art. 18 pour obtenir des précisions;
    - Le **droit d'opposition** au traitement peut être exercé lorsque les données sont traitées à des fins de prospection, de recherche scientifique ou historique ou à des fins statistiques, ou sur une base juridique dans l'intérêt légitime ou public, sous réserve de certaines exceptions pour les tâches d'intérêt public ou des motifs légitimes et impérieux : se reporter à l'art. 21;
    - le **droit à l'effacement ou à l'oubli** (**art. 17**) peut être exercé dans un certain nombre de situations, notamment le retrait du consentement et s'il n'existe pas d'autre fondement juridique, ou lorsque les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

- Le projet de loi 64 confère également le droit d'exiger la réindexation dans les mêmes circonstances où elles ont le droit de faire cesser la diffusion du renseignement ou de désindexer les hyperliens (projet de loi 64, art. 28.1). Un tel droit n'est pas prévu dans le RGPD.
- Le projet de loi 64 autorise un plus large éventail de personnes à soumettre des demandes pour la cessation de la diffusion, l'indexation ou la réindexation, dont les représentants, les héritiers et les successeurs (projet de loi 64, art. 30). Le RGPD confère un droit à la limitation du traitement, à l'effacement et d'opposition qu'à la seule personne concernée (art. 17, art. 18, art. 21).

Personne qui exerce la fonction de responsable (le responsable)

Se reporter à la rubrique sur le droit d'accès pour connaître les obligations relatives aux demandes et les exigences en matière de délai.

Exceptions

Le projet de loi ne prévoit aucune exception aux droits de cessation de diffusion, de désindexation et de réindexation, contrairement au RGPD et aux dispositions nationales des États membres à l'égard de droits semblables. En vertu du RGPD, le droit d'opposition, le droit à la limitation du traitement et le droit à l'effacement comportent des exceptions, lorsque la demande n'est manifestement pas fondée ou qu'elle est excessive, notamment en raison de son caractère répétitif. Le droit à l'effacement contient d'autres exceptions, lorsque le traitement est notamment nécessaire pour l'exercice du droit à la liberté d'expression et d'information, des raisons de santé publique et des motifs d'intérêt public : (se reporter à l'art. 17).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Rejet d'une demande

Advenant un refus de cesser la diffusion, de désindexer ou de réindexer, le projet de loi 64, contrairement au RGPD, exige que le responsable :

- indique la disposition de la loi sur laquelle ce refus s'appuie;
- précise le délai dans lequel il peut exercer des recours;
- prête assistance au requérant, à sa demande, pour l'aider à comprendre le refus (se reporter au projet de loi 64, art. 34).

Amendes, sanctions et droit aux dommages-intérêts

Catégories des amendes et des sanctions

En vertu du projet de loi 64, il existe deux types de sanctions pécuniaires :

1. **amendes** pouvant atteindre 25 000 000 $ ou le montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé, à la perpétration de certaines infractions (projet de loi 64, art. 91);
2. **sanctions administratives pécuniaires** pouvant atteindre 10 000 000 $ ou le montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé, à la perpétration des infractions énumérée (projet de loi 64, art. 90.12).

Osler, Hoskin & Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Ces catégories sont le reflet des deux tranches d'amendes figurant dans le RGPD (à l'art. 83), en fonction de la gravité de l'infraction :

1. **Les infractions plus graves** font l'objet d'une amende maximale de 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

2. Les **infractions moins graves** font l'objet d'une amende maximale de 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Portée des amendes et des sanctions

Malgré les catégories analogues, les sanctions sont susceptibles d'être plus onéreuses en vertu du projet de loi 64 que du RGPD :

- **Sanctions potentiellement plus élevées pour des infractions équivalentes :** Par exemple, en vertu du RGPD, le défaut de se conformer aux exigences de consentement pour des services d'une société de l'information offerts directement à une personne mineure est classé comme une infraction moins grave (RGPD, par. 83(4)). En vertu du projet de loi 64, l'utilisation de renseignements personnels en contravention à une partie quelconque de la Loi (ce qui comprend le défaut de se conformer aux obligations en matière de consentement d'une personne mineure) est passible d'une amende maximale de 25 000 000 $ ou du montant correspondant à 4 % du chiffre d'affaires mondial si ce dernier montant est plus élevé (projet de loi 64, art. 91). Cependant, en vertu du projet de loi 64, le chiffre d'affaires est établi pour l'entité juridique en cause et, contrairement au RGPD, il ne tient pas compte de la totalité de l'unité économique. Cela signifie qu'une amende au titre du RGPD pourrait être supérieure dans certains cas.

- **Infraction particulière de « ré-identification » :** En vertu du projet de loi 64, quiconque commet une infraction qui procède ou tente de procéder à l'identification d'une personne physique à partir de renseignements dépersonnalisés sans l'autorisation de la personne les détenant ou à partir de renseignements anonymisés est passible d'amendes (projet de loi 64, par. 91(3)). Aucune infraction équivalente n'est prévue dans le RGPD.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

- **Amende automatiquement portée au double en cas de récidive** En vertu du projet de loi 64, dans le cas d'une infraction subséquente, les amendes sont automatiquement portées au double (projet de loi 64, art. 92.1). En vertu du RGPD, les infractions antérieures pertinentes sont prises en compte pour établir le montant des amendes, mais sans augmentation automatique. Lorsque l'amende est portée au double en raison d'une infraction antérieure, l'amende maximale en vertu du projet de loi 64 est supérieure à celle prévue en vertu du RGPD (8 % c. 4 % du chiffre d'affaires mondial), bien que, tel qu'il est mentionné précédemment, ce chiffre d'affaires soit calculé différemment pour les besoins du RGPD.
- **Absence de plafond cumulatif :** En vertu du RGPD, si la même activité de traitement ou une activité semblable enfreint plusieurs dispositions, l'amende ne dépassera pas le montant précisé pour la plus grave des violations. Bien que le projet de loi 64 limite les amendes cumulatives pour les violations d'une même disposition, aucun plafond n'est fixé pour les violations multiples de différentes dispositions découlant des mêmes activités de traitement ou d'activités associées.
- **Amendes minimales :** Le projet de loi 64 prévoit une amende minimale pour des infractions en vertu de la Loi de 5 000 $ dans le cas d'une personne physique et de 15 000 $ dans le cas des organismes (projet de loi 64, art. 91). Le RGPD ne prévoit pas d'amendes minimales.

- **Responsabilité personnelle :** Au Québec, la loi établit déjà la responsabilité personnelle d'un administrateur, d'un dirigeant ou d'un représentant de la personne qui ordonne ou autorise un acte ou une omission qui constitue l'infraction ou expose ces personnes aux sanctions prescrites en vertu de la Loi. Le projet de loi 64 ne modifie pas cette disposition (art. 93), mais il augmente considérablement l'exposition personnelle. La responsabilité personnelle n'a pas cette forme dans le RGPD, bien que cela puisse être le cas dans les dispositions nationales des États membres.
- **Critère de fixation des sanctions :** Le projet de loi 64 pourrait, dans certains cas, être plus rigoureux que le RGPD au moment de fixer des sanctions administratives pécuniaires ou des amendes. En particulier, le cadre d'application des critères qui doivent guider la décision d'imposer une sanction administrative pécuniaire en vertu du projet de loi 64 (par. 90.2(2)) diffère des critères prévus à l'art. 83 du RGPD, notamment, à l'égard de ce qui suit :
    - la Commission pourrait tenir compte du « risque » de préjudice aux termes du cadre prévu dans le projet de loi 64, tandis

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

que seuls les dommages réels sont pris en compte en vertu du RGPD;

- le cadre d'application du projet de loi 64 ne tient pas compte de l'application ou non par la personne qui exerce la fonction de responsable/le responsable d'un code de conduite approuvé;
- le cadre d'application du projet de loi 64 ne prévoit pas de disposition fourre-tout pour tout autre facteur aggravant/atténuant;
- le cadre d'application du projet de loi 64 tient compte des mesures prises pour remédier au « manquement », tandis que le RGPD se concentre sur les mesures prises pour atténuer le « dommage ».

- **Appels auprès de la Cour du Québec :** En vertu du projet de loi 64, les appels sont interjetés devant la Cour du Québec, plutôt que la Cour supérieure (pour les sanctions administratives pécuniaires, se reporter à l'art. 90.9). En outre, l'art. 90.9 prévoit que la contestation des sanctions administratives pécuniaires est assujettie aux règles prévues aux articles 61 à 69 de la Loi actuelle. Cela signifie que seuls les appels sur une question de droit ou de compétence (art. 61) sont possibles et que la décision du juge de la Cour du Québec est sans appel (art. 69). Par conséquent, la seule voie pour poursuivre la contestation serait par l'entremise d'un contrôle judiciaire devant la Cour supérieure, qui n'offre qu'un champ d'intervention fort limité à cette Cour et aux autres tribunaux d'appel. Ces recours limités sont une source de préoccupation, étant donné l'ampleur potentielle des sanctions administratives pécuniaires pouvant être en cause, car ces montants dépasseraient largement la compétence normale de la Cour du Québec qui, pour les questions de droit civil, est limitée aux réclamations de moins de 85 000 $ et, dans un tel cas, compte tenu de tous les droits d'appel de la Cour d'appel du Québec.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

Droits aux dommages-intérêts sur la base d'une indemnisation

Le projet de loi 64 prévoit des droits aux dommages-intérêts comme indemnisation en cas de dommage (art. 93.1). En vertu du RGPD, il existe un droit à la réparation pour « un dommage matériel ou moral » qui est subi (RGPD, art. 82).

Responsable du traitement seulement

Le projet de loi 64 n'établit pas de responsabilité pour un dommage causé par les sous-traitants, contrairement au RGPD, qui prévoit qu'un sous-traitait est responsable du dommage causé par le traitement, seulement s'il n'a pas respecté les obligations prévues dans le RGPD qui incombent spécifiquement aux sous-traitants ou s'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci (RGPD, art. 82).

Exemption de responsabilité

Le projet de loi 64 prévoit un critère différent et sans doute plus limité pour l'exemption de responsabilité (« force majeure ») que le RGPD (« ne lui est nullement imputable »).

Dommages-intérêts minimaux/punitifs

Le projet de loi 64 impose des dommages-intérêts punitifs en cas de fautes lourdes ou intentionnelles (1 000 $, se reporter au projet de loi 64, art. 93.1). Le RGPD n'en prévoit pas.

Responsabilité conjointe

Le projet de loi 64 ne mentionne pas la responsabilité conjointe de plusieurs responsables pas plus qu'il n'offre la possibilité de récupérer les dommages-intérêts auprès des sous-traitants ou d'autres responsables participant au même traitement. Le RGPD aborde la responsabilité conjointe à l'art. 82.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres cons`eils professionnels.

ACCESSPRIVACY BY OSLER

Comparaison des éléments clés de la réforme des dispositions législatives en matière de protection des renseignements personnels proposée par le gouvernement du Québec avec le Règlement général sur la protection des données de l'Union européenne (UE)

En juin 2020, le gouvernement du Québec a déposé le projet de loi 64, une *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, qui comporte des modifications importantes proposées à la *Loi sur la protection des renseignements personnels dans le secteur privé* (la « Loi du Québec sur la protection des renseignements personnels »).

De nombreux nouveaux droits individuels et de nombreuses nouvelles exigences proposés par le projet de loi 64 sont semblables à ceux énoncés dans le *Règlement général sur la protection des données (UE)* (« RGPD »). Souvent, toutefois, ces exigences et d'autres dispositions du projet de loi 64 sont plus contraignantes, plus normatives ou simplement différentes du RGPD et sont particulières à la province de Québec.

Si le projet de loi 64 est promulgué dans sa forme actuelle, les entreprises qui sont soumises à la loi du Québec et qui ont mis en place des politiques, procédures et pratiques visant à satisfaire les exigences du RGPD devront prendre des mesures accrues en vue d'assurer leur conformité au projet de loi (dans la mesure où il est possible de le faire, vu la sévérité de nombreuses dispositions du projet de loi). Par ailleurs, le projet de loi 64 expose les entreprises à des sanctions financières élevées et des dommages-intérêts encore plus importants que ceux prévus dans le RGPD.

Étant donné les coûts élevés des mesures de conformité aux exigences particulières et contraignantes du projet de loi 64 et les graves risques financiers liés à son régime d'application, il est raisonnable de penser que celui-ci (dans sa forme actuelle) provoquera le retrait de nombreux produits ou services du marché québécois et la relocalisation de certaines activités d'entreprises établies au Québec hors de la province.

Certains commentateurs ont dévoilé de quelles manières le RGPD a nui aux entreprises, à l'innovation numérique, au marché du travail et aux consommateurs au sein de l'UE. [1] En introduisant des exigences et des sanctions plus sévères que celles du RGPD, il est raisonnable de penser que les répercussions au Québec du projet de loi 64 seront plus marquées que celles du RGPD dans l'Union européenne.

Le tableau ci-dessous récapitule les principales différences entre le projet de loi 64 et le RGPD, et présente leurs répercussions attendues. Ce tableau est suivi d'un compte rendu plus détaillé de la façon dont les dispositions du projet de loi sont plus contraignantes, normatives ou simplement différentes de celles du RGPD.

[1] Voir par exemple : What the Evidence Shows About the Impact of the GDPR After One Year (L'impact démontré du RGPD une année après son entrée en vigueur) (https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/); Regulations like GDPR will make big tech stronger (Les règlements comme le RGPD rendront les sociétés de haute technologie encore plus puissantes) (https://qz.com/1332215/regulations-like-gdpr-will-make-big-tech-stronger/).

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Circulation des données hors territoire	Le projet de loi 64 prévoit qu'avant de communiquer à l'extérieur du Québec un renseignement personnel, le responsable de la protection des renseignements personnels doit procéder à une évaluation des facteurs relatifs à la vie privée et la communication ne peut être effectuée que si : (i) le responsable de la protection des renseignements personnels détermine que le renseignement bénéficierait dans l'autre territoire d'une protection équivalente à celle prévue à la présente loi. (ii) elle fait l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation et des risques identifiés dans le cadre de cette évaluation. Les entreprises pourraient être empêchées de communiquer des renseignements personnels à l'extérieur du Québec si le régime juridique applicable dans l'État en question n'offre pas une protection équivalant à celle prévue dans le projet de loi 64, même si la personne concernée a consenti explicitement à la communication, ou si le responsable de la protection a conclu une entente écrite qui oblige le destinataire à protéger les renseignements personnels de manière conforme aux dispositions du projet de loi.	Dans le RGPD, les restrictions concernant le transfert de données vers un pays tiers sont beaucoup plus souples, car les diverses bases juridiques autres que l'adéquation pour le responsable de la protection de transférer les renseignements personnels à l'extérieur de l'UE, notamment le consentement explicite, les clauses types, les obligations contractuelles, les codes de conduite et les règles d'entreprise contraignantes (art. 49).	Les dispositions très restrictives et très coûteuses du projet de loi 64 concernant la circulation des données hors frontières pourraient empêcher les entreprises du Québec d'utiliser de nombreux produits et services disponibles sur le marché, y compris l'infrastructure infonuagique, les solutions de commerce en ligne, les plates-formes de paiement en ligne, et les outils de marketing et de relations avec la clientèle. Les multinationales établies au Québec envisageront sérieusement de déplacer leurs activités administratives destinées à conserver et traiter les renseignements sur les clients et les employés dans un autre territoire (afin de pouvoir communiquer les données à leurs activités mondiales). Les entreprises engageront des dépenses substantielles et subiront des retards significatifs dans leurs activités afin d'évaluer le degré d'équivalence de la protection des renseignements personnels dans chaque territoire (y compris dans les autres provinces canadiennes) vers laquelle les renseignements personnels pourraient être communiqués, ce qui apparaît impossible sur le plan pratique.

Osler, Hoskin &Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Confidentialité par défaut	Le projet de loi 64 exige d'un gestionnaire des renseignements personnels qui recueille des renseignements personnels en offrant un produit ou un service technologique qu'il s'assure que, par défaut, les paramètres de ce produit ou de ce service assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée (art. 9.1).	La clause « confidentialité par défaut » du projet de loi est beaucoup plus vaste et beaucoup plus stricte que le concept de « protection des données dès la conception » énoncé dans le RGPD (qui exige du responsable du traitement qu'il mette en œuvre des « mesures techniques et organisationnelles appropriées » qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective, compte tenu de la nature, le de la portée, du contexte et des finalités du traitement ainsi que des risques) (art. 25(1)). Le RGPD exige par ailleurs du responsable du traitement qu'il mette en œuvre des mesures techniques et organisationnelles « appropriées » pour garantir que, par défaut, « seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées » (art. 25(2)).	Souvent, les organisations qui ont appliqué le principe de la « protection des données dès la conception » pour leurs produits et services, conformément aux dispositions du RGPD, ne seront pas conformes aux exigences très contraignantes de la « confidentialité par défaut » du projet de loi. Vu la taille réduite du marché du Québec, Il n'est pas réaliste de s'attendre à ce que des sociétés technologiques établies à l'étranger créent des versions personnalisées de leurs produits et services afin de satisfaire cette exigence particulière du projet de loi.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Comparaison sommaire du projet de loi 64 et du Règlement général sur la protection des données (RGPD)

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Évaluations des répercussions des données	Le projet de loi 64 exige des entreprises qu'elles procèdent à une évaluation des facteurs relatifs à la vie privée de « tout projet de système d'information ou de prestation électronique de services ». Les responsables de la protection des renseignements personnels doivent effectuer des évaluations, même lorsque le risque associé à l'activité en question est faible ou minime (art. 3.3).	Le RGPD exige une analyse de l'impact sur la protection des données uniquement si le traitement est susceptible d'engendrer un « risque élevé » pour les droits et libertés des personnes physiques (art. 35(1)).	Les entreprises qui ont des activités au Québec devront consacrer les ressources nécessaires pour effectuer un nombre beaucoup plus élevé d'évaluations que si elles étaient dans une autre territoire. Vu la taille réduite du marché du Québec, les entreprises situées à l'extérieur de la province pourraient ne plus offrir leurs produits et services sur ce marché.

Osler, Hoskin &Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Comparaison sommaire du projet de loi 64 et du Règlement général sur la protection des données (RGPD)

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Consentement et autres autorisations légales pour le traitement	Primauté du consentement Le projet de loi 64 renforce la primauté du consentement comme l'autorisation par défaut préalable au traitement des renseignements personnels en vertu de la loi. Consentement distinct Le projet de loi 64 stipule qu'il faut demander le consentement pour chacune des fins spécifiques, distinctement de toute autre information (art. 14). Consentement explicite Le projet de loi 64 exige un consentement explicite pour le traitement d'un « renseignement personnel sensible », qui est défini comme un renseignement qui « suscite un haut degré d'attente raisonnable en matière de vie privée » (art. 12). Consentement tacite Il n'y a pas de dispositions explicites dans le projet de loi 64 concernant un consentement tacite ou présumé pour le traitement légal des renseignements personnels non sensibles. De plus, il n'est pas évident de voir comment une forme tacite de consentement pourrait avoir lieu, étant donné l'exigence selon laquelle un consentement doit être demandé à chacune des fins spécifiques, distinctement de toute autre information (selon l'article 14).	Primauté du consentement Le consentement n'est pas considéré comme une autorisation primaire ou par défaut pour le traitement des renseignements personnels. Le RGPD établit d'autres fondements légaux et valides pour le traitement des renseignements personnels (p. ex., nécessité contractuelle, respect d'obligations juridiques, intérêts vitaux, intérêt public, intérêts légitimes, droit de l'État membre) (art. 6). Consentement distinct Le RGPD n'exige pas explicitement de demander le consentement séparément. Consentement explicite Le RGPD établit des catégories prescrites de renseignements sensibles. Consentement tacite Même si le RGPD ne fait pas mention du consentement tacite, le consentement ne constitue que l'une des nombreuses bases valides pour le traitement des données à caractère personnel.	Les entreprises qui sont soumises à la Loi du Québec sur la protection des renseignements personnels et qui ont mis en place des politiques, procédures et pratiques visant à se conformer au RGPD devront prendre une série de mesures accrues en vue de satisfaire les exigences du projet de loi 64 relatives au consentement. Les entreprises engageront ainsi des frais substantiels et devront limiter l'utilisation des renseignements personnels d'une manière autorisée en vertu du RGPD.

Osler, Hoskin &Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

	Expiration du consentement En vertu du projet de loi 64, le consentement n'est valide que pendant la période nécessaire pour atteindre la fin pour laquelle il avait été demandé (art. 14). Traitement autorisé sans consentement Le projet de loi 64 autorise l'utilisation de renseignements personnels à une autre fin sans le consentement de la personne concernée dans les cas où les fins sont « compatibles » (« lien pertinent et direct ») avec les fins auxquelles le renseignement a été recueilli (art. 17, art. 12). Autres exceptions au consentement Le projet de loi 64 exige qu'un renseignement personnel utilisé sans le consentement de la personne concernée à des fins de recherche ou de production de statistiques soit dépersonnalisé (art. 12(3)). Le projet de loi 64 n'autorise pas le traitement ultérieur des renseignements à des fins d'archivage dans l'intérêt public. Il établit que le traitement ultérieur des renseignements à des fins de prospection commerciale ou philanthropique n'est pas autorisé (art. 12).	Expiration du consentement Les dispositions du RGPD concernant le consentement ne traitent pas expressément de la question de l'expiration ou d'autres aspects temporels liés au consentement. Traitement autorisé sans consentement Le RGPD est plus permissif en permettant de traiter ultérieurement les données à caractère personnel pour une finalité secondaire qui n'est pas « incompatible » avec les finalités initiales de la collecte (rec. 50; art. 5(1)(b)). Une évaluation contextuelle est nécessaire afin de déterminer le degré de compatibilité dans les circonstances (art. 6(4)). Le RGPD autorise expressément le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (art. 5(1)(b)). Autres exceptions au consentement Le RGPD n'exige pas la « pseudonymisation » dans tous les cas où des renseignements personnels sont utilisés à des fins de recherche et de production de statistiques (art 6(4)(e)). Le RGPD n'établit pas que le traitement ultérieur des données pour la prospection commerciale ou philanthropique n'est pas autorisé (art. 12).	

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Comparaison sommaire du projet de loi 64 et du Règlement général sur la protection des données (RGPD)

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Décisions automatisées	Le projet de loi 64 régit toute décision fondée exclusivement sur un traitement automatisé des renseignements personnels, sans exception (art. 12.1).	En vertu du RGPD, les règles applicables aux décisions automatisées ne s'appliquent que si une décision touche le statut juridique ou les droits légaux d'une personne ou a un impact équivalent sur les circonstances, le comportement ou les choix de la personne. De plus, le Règlement prévoit certaines dérogations, y compris lorsqu'une décision automatisée est nécessaire à la conclusion ou l'exécution d'un contrat entre la personne concernée et un responsable du traitement (art. 22).	Les entreprises établies au Québec déploieront moins de processus décisionnels automatisés (p. ex., IA) (en raison des exigences relatives aux avis de réunion, à la transparence et à l'« analyse des décisions » contenues dans le projet de loi 64, même lorsqu'une décision n'a pas d'incidence importante sur le statut juridique ou les droits légaux d'un particulier). Le Québec pourrait devenir un lieu moins propice à la création, à l'exploitation et au développement d'entreprises qui vendent ou utilisent des solutions IA, ou moins attrayant pour les investissements dans ce secteur. Toutes les activités de recherche-développement dans le domaine de l'intelligence artificielle auraient probablement lieu à l'extérieur du Québec. On assisterait à une baisse du nombre de nouvelles entreprises d'IA au Québec. Les entreprises existantes dans ce secteur auraient tendance à se relocaliser à l'extérieur du Québec.

Osler, Hoskin &Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Désactivation des fonctions d'identification, de localisation ou de profilage	Une entreprise qui déploie une technologie comprenant des fonctions permettant d'identifier et de localiser la personne concernée et d'effectuer un profilage de celle-ci doit au préalable l'informer du recours à une telle technologie et des moyens offerts pour désactiver ces fonctions (art. 8.1).	Même si un responsable du traitement doit être transparent relativement à l'existence du processus décisionnel automatisé, y compris le profilage, et fournir des renseignements utiles sur la logique du processus (art. 13, 2(f)), le « droit de désactivation » du projet de loi 64 semble plus vaste que le droit d'opposition du RGPD (art. 21).	Les entreprises établies au Québec devront engager des frais et consacrer des ressources en vue d'appliquer et de gérer un droit de désactivation qui est plus étendu que le droit équivalant contenu dans le RGPD. Les entreprises de haute technologie établies à l'extérieur du Québec devraient créer des versions de leurs produits et services particulières au Québec, afin de satisfaire ces exigences spécifiques.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Cessation de diffusion, désindexation et réindexation	Le projet de loi 64 donne aux personnes concernées le droit de faire cesser la diffusion du renseignement ou de désindexer tout hyperlien associé (art. 28.1), si cette diffusion contrevient à la loi ou à une ordonnance judiciaire, lorsque certaines conditions s'appliquent. Les personnes concernées ont aussi le droit d'exiger la réindexation dans les mêmes circonstances où elles ont le droit de faire cesser la diffusion du renseignement ou de désindexer les hyperliens (projet de loi 64, art. 28.1). Le projet de loi ne prévoit aucune exception aux droits de cessation de diffusion, de désindexation et de réindexation.	Le RGPD donne aux particuliers le droit à la limitation du traitement (art. 18) et le droit d'opposition (art. 21) ainsi qu'un droit à l'effacement « droit à l'oubli » (art. 17). Le RGPD ne comporte pas de droit de réindexation. En vertu du RGPD, le droit d'opposition, le droit à la limitation du traitement et le droit à l'effacement sont assujettis à des exceptions, lorsque la demande n'est manifestement pas fondée ou qu'elle est excessive, notamment en raison de son caractère répétitif. Le droit à l'effacement contient d'autres exceptions, lorsque le traitement est notamment nécessaire pour l'exercice du droit à la liberté d'expression et d'information, des raisons de santé publique et des motifs d'intérêt public (art. 17).	Les entreprises qui sont soumises à la Loi du Québec sur la protection des renseignements personnels et qui ont mis en place des politiques, procédures et pratiques visant à se conformer au RGPD devront prendre une série de mesures accrues et engager des frais substantiels en vue de satisfaire les exigences plus contraignantes du projet de loi 64 relativement à la cessation de la diffusion, à la désindexation et à la réindexation des hyperliens.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Conservation des données	<u>Période de conservation minimale prescrite</u> Le projet de loi 64 exige des responsables de la protection des renseignements personnels de conserver les renseignements utilisés pour prendre une décision pendant au moins un an suivant celle-ci (art. 11). <u>Limite de la période de conservation :</u> Le projet de loi 64 autorise la conservation des renseignements personnels après que les fins initiales ont été accomplies « sous réserve d'un délai de conservation prévue par la loi » (art. 23).	<u>Période de conservation minimale prescrite :</u> Le RGPD ne prévoit pas de période de conservation minimale (ou normative) des renseignements personnels et exige seulement qu'elles soient conservées « pendant une durée n'excédant pas celle nécessaire » (rec. 39; art. 5(1)(e)).	Les entreprises qui sont soumises à la Loi du Québec sur la protection des renseignements personnels et qui ont mis en place des politiques, procédures et pratiques visant à se conformer au RGPD devront prendre une série de mesures accrues et engager des frais substantiels en vue de satisfaire les exigences plus contraignantes du projet de loi 64 relativement à la conservation des renseignements personnels.

Osler, Hoskin &Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
	Anonymisation : Lorsqu'une organisation anonymise des renseignements personnels qui ne sont plus nécessaires, elle doit le faire « selon les meilleures pratiques généralement reconnues ». (art. 23). Selon le projet de loi 64, un renseignement personnel est « anonymisé » lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne. Transparence de la période de conservation : Le projet de loi 64 stipule que la personne concernée doit être informée, sur demande, de la durée de conservation des renseignements personnels (art. 8).	Limite de la période de conservation : Le RGPD offre plus de souplesse en autorisant les responsables du traitement de conserver les données à caractère personnel pour une série plus étendue de finalités au-delà des finalités initiales du traitement, en particulier celles qui sont compatibles à ces finalités, ainsi que d'autres finalités spécifiées (voir rec. 39; art. 5(1)(e)). Anonymisation : Le RGPD ne prescrit aucune norme d'anonymisation, et la définition de ce terme semble moins stricte que celle donnée par le projet de loi, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable (rec. 26). Transparence de la période de conservation : Le Règlement montre plus de souplesse en exigeant que le responsable du traitement fournisse à la personne concernée, au moment où les données à caractère personnel sont obtenues, la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée (art. 13(2)(a)).	

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Comparaison sommaire du projet de loi 64 et du Règlement général sur la protection des données (RGPD)

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Responsabilisation	Un chef de la direction ou un président d'entreprise doit approuver les politiques et pratiques de gouvernance à l'égard des renseignements personnels (art. 3.2) et participer directement à la réponse aux demandes d'accès, de rectification, de cessation de la diffusion ou de désindexation (art. 35).	Il n'existe pas d'obligations explicites correspondantes pour un chef de la direction ou un président d'entreprise.	Cette disposition de responsabilisation peut accroître de manière sensible les risques personnels pour un chef de la direction ou un président d'entreprise, car au Québec, la législation actuelle stipule qu'un particulier qui ordonne ou autorise un acte ou une omission constituant une violation de la part du responsable de la protection des renseignements personnels au titre de cette loi, est considéré comme partie à la violation et personnellement responsable des sanctions prescrites en vertu de la loi.
Avis d'incident de confidentialité	Le projet de loi 64 renferme une obligation pour le commissaire et les particuliers d'aviser d'un « incident de confidentialité » qui présente un « risque qu'un préjudice sérieux soit causé » (art. 3.5). Dans le projet de loi, on entend par « incident de confidentialité », toute communication « non autorisée par la loi » de renseignements personnels et (plus généralement) « toute autre atteinte à la protection d'un tel renseignement ».	Dans le cas du RGPD, le seuil d'avis est sans doute plus élevé à la fois au niveau i) du degré de préjudice (« risque élevé » pour les droits et libertés des personnes physiques, plutôt que le « risque qu'un préjudice sérieux soit causé » du projet de loi 64); et ii) de la définition d'une « violation de données à caractère personnel » (qui est le terme comparable à « incidents de confidentialité » dans le projet de loi) (art. 33).	Les entreprises qui sont soumises à la Loi du Québec sur la protection des renseignements personnels et qui ont mis en place des politiques, procédures et pratiques visant à se conformer au RGPD (ou d'autres lois sur la protection des renseignements personnels, comme la LPRPDE) devront prendre une série de mesures accrues et engager des frais substantiels en vue de satisfaire les exigences du projet de loi 64 relativement aux avis en cas d'incident de confidentialité.

Osler, Hoskin &Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Norme relative à la protection des renseignements personnels	Le projet de loi 64 renferme une exigence absolue pour que toute organisation assure la « protection des renseignements personnels qu'elle détient », ce qui oblige les responsables de la protection d'établir et de mettre en œuvre des politiques et pratiques de gouvernance propres à « assurer » cette protection (c.-à-d., qu'il n'y a aucun concept qualifiant ce qu'est une mesure de protection raisonnable ou appropriée) (art. 3.2). Ces dispositions sont toutefois en contradiction avec les exigences qualifiées énoncées dans l'article 10 « raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support » (art. 10).	Dans le cas du Règlement, la norme de protection est moins sévère, car on parle de « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adaptée au risque » (art. 5(1)).	La norme plus sévère de protection des renseignements personnels existant au Québec (combinée aux autres sanctions prévues dans le projet de loi 64) incitera les entreprises à restreindre les données conservées ou traitées dans la province. Les entreprises auront également tendance à relocaliser leurs activités à l'extérieur du Québec.

Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

Comparaison sommaire du projet de loi 64 et du Règlement général sur la protection des données (RGPD)

Question en cause	Projet de loi 64	RGPD	Exemples de répercussions attendues
Sanction	Le projet de loi 64 établit un régime de responsabilité sans faute qui rend l'entreprise automatiquement responsable (à moins que le préjudice résulte d'une force majeure) des préjudices causés par la violation des droits conférés par la Loi du Québec sur la protection des renseignements personnels ou des droits au respect de sa réputation et de sa vie privée conférés dans le Code civil du Québec (art. 93.1). Combiné à la norme de protection des renseignements confidentiels (art. 3.2), le projet de loi 64 établit potentiellement un régime de responsabilité absolue pour les incidents de confidentialité. Le projet de loi 64 impose des dommages-intérêts punitifs d'au moins 1 000 $ pour les fautes lourdes (art. 93.1). Il prévoit des sanctions administratives pécuniaires maximales pouvant s'élever à 8 % du chiffre d'affaires mondial, qui correspond à deux fois les amendes maximales prévues au sein de l'UE, même si la population du Québec équivaut à 2 % de la population des membres de l'UE (art 92.1). Le projet de loi 64 n'établit pas de plafond pour les violations multiples de différentes dispositions découlant des mêmes activités de traitement ou d'activités associées.	Le RGPD n'établit pas de responsabilité absolue pour les violations de données à caractère personnel. Il ne prévoit pas de dommages-intérêts punitifs minimaux. Les amendes prévues par le RGPD ne doublent pas en cas de récidive (p. ex., passant de 4 % à 8 % du chiffre d'affaires mondial). Le RGPD n'établit pas de plafond pour les violations multiples de différentes dispositions découlant des mêmes activités de traitement ou d'activités associées.	Les dispositions du projet de loi 64 relatives aux sanctions devraient accroître le nombre de litiges liés à la protection des renseignements personnels au Québec, y compris les recours collectifs. Les entreprises établies au Québec devront évaluer si le risque accru de poursuite et l'établissement de sanctions administratives pécuniaires non proportionnelles à la taille du marché de la province justifient d'envisager de relocaliser leurs activités dans un autre territoire.

Osler, Hoskin &Harcourt LLP
Le présent document fournit seulement des renseignements généraux et ne donne pas de conseils juridiques ou autres conseils professionnels.

ACCESSPRIVACY BY OSLER

Comparison of Key Elements of Quebec's Proposed Privacy Law Reform, Bill 64, and the General Data Protection Regulation (EU)

On June 12, 2020, at the National Assembly, the Quebec government tabled Bill 64, An Act to modernize legislative provisions as regards the protection of personal information, which includes significant proposed amendments to an Act Respecting the Protection of Personal Information in the Private Sector (the "Quebec Act").

Many of the new requirements and individual rights proposed in Bill 64 are similar to those within the General Data Protection Regulation (EU) ("GDPR").

However, in many instances the requirements and other provisions under Bill 64 are more stringent, prescriptive or otherwise distinct from the requirements set out under the GDPR, including the requirements under Bill 64 relating to accountability, a novel "confidentiality by default" requirement, a broad "deactivation" right for identification, location or profiling functions, transborder data flows, data impact assessments, consent and exceptions to consent, the standard for information security, data retention, transparency, automated decision making, and multiple subject matter data rights. In addition, differences in security breach terminology under Bill 64 and the GDPR may result in different standards for the notification trigger under the two statutes, and a lower threshold for notification (and more data incidents being notifiable) under Bill 64 compared to the GDPR. More broadly, unlike the GDPR which provides clarity as to the statutory obligations of data controllers and processors, it is unclear from the drafting of Bill 64 as to precisely which provisions under the Act are intended to apply only to data controllers, or to both controllers and processors.

As such, if Bill 64 is enacted in its current form, companies who are subject to the Quebec Act that have established policies, procedures and practices to comply with the GDPR will need to take a series of additional steps to operationalize their compliance with Bill 64 (to the extent it is even practicable to even do so, given the stringent features of many provisions in the Bill).

The table below provides a description of the manner in which Bill 64's provisions are more stringent, prescriptive or otherwise distinct from the GDPR. This comparison table has been prepared in tandem with the Summary Table of Key Elements of Bill 64 and the GDPR which summarizes the key differences between Bill 64 and the GDPR and the anticipated impacts of these distinctions.

This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

For clarity, the table below does not list requirements or other provisions that are substantively similar or more permissive than under the GDPR, or that otherwise would not impose an operational burden on an organization whose policies, procedures and practices comply with the GDPR.

For the purposes of this table, references under Bill 64 to a "person carrying on an enterprise" are referred to as "data controllers" (see also Controller vs. Processor).

For ease of reference, you may navigate to a topic of interest using the following Table of Contents:

Summary Table 4

Bill 64 Provisions that are more Stringent, Prescriptive or otherwise Distinct from the GDPR 4

- Accountability - Data Protection Officer/Person in Charge 4
- Accountability - Policies and Practices 5
- Controller vs. Processor 7
- Data Protection by Design/Confidentiality by Default 8
- Data Impact Assessments 9
- Consent and other Legal Authority for Processing 9
- Limitation of Collection 12
- Security 13
- Security Breach Notification 14
- Data Retention 15
- Transparency 17
- Automated Decision Making 19
- Data Accuracy 19
- Transborder Data Flow Requirements 20
- Right of Access 21
- Right of Data Portability 24

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Right of Rectification 25
Rights of Restriction, Objection and Erasure (GDPR) vs. Right to Cessation of Dissemination, De-indexing, and Re-indexing (Quebec Bill) 27
Fines, Penalties and Statutory Right of Damages 30

This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Summary Table Bill 64 Provisions that are more Stringent, Prescriptive or otherwise Distinct from the GDPR
Accountability - Data Protection Officer/Person in Charge
Senior Executive Responsibility for Data Protection Under Bill 64, the individual who has the "highest authority" (e.g. the Chief Executive Officer or President) is required to exercise the function of a "person in charge" ("PIC") of the data controller's protection of personal information. The Quebec Act currently provides that an individual who orders or authorizes an act or omission that constitutes an offence of the data controller under the statue, is deemed to be a party to the offence and is personally liable to prescribed penalties under the Act. (See s. 93, "Fines, Penalties and Statutory Right of Damages"). The GDPR does not impose a similar responsibility on a data controller's CEO or senior executive. (Art. 37) Approval of Policies and Practices Under Bill 64, the PIC role includes "approving" governance policies and practices regarding personal information. (Bill 64, s. 3.2) Under the GDPR, the DPO is not expressly required to "approve" governance policies and practices. (Art. 37-39)

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Delegation of "Person in Charge" Functions

Under Bill 64, the PIC may delegate all or part of that function to a "personnel member", although it is unclear whether the "personnel member" must be an employee of the particular data controller (or whether an employee of an affiliate would be permitted) (Bill 64, s. 3.1). Presumably, any individual who is delegated PIC functions would be exposed to the personal liability provision under the Quebec Act (as described above).

The GDPR permits a group of companies to appoint a single DPO (and as noted above, Bill 64 may not permit this). (Art. 37(3))

Obligations on PIC Regarding Requests for Access, Rectification, De-indexing

Bill 64 specifically required the PIC to be directly involved In response to requests for access, rectification, ceasing dissemination or de-indexing, (Bill 64, s. 35).

The GDPR does not require any particular person to be involved in requests (though see section on DPO generally). (Art. 37)

Accountability - Policies and Practices

Standard for Compliance:

Bill 64 stringently requires organizations to implement governance policies and practices that "ensure" the protection of information. (Bill 64, s. 3.2)

The GDPR sets out a less stringent standard by requiring companies to take "appropriate" measures to demonstrate compliance with the GDPR. (Art. 12(1))

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Content of Governance Policies:

Bill 64 requires that governance policies and practices: (i) provide a framework for the keeping and destruction of personal information; (ii) define the roles and responsibilities of the members of its personnel throughout the life cycle of the personal information; (iii) provide a process for dealing with complaints regarding the protection of the personal information; and (iv) are proportionate to the nature and scope of the enterprises activities. (Bill 64, s. 3.2)

These prescriptive content requirements are not expressly contained in the GDPR.

Approval:

Bill 64 requires that governance policies and practices be approved by the PIC. (Bill 64, s. 3.2)

Such an approval is not required by the GDPR.

Adherence to codes of conduct / certification schemes:

Bill 64 does not provide for adherence to an approved code of conduct or certification mechanisms to be used as an element by which to demonstrate compliance, unlike the GDPR. (Art. 24, Rec. 74.)

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Controller vs. Processor

While many provisions in Bill 64 refer to "persons carrying on an enterprise" (a concept that includes data controllers), there are multiple provisions drafted with reference merely to "a person" or a "person or body" that suggests that those provisions may apply to both data controllers and data processors. These include:

- "person who collects personal information", regarding individual rights of access and certain notice provisions (ss. 1.1, 8, 8.1 and 8.2);
- "person holding personal information on behalf of person carrying on an enterprise" (s. 16), regarding referring requests for access or rectification;
- "person or body carrying out a mandate or performing a contract of enterprise", regarding the exception to consent related to performance of a contract (s. 18.3);
- "person or body wishing to use the information for study" (s. 21); "person or body wishing to use personal information for study" (s. 21.0.1); and "person who communicates personal information" (s. 21.0.2), regarding the exception to consent related to study/research/statistics;
- "person holding information that is the subject of a request" (s. 36) for access or rectification;
- "person holding the file" (s. 53), in relation to disagreements about requests for rectification;
- "person holding the information" (s. 91), regarding offences.

This document is provided for general information purposes only and does not constitute legal or other professional advice.

It is unclear whether these provisions were expressly intended to make a distinction between data controllers and processors, and it is otherwise it's not entirely clear which provisions in Bill 64 that refer to "a person carrying on an enterprise" may apply to processors.

The GDPR provides more clarity about the obligations of controllers vs. processors, by including definitions of "controller" (Art. 4(7)) and "processor" (Art. 4(8)). and specifically enumerates the obligations that apply only to processors (Art. 28).

Data Protection by Design/Confidentiality by Default

Bill 64 contains a broad and very stringent requirement whereby a data controller who collects personal information when "offering a technological product or service must ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned." (Bill 64, 9.1).

The term "confidentiality" is not defined by Bill 64, but the use of the term "confidentiality" in other provisions of the Bill suggests that the concept refers to both security and privacy. As such, this provision appears to require a data controller to implement the "highest level of security and privacy, by default." (Bill 64, 9.1)

Bill 64's "confidentiality by default" clause in section 9.1 is far broader in scope and significantly more stringent than the "privacy by design" concept under the GDPR, which requires the data controller to implement "appropriate technical and organizational measures" for implementing data protection principles in an effective manner, taking into account the nature, scope, context, risks and purposes of processing. (Art. 25(1)).

Similarly, the GDPR also requires data controllers to implement "appropriate" technical and organizational measures to ensure that by default, "only personal data which are necessary for each specific purpose of the processing are processed." (Art. 25(2))

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Data Impact Assessments

Bill 64 requires data controllers to conduct an assessment of the privacy-related factors to be undertaken for use of "any information system project or electronic service delivery project". As drafted, data controllers would be required to conduct assessments even in circumstances where there may be low or nominal risk associated with the personal information processing activity in question. (Bill 64, s. 3.3).

The GDPR requires a data protection impact assessment ("DPIA") for processing in far less breadth and volume of circumstances, namely only where the processing is likely to result in a 'high risk' to the rights and freedoms of natural persons. (Art. 35(1))

Consent and other Legal Authority for Processing

Structural Differences

Bill 64 enhances the primacy of consent as the default authority for processing personal information under the statute.

Under the GDPR consent is not a primary or default authority for processing personal information, and more clearly sets out other lawful and valid bases for processing of personal data (e.g. contractual necessity, compliance with legal obligations, vital interests, public interest, legitimate interests, or pursuant to a power of a Member state. (Art. 6)

This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Separate Consent:

Among the requirements for consent, Bill 64 requires that consent be requested for each specific purpose, separately from any other information. (Bill 64, s. 14)

The GDPR does not expressly require that consent be sought separately.

Express Consent

Bill 64 requires express consent for the processing of "sensitive personal information", which is defined as information that "entails a high level of reasonable expectation of privacy" (Bill 64, s. 12).

Unlike the GDPR, which sets out prescribed categories of sensitive information, Bill 64 will operationally require a contextual assessment on a case-by-case basis to determine whether express consent would be required in the circumstances.

Implied Consent

While Bill 64 contemplates express consent for the processing of sensitive personal information, there is no express provision in Bill 64 for an implied, or assumed, consent for the lawful processing of non-sensitive personal information. Moreover, it is not clear how an implied form of consent can practically be operationalized given that requirement that consent be "requested for each specific purpose, separately from other information (as required under s. 14 of the Bill).

Expiration of Consent:

Under Bill 64, consent is valid only for the time necessary to achieve the purpose for which it was requested. (Bill 64, s. 14)

The GDPR's consent provisions do not expressly address the expiration or other temporal aspects of consent.

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

Assistance:

Bill 64 requires that if requested, assistance be provided to an individual to understand the scope of consent requested. (Bill 64, s. 14)

This is not required by the GDPR.

Permissible Processing Without Consent:

Bill 64 permits the use of personal information as a secondary purpose without the consent of the individual concerned if it is used for purposes "consistent" (a "direct and relevant connection") with the purposes for which it was collected. (Bill 64, s. 17, s. 12)

The GDPR more permissively allows personal data to be further processed for secondary purposes that are not "incompatible" with the initial purposes for its collection (Rec.50; Art.5(1)(b)), and a contextual assessment is required to determine the extent of compatibility in the circumstances. (Art .6(4)).

Moreover, the GDPR expressly permits the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, are not considered "incompatible" with initial purposes. (Art.5(1)(b)).

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and
does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Other Exceptions to Consent:

In regard to the following exceptions to consent, Bill 64 may impose more stringent requirements on organizations than the GDPR:

- The use of personal information for research and the production of statistics (s. 12(3)). Bill 64 requires de-identification (defined at s. 12) for all such uses, whereas the GDPR does not require the equivalent "pseudonymization" in all cases. (Art 6(4)(e)).
- Bill 64 does not allow for further processing for archiving purposes in the public interest, unlike the GDPR (Art. 5(1)(b)).
- Bill 64 sets out that further processing of data for commercial or philanthropic prospection is not permissible (s.12). The GDPR does not.
- Bill 64's exception to consent for the performance of a contract includes requirements to specify measures to protect confidentiality of the personal information (Bill 64, s.18.3), which appear more prescriptive than the requirements for the analogous exception in the GDPR. (Art. 6(1)(b))

Limitation of Collection

Bill 64 prohibits the collection of personal information to circumstance to where it is "necessary" for the purposes determined before collecting it", and contains provisions which suggest that there must be a "serious and legitimate reason" for the collection (ss. 1.1,4, 5).

The GDPR more permissively allows you to collect and process personal data for "specified, explicit and legitimate" purposes (e.g. the purpose for collection does not have to be "serious"). (Art. 5(1)(b))

This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Security

More Stringent/Unqualified Safeguarding Measures

Bill 64 introduces provisions that impose a very high information security standard that are inconsistent with the unamended information security requirements under the statute.

Specifically, under Bill 64 organizations are required to "protect personal information held by a person" (Bill 64, s. 3.1) and establish and implement governance policies and practices that "ensure" the protection of such information. (Bill 64, s. 3.2)

Bill 64 also requires organizations who collect personal information when "offering a technological product or service must ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned." (Bill 64, s. 9.1)

The information security standards in sections 3.1, 3.2 and 9.1 are inconsistent with the qualified requirements set out in section 10 of the Act which provides that organizations must implement security measures that are "reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored." (Bill 64, s. 10)

The GDPR's standard for safeguarding is less stringent, as it requires "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." (Art. 5(1))

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Approval of Policies and Practices

Under Bill 64, a data controller's policies and practices must be approved by the person in charge of the protection of personal information. (Bill 64, s. 3.2).

There is no requirement under the GDPR for an individual employed or engaged by a data controller to approve information security policies and practices.

Security Breach Notification

Notification of "Confidentiality Incidents"

Bill 64 contains a mandatory breach notification obligation to the Commissioner and individuals for "confidentiality incidents" that present a "risk of serious injury" (Bill 64, s. 3.5).

The definition of a "confidentiality incident" under Bill 64 is different than the definition of a "personal data breach" under the GDPR. In particular, Bill 64 defines a "confidentiality incident" to include the communication of personal information "not authorized by law" and (more broadly) "any other breach in the protection of such information." The breadth of the phrase "any other breach" and the differences in terminology may ultimately result in a broader set of security incidents being subject to Bill 64's notification regime compared to the mandatory breach reporting regime under the GDPR.

In addition, the notification trigger under Bill 64 ("risk of serious injury") appears substantively similar to the notification trigger concept under the GDPR (which requires notification to individuals where a personal data breach is likely to result in a "high risk" to individuals' rights and freedoms). However, the difference in notification trigger terminology under Bill 64 and the GDPR may result in different standards for the notification trigger, and perhaps a lower threshold for notification (and more data incidents being notifiable) under Bill 64, compared to the GDPR.

This document is provided for general information purposes only and does not constitute legal or other professional advice.

No Specific Notification Obligations for Controllers vs. Processors

The notification obligations under Bill 64 apply to "any person carrying on an enterprise" and, unlike the GDPR, do not expressly address the different notification obligations on "controllers" vs. "processors." However, service provider contracts are required to include a requirement for the service provider to notify the outsourcing entity "without delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated." (s. 18.3)

Unlike the GDPR, Bill 64 requires that specific criteria be considered in assessing the "risk of injury" and contains a positive obligation to consult the person in charge of the protection of personal information within the enterprise (i.e. Privacy Officer) (Bill 64, s. 3.7).

Requirements to be set out in Regulations

Certain details such as the content of the notifications and record keeping requirements are to be set out in regulations, so it is not yet clear whether they will be more stringent than under the GDPR's Article 33.

Data Retention

Prescribed Minimum Retention Period:

Bill 64 requires data controllers to retain personal information at least one (1) year where the personal information is used to make a decision. (Bill 64, s. 11)

The GDPR does not provide any minimum (or other prescriptive) retention period for personal data and only requires personal data to be retained for "no longer than necessary." (Rec.39; Art.5(1)(e))

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Limitation on Retention Period:

Bill 64 permits the retention of personal information after the original purpose of the personal information processing is achieved only "where a preservation period is provided for by an Act". (Bill 64, s. 23)

The GDPR more flexibly permits data controllers to retain personal data for a broader set of purposes beyond the purposes for which such personal data was initially processed, specifically for purposes that are compatible with such purposes, as well as other specified purposes: see Rec.39; Art.5(1)(e))

Anonymization:

Where an organization anonymizes personal information after no longer being required, the organization must anonymize the data in accordance with "generally accepted best practices." (Bill 64, s. 23). Bill 64 defines "anonymize" in absolute and stringent fashion as "irreversibly no longer allows the person to be identified directly or indirectly" (Bill 64, s.23).

The GDPR does not prescribe any standards for anonymization, and the GDPR's definition of "anonymization" is similar but appears less stringent than Bill 64 as "anonymous" information for the purposes of the GDPR is information which "does not relate to an identified or identifiable natural person", or is rendered anonymous in such a manner than the data subject is no longer identifiable. (Rec. 26)

Transparency of Retention Period:

Bill 64 requires that on request, from a data processor or controller, an individual must be informed of the duration of the period of time their personal information will be kept. (Bill 64, s. 8)

The GDPR more flexibly requires that when personal data is collected from a data subject, the data controller shall provide the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. (Art.13(2)(a))

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Transparency

Notice of Policies

Bill 64 requires publication of a data controller's internal governance policies on its website, or if it doesn't have a website, by other appropriate means. (Bill 64, s. 3.2).

The public posting of a data controller's internal governance policies is not required by the GDPR.

Confidentiality Policy

Bill 64 requires any person (i.e. a data controller or processor) that collects information through technological means to publicize a confidentiality policy (and any amendments) on the website, as well as disseminate this policy so it reaches the appropriate person. (Bill 64, s. 8.2). The precise scope of the content of this policy and the circumstances when it would need to be posted is unclear, given the drafting of this provision, and that the term "confidentiality" is not defined under the Bill.

The scope of content in the GDPR for similar transparency requirements is articulated more clearly. (Art. 12-14)

Information About Means of Collection

Bill 64 requires that at the point of collection, an individual must be informed of the means of collection. (Bill 64, s. 8)

The GDPR does not expressly require this type of notice at the point of collection, whether or not the data has been obtained from the data subject: see Art. 13-14).

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Transparency and Access Requests

As part of the obligations for a data controller to respond to an access request, Bill 64 requires that on request, a person must be informed of (i) the means of collection of the individual's personal information and (ii) the categories of persons within the enterprise that have access to their personal information. (Bill 64, s. 8)

There is no requirement under the GDPR to provide the above type of information in response to an access request.

Transparency Requirements for Identification, Location and Profiling Technologies

Bill 64 sets out a broad requirement that where personal information is collected through technology that includes functions allowing the person concerned to be "identified, located or profiled", the data controller must first inform the person of the use of such technology, and the means to deactivate the functions that allow a person to be identified, located or profiled. (Bill 64, s. 8.1)

While under the GDPR the controller must be transparent about the existence of automated decision-making, including profiling, and provide meaningful information about the logic involved (see Art. 13, 2(f)), a very broad "deactivation right" seems similar to but potentially broader than the GDPR's right of objection (Art. 21).

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Automated Decision Making
Bill 64 requires data controllers who use personal information to render a decision "based exclusively on an automated processing of such information" inform the person concerned. As drafted, this notice requirement would be applicable in all circumstances involving decisions based on automated processing, regardless of materiality of the impact of the decision on the individual. The GDPR's automated decision-making provisions are less stringent, as there are broad transparency obligations on data controllers (unlike a notice requirement under Bill 64) (Art. 13(2)(f)), and the rights of individual to object to the decision apply only where the decision produces "legal effects or has similarly significant effects" on individuals. (Art. 22(1))
Data Accuracy
Bill 64 sets out an unqualified requirement for data controllers to ensure that personal information be up-to-date and accurate when used to make a decision (i.e. there is no limitation as to the time or circumstance when personal information needs to be up-dated) (Bill 64, ss. 11) Under the GDPR the retention requirement is qualified, as personal data must only be kept up to date "where necessary". (Rec.39; Art.5(1)(d))

This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Transborder Data Flow Requirements

Scope of obligations

Bill 64 contains highly restrictive and very onerous transborder data flow requirements, which apply to disclosures of personal information by a data controller to other data controllers and transfer to third party processors.

The cross-border transfer rules in Bill 64 apply to all disclosures and transfers of personal information outside Quebec (including transfers to other provinces and territories within Canada), (Bill 64, s. 17), unlike the GDPR which only restricts transfers to countries or territories outside the EEA. (Art. 45)

Requirement for Privacy Impact Assessment

Bill 64 provides that, prior to any transborder data disclosure or transfer, data controllers are required to undertake a privacy impact assessment and only transfer personal information outside Quebec if:

(i) the data controller determines that the personal information will receive equivalent protection in the other jurisdiction; and

(ii) a written agreement is in place that reflects the results of the privacy assessment and any identified risks.

Equivalence of Protection in other Jurisdictions

Bill 64 provides that the Minister may publish a list of jurisdictions with equivalent protection, although it is unclear as to whether a privacy impact assessment and/or a written agreement that reflects risks (as described above) would still be required for transfers of personal information to jurisdictions contained on this list. (Bill 64, s.17.1)

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Lack of Lawful Authority for Transborder Data Flows where no Equivalency

As drafted, data controllers would be prohibited under Section 17 of Bill 64 from transferring or disclosing personal information to a jurisdiction outside of Quebec that did not have equivalent protections as set out under Bill 64, even if the individual concerned expressly consented to the transfer, or the data controller had previously entered into a written agreement with obligations on the recipient to protect the personal information in a manner consistent with the provisions under Bill 64.

The transborder data flow restrictions under the GDPR are far more flexible, as the GDPR provides for various lawful bases other than adequacy for data controllers to transfer personal data outside the EU, including express consent, Model Clauses, contractual necessity, codes of conduct, and Binding Corporate Rules) (Art. 49)

Right of Access

Notice of Right:

Bill 64 provides that any person (i.e. a data controller or a processor) who collects personal information from a person must inform that person of the rights of access and rectification provided by law. (Bill 64, s. 8)

The GDPR right of access provisions apply only to data controllers, and requires that at the time when personal data is collected from a data subject, the controller provides the existence of the right to request access to, rectification of or erasure of personal data, or restriction of processing concerning the data subject. (Art. 13(2)(b))

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

Scope of right:

Under Bill 64 every person (i.e. a data controller or a processor) who holds personal information on another individual, must confirm the existence of the personal information and allow the individual to retain a copy of it. (Bill 64, s. 27)

The GDPR provides that a data controller (but not a process) shall provide confirmation as to whether the individuals' personal data has been processed, and access to the personal data and prescribed details. (Art. 15(1))

Under Bill 64, requests for access may be made by a person who provides that they are the person concerned, their representative, heir or successor and other specified persons: see Bill 64, s. 30. The GDPR has no equivalent requirement, and allows access to the individual only.

Form of Response:

Bill 64 provides that upon request, computerized personal information must be communicated in the form of a "written and intelligible transcript." (Bill 64, s. 27) If the person concerned is handicapped, "reasonable accommodation" must be provided upon request. (Bill 64, s. 27)

Under the GDPR, the information must be provided in a "commonly used electronic form" when responding to a request by electronic means. (Art. 15(3))

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Timing of Response

Bill 64 requires a response by PIC to requests for access 'promptly' and no later than 30 days (Bill 64, s. 32). There is no provision allowing this time period to be extended.

(The GDPR is 'without undue delay' and in any event within 1 month: see Art. 12(3)).

The GDPR allows, with respect to similar rights, for extension of 2 months where necessary, having regard to the complexity and number of requests (Art. 12(3)).

Person in Charge:

See the Person in Charge section for other obligations about subject matter rights requests and timing requirements.

Refusals:

Under Bill 64, any refusal to grant a request must be accompanied by reasons for refusal and an indication of the provision of law on which the refusal is based, the remedies available to the applicant, the time limits for exercising them, and on request help in understanding the refusal. (Bill 64, s. 34)

Under the GDPR, where a data controller intends to refuse to respond to a request, the data controller less prescriptively is obligated only to give reasons where they do not intend to comply with access requests. (Rec. 59)

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Deceased Persons:

Under Bill 64, an individual may be able to access the personal information concerning a deceased person, if they are the spouse or close relative of the person if knowledge of the information could help the applicant in the grieving process and if the deceased person did not record in writing his refusal to grant such a right of access. (s. 40.1)

Data relating to deceased persons generally falls outside the scope of the GDPR (except to the extent it also relates to a living person).

Right of Data Portability

Bill 64's provisions setting out the scope of the right of access generally apply to the right of data portability. The following differences between Bill 64 and the GDPR are notable as potentially providing a more expansive right of portability in the Quebec context compared to the GDPR (Art. 20):

- Bill 64's right of portability applies in all cases to provided computerized information, unless doing so raises serious practical difficulties (Bill 64, s. 27). The GDPR limits the portability right to the following circumstances:
    - the individual 'provided' (this is interpreted widely by supervisory authorities to include 'observed' data, but not so far as inferred or derived data) the personal data in the first place;
    - the data is automated (i.e. no paper records); and
    - the basis for processing of the data is consent or to fulfil a contract or steps preparatory to a contract.

This document is provided for general information purposes only and does not constitute legal or other professional advice.

- The GDPR provides a portability right to the individual only. Bill 64 permits a wider range of people to submit requests, including representatives, heirs, and successors (see Bill 64, s. 30).
- Bill 64 provides a portability right with respect to data relating to deceased individuals (Bill 64, s. 40.1). Data relating to deceased persons generally falls outside the scope of the GDPR (except to the extent it also relates to a living person).
- Unlike Bill 64, under the GDPR, there is an exception to the right of portability where a request is manifestly unfounded or excessive, particularly because of its repetitive character, the controller may refuse to act on the request or charge a reasonable fee (Art. 12(5)).

Right of Rectification

Scope of Right

Bill 64 permits a wide range of people to submit requests for rectification, including representatives, heirs and successors (Bill 64, s. 30). The GDPR provides a right of rectification to the individual only. (Art. 16)

Bill 64 provides rectification rights with respect to data relating to deceased individuals (Bill 64, s.30). Data relating to deceased persons generally falls outside the scope of the GDPR (except to the extent it also relates to a living person).

Bill 64 provides a rectification right with respect to equivocal data or where keeping or collecting it is not authorised by law, in addition to inaccurate or incomplete data (Bill 64, s.28). The GDPR's rectification right is limited to inaccurate or incomplete data. (Art. 16)

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Bill 64's right to have incomplete personal data completed is not limited having regard to the purpose of the processing, unlike the GDPR. As such, Bill 64 more broadly requires processors to take steps to rectify the personal information regardless of the purpose of the processing, whereas the GDPR requires that the purpose be taken into account. (Art. 16)

Burden of Proof:

Bill 64 requires the person holding the file, in case of disagreement, to prove that the file need not be rectified, unless the information was communicated to him by the person concerned or with their consent (Bill 64, s. 53)

The GDPR does not expressly address the burden of proof on the controller (though under the accountability principle a controller must be able to demonstrate compliance with the accuracy principle).

Person in Charge and Timing:

See the Right of Access section for obligations for requests and timing requirements.

Exceptions:

Bill 64 does not provide any exceptions to the right of rectification unlike the GDPR and Member State national laws.

Rejection:

Bill 64, unlike the GDPR, requires the person in charge to:

- indicate the provision of law on which refusal is based;
- inform the requestor of the time limit for exercising remedies; and
- on request, help the requestor understand the refusal. (Bill 64, s. 34)

This document is provided for general information purposes only and does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Rights of Restriction, Objection and Erasure (GDPR) vs. Right to Cessation of Dissemination, De-indexing, and Re-indexing (Quebec Bill)

Scope of right

There is a right in Bill 64 to require **cessation of dissemination or de-indexing** (Bill 64, s. 28.1), if the dissemination contravenes the law or a court order, where certain conditions are met. The GDPR does not contain such rights, but does contain **rights of restriction** (Art. 18) and **objection** (Art. 21) and a **right of erasure or "right to be forgotten"** (Art. 17), which may achieve the same outcomes.

Comparing the scope of the rights:

- The right to require cessation of dissemination or de-indexing in Bill 64 arises in different circumstances to the rights of restriction, objection and erasure in the GDPR. Under Bill 64, the person may require cessation of dissemination or de-indexing of hyperlinks where:
    - the dissemination of the information causes the person concerned serious injury in relation to his right to the respect of his reputation or privacy;
    - the injury is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing himself freely; and
    - the cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury. (Bill 64, s. 28.1)

This document is provided for general information purposes only and does not constitute legal or other professional advice.

- In contrast, under the GDPR:
    - the **person may require restriction** in certain circumstances involving contested accuracy, the exercise or defence or legal claims, or where the controller is verifying whether to stop processing, in which cases the data can be stored but not used: see details at Art. 18;
    - the **right to object** to processing can be exercised in circumstances involving direct marketing, processing for scientific, historical research or statistical purposes, or legitimate interest or public interest legal basis, subject to certain exceptions for public interest tasks or compelling legitimate grounds: see Art. 21;
    - the **right to erasure or to be forgotten** (Art. 17) can be exercised in any of a number of situations, including withdrawal of consent and there is no other lawful basis, or the data is no longer necessary for the purposes for which it was collected/processed.
- There is also a right in Bill 64 to require re-indexation in the same circumstances where a person may require cessation of dissemination or de-indexing of hyperlinks (Bill 64, s. 28.1). There is no such right in the GDPR.
- Bill 64 permits a wider range of people to submit requests for cessation of dissemination, indexing or re-indexing, including representatives, heirs or successors (Bill 64, s. 30). The GDPR provides a right of restriction, erasure and objection to the individual only. (Art. 17, Art. 18, Art. 21).

Person in charge (PIC)

See the Right of Access section for obligations for requests and timing requirements.

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Exceptions

Bill 64 does not provide any exceptions to the rights of cessation of dissemination, de-indexing, and re-indexing, unlike the GDPR and Member State national laws with respect to similar rights. Under the GDPR, the rights of objection and restriction and erasure contain exceptions where the request is manifestly unfounded or excessive, particularly because of its repetitive character. The rights of erasure contains further exceptions where processing is necessary for the rights of freedom of expression and information, public health reasons, the performance of a public interest task, and other enumerated reasons: see Art. 17.

Rejection of Request

For refusals to cease dissemination, de-index or re-index, Bill 64, unlike the GDPR, requires the person in charge to:

- indicate the provision of law on which refusal is based;
- inform the requestor of the time limit for exercising remedies; and
- on request, help the requestor understand the refusal. (see Bill 64, s. 34)

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and
does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Fines, Penalties and Statutory Right of Damages

Categories of Fines and Penalties

Under Bill 64, there are two types of monetary penalties:

1. **fines** of up to CAD $25 million, or if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year, on the commission of certain offences (Bill 64, s. 91); and

2. **administrative monetary penalties ("AMP")** of up to CAD $10 million, or if greater, the amount corresponding to 2% of the organization's worldwide turnover for the preceding fiscal year, for enumerated infringements (Bill 64, s. 90.12).

These mirror the two brackets of fines set out in the GDPR (at Art. 83), based on the seriousness of the infringement:

1. **More serious infringements** are subject to a maximum fine of €20m, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

2. **Less serious infringements** are subject to a maximum fine of €10m, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

Scope of Fines and Penalties

Despite the analogous categories, penalties are potentially more onerous under Bill 64 than the GDPR:

- **Potentially higher penalties for equivalent infringements:** For example, under the GDPR, failure to comply with the consent requirements when offering information society services directly to a minor is classified as a less serious infringement (Art. 83(4)). Under Bill 64, the use of personal information in contravention of any part of the Act (which would include failure to comply with the consent requirements for minors) is subject to a maximum fine of the greater of $25m or 4% of global turnover (Bill 64, s. 91). However, under Bill 64 'turnover' is based upon the legal entity in question and does not, unlike the GDPR, extend to the wider economic unit. This means a GDPR fine could still be higher in some cases.
- **Unique offence of "re-identification".** Under Bill 64, anyone commits an offence who identifies or attempts to identify a natural person using de-identified information, without the authorization of the person holding the information or using anonymized information, and is liable to fines (Bill 64, s. 91(3)). There is no specific equivalent offence under the GDPR.
- **Automatic doubled fine for subsequent offences:** Under Bill 64, in the case of a subsequent offence, the fines are automatically doubled (Bill 64, s. 92.1). Under the GDPR, relevant previous infringements are taken into account in setting the quantum of the fine, but there is no automatic increase. Where the fine is doubled due to a previous infringement, the maximum fine under Bill 64 is higher than that under the GDPR (8% vs. 4% of global turnover), although, as mentioned above, turnover is computed differently for the purposes of the GDPR.
- **No cumulative cap:** Under the GDPR, where the same or linked processing activity infringes several provisions, the fine will not exceed the specified amount for the gravest breach. While Bill 64 limits cumulative fines for infringement of the same provision, no cap is set out for multiple infringements of different provisions resulting from the same or linked processing activities.
- **Minimum fines:** Bill 64 provides for a minimum fine for offences under the Act of $5,000 for natural persons and $15,000 for organizations (Bill 64, s. 91). The GDPR does not set out any minimum fines.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and
does not constitute legal or other professional advice.

- **Personal liability:** The Quebec Act already sets out personal liability for the administrator, director or representative of the person who ordered or authorized the act or omission constituting the offence and exposes individuals to the prescribed penalties under the Act. Bill 64 did not change this provision (s. 93), but drastically increases the personal exposure. The GDPR does not set out personal liability in this way, though Member State national laws may potentially do so.

- **Criteria for Quantum of Penalties:** In setting an AMP or fine, Bill 64 may, in some cases, be potentially more stringent than the GDPR. In particular, the framework criteria guiding the decision to impose an AMP under Bill 64 (s. 90.2(2)) differs from the GDPR criteria at Art. 83 in the following respects, including:

    - the Commission may take into account "risk" of prejudice under Bill 64 framework, whereas, under the GDPR, only actual damage is to be taken into account;

    - Bill 64 framework does not take account of whether or not the PIC/controller has adhered to an approved code of conduct;

    - Bill 64 framework does not include a catch-all for other aggravating/mitigating factor;

    - Bill 64 framework takes into account the measures taken to remedy the "failure", whereas the GDPR focuses on measures taken to remedy the "damage".

- **Appeals to provincial Court of Quebec.** Appeals under Bill 64 are to the provincial Court of Quebec rather than the Superior Court (see s. 90.9, re: AMPs). Moreover, s. 90.9 provides that sections 61 to 69 of the current Act will govern the contestation of the monetary administrative penalty. This entails that appeals are only possible on questions of law or jurisdiction (s. 61) and that the decision of the judge of the Court of Québec is without appeal (s. 69). As such, the only avenue for further contestation would be through judicial review to the Superior Court, with a very limited scope of possible intervention by that Court and further appellate Courts. These limited recourses are concerning considering the potential scope of monetary administrative penalties that could be at issue, which amounts would far exceed the normal jurisdiction of the Court of Québec, which in civil matters is limited to claims under $85,000, and even then with full appeal rights to the Québec Court of Appeal.

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

Statutory damages basis of compensation:

Bill 64 provides a statutory right of damages compensating for injury (s. 93.1). Under the GDPR, the right to compensation is for "material or non-material damage" suffered. (Art. 82)

Controller only:

Bill 64 does not provide for liability for damages by processors, unlike the GDPR, which provides that a processor shall be liable for the damage caused by processing, but only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. (Art. 82)

Exemption from liability:

Bill 64 contains a different, arguably more limited test for exemption from liability ("superior force") than the GDPR ("not in any way responsible").

Minimum / punitive damages:

Bill 64 imposes a minimum quantum of punitive damages for intentional or gross fault ($1,000: see Bill 64, s. 93.1). The GDPR does not.

Joint responsibility:

Bill 64 does not address where there is more than one party responsible or provide for the possibility to recoup damages from processors or other controllers involved in the same processing. The GDPR addresses this joint responsibility at Art. 82.

This document is provided for general information purposes only and
does not constitute legal or other professional advice.

ACCESSPRIVACY BY OSLER

Summary Table of Key Elements of Quebec's Proposed Privacy Law Reform, Bill 64, and the General Data Protection Regulation (EU)

In June 2020, the Quebec government tabled Bill 64, An Act to modernize legislative provisions as regards the protection of personal information, which includes significant proposed amendments to an Act Respecting the Protection of Personal Information in the Private Sector (the "Quebec Privacy Act").

Many of the new requirements and individual rights proposed in Bill 64 are similar to those within the General Data Protection Regulation (EU) ("GDPR"). However, in many instances the requirements and other provisions under Bill 64 are more stringent, prescriptive or otherwise distinct from the requirements set out under the GDPR and are unique to the Province of Quebec.

If Bill 64 is enacted in its current form, companies who are subject to the Quebec Act that have established policies, procedures and practices to comply with the GDPR will need to take a series of additional steps to operationalize their compliance with Bill 64 (to the extent it is even practicable to even do so, given the stringent features of many provisions in the Bill). Moreover, Bill 64 exposes companies to significant financial penalties and damages that are even more severe than the potential penalties under the GDPR.

Given the significant compliance costs to comply with Bill 64's unique and stringent requirements and the severe financial risks under Bill 64's enforcement regime, it is reasonable to anticipate that Bill 64 (as currently drafted) will result in many products or services being withdrawn from the Quebec market and some Quebec-based businesses relocating certain of their operations outside the Province.

Commentators have identified multiple ways in which the GDPR has negatively impacted businesses, digital innovation, the labour market and consumers in the EU.[1] By introducing requirements and penalties that go beyond even the GDPR, it is reasonable to anticipate that the impacts in Quebec of Bill 64 will be greater than the impacts in the EU of the GDPR.

The table below summarizes the key differences between Bill 64 and the GDPR and identifies anticipated impacts of these distinctions. The summary comparison table has been prepared in tandem with the Comparison of Key Elements of Bill 64 and the GDPR Table, which provides a more detailed description of the manner in which Bill 64's provisions are more stringent, prescriptive or otherwise distinct from the GDPR.

[1] See for example: What the Evidence Shows About the Impact of the GDPR After One Year (https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/); Regulations like GDPR will make big tech stronger (https://qz.com/1332215/regulations-like-gdpr-will-make-big-tech-stronger/).

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Trans-border Data Flows	Bill 64 provides that, prior to any transborder data disclosure or transfer of data, controllers are required to undertake a privacy impact assessment and only transfer personal information outside Quebec if: (i) the data controller determines that the personal information will receive equivalent protection in the other jurisdiction, and (ii) a written agreement is in place that reflects the results of the privacy assessment and any identified risks. Enterprises may be prohibited from transferring or disclosing personal information to a jurisdiction outside of Quebec that does not have equivalent protections as set out under Bill 64, even if the individual concerned expressly consented to the transfer, or the data controller had previously entered into a written agreement with obligations on the recipient to protect the personal information in a manner consistent with the provisions under Bill 64.	The transborder data flow restrictions under the GDPR are far more flexible, as the GDPR provides for various lawful bases other than adequacy for data controllers to transfer personal data outside the EU, including express consent, Model Clauses, contractual necessity, codes of conduct, and Binding Corporate Rules (Art. 49).	Bill 64's highly restrictive and onerous trans-border data flow provisions may prevent enterprises in Quebec from using many commercially available products and services, including cloud infrastructure, e-commerce solutions, online payment platforms, and customer relationship and marketing tools. Quebec-based multinationals will need to give serious consideration to moving their Quebec-based back office operations used to store and process customer and employee information to another jurisdiction (so that they are able to transfer data within their global operations). Enterprises will incur material expenses and experience significant delays associated with assessing the equivalence of data protection laws in each jurisdiction (including other provinces in Canada) to which they may communicate personal information – something that, as a practical matter, is unworkable.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Confidentiality by Default	Bill 64 requires a data controller who collects personal information when offering a technological product or service to ensure that the parameters of the product or service provide the highest level of confidentiality by default, without any intervention by the person concerned (s. 9.1).	Bill 64's "confidentiality by default" clause is far broader in scope and significantly more stringent than the "privacy by design" concept under the GDPR (which requires the data controller to implement "appropriate technical and organizational measures" for implementing data protection principles in an effective manner, taking into account the nature, scope, context, risks and purposes of processing) (Art. 25(1)). The GDPR also requires data controllers to implement "appropriate" technical and organizational measures to ensure that by default, "only personal data which are necessary for each specific purpose of the processing are processed" (Art. 25(2)).	In many instances, organizations that have implemented "privacy by design" for their product and services in compliance with the GDPR standard will still not be compliant with Bill 64's very stringent "confidentiality by default" requirement. Given the small size of the Quebec market, it is unrealistic to expect that foreign-based technology businesses will create versions of their products and services that are customized to meet the requirements of Bill 64's "confidentiality by default" provision.
Data Impact Assessments	Bill 64 requires enterprises to conduct an assessment of the privacy-related factors of "any information system project or electronic service delivery project". Data controllers will be required to conduct assessments even in circumstances where there may be low or nominal risk associated with the personal information processing activity in question (s. 3.3).	The GDPR requires a data protection impact assessment only where the processing is likely to result in a 'high risk' to the rights and freedoms of natural persons (Art. 35(1)).	Enterprises that carry on business in Quebec will be required to dedicate sufficient resources to perform significantly more impact assessments than if they were not located in Quebec. Given the small size of the Quebec market, businesses located outside Quebec may decide to no longer offer their products or services in the Quebec market.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Consent and other Legal Authority for Processing	Primacy of Consent: Bill 64 enhances the primacy of consent as the default authority for processing personal information under the statute. Separate Consent: Bill 64 requires that consent be requested for each specific purpose, separately from any other information (s. 14). Express Consent: Bill 64 requires express consent for the processing of "sensitive personal information", which is defined as information that "entails a high level of reasonable expectation of privacy" (s. 12). Implied Consent: There is no express provision in Bill 64 for an implied, or assumed, consent for the lawful processing of non-sensitive personal information. Moreover, it is not clear how an implied form of consent can practically be operationalized given the requirement that consent be requested for each specific purpose, separately from other information (as required under s. 14).	Primacy of Consent: Consent is not a primary or default authority for processing personal information. The GDPR sets out other lawful and valid bases for processing of personal data (e.g. contractual necessity, compliance with legal obligations, vital interests, public interest, legitimate interests, or pursuant to a power of a Member state) (Art. 6). Separate Consent: The GDPR does not expressly require that consent be sought separately. Express Consent: The GDPR sets out prescribed categories of sensitive information. Implied Consent: Although the GDPR includes no reference to implied consent, consent is only one of many valid bases for processing of personal data. Expiration of Consent: The GDPR's consent provisions do not expressly address the expiration or other temporal aspects of consent.	Enterprises who are subject to the Quebec Privacy Act that have established policies, procedures and practices to comply with GDPR will need to take a series of additional steps to operationalize their compliance with Bill 64's consent requirements. This will result in businesses incurring material costs and limiting the use of personal information in ways that are permissible under the GDPR.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
	Expiration of Consent: Under Bill 64, consent is valid only for the time necessary to achieve the purpose for which it was requested (s. 14). Permissible Processing Without Consent: Bill 64 permits the use of personal information as a secondary purpose without the consent of the individual concerned if it is used for purposes "consistent" (a "direct and relevant connection") with the purposes for which it was collected (s. 17, s. 12). Other Exceptions to Consent: Bill 64 requires that personal information used without consent for research or the production of statistics be de-identified (s. 12(3)). Bill 64 does not allow for further processing for archiving purposes in the public interest. Bill 64 sets out that further processing of data for commercial or philanthropic prospection is not permissible (s. 12).	Permissible Processing Without Consent: The GDPR more permissively allows personal data to be further processed for secondary purposes that are not "incompatible" with the initial purposes for its collection (Rec.50; Art.5(1)(b)). A contextual assessment is required to determine the extent of compatibility in the circumstances (Art .6(4)). The GDPR expressly permits the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Art.5(1)(b)). Other Exceptions to Consent: The GDPR does not require "pseudonymization" in all cases in which personal information is used for research and the production of statistics (Art 6(4)(e)). The GDPR does not set out that further processing of data for commercial or philanthropic prospection is not permissible (s.12).	

This document is provided for general information purposes only and does not constitute legal or other professional advice.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Automated Decisions	Bill 64 regulates any decision based exclusively on an automated processing of personal information, with no exceptions (s. 12.1).	Under the GDPR, rules applicable to automated decisions apply only if a decision affects a person's legal status or legal rights or has an equivalent impact on the person's circumstances, behaviour or choices. Additionally, the GDPR provides a number of exemptions, including where an automated decision is necessary for entering into, or performance of, a contract between the data subject and a data controller (Art.22).	Quebec-based businesses will deploy fewer automated (e.g. AI) decision-making processes (due to the necessity of meeting notice, transparency and "decision-review" requirements found in Bill 64, even when a decision has no material impact on the legal status or legal rights of an individual). Quebec may become a less desirable jurisdiction in which to create, scale, operate or invest in businesses that sell or use AI solutions. AI-related research and development activities will be more likely to be performed outside Quebec. There will be fewer new AI-based businesses established in Quebec. There will be an increased likelihood of existing AI-based businesses in Quebec relocating to another jurisdiction.
Deactivation of Identification, Location or Profiling Functions	An enterprise deploying technology that includes functions allowing an individual to be identified, located or profiled must first inform the individual of the use of such technology and the means to deactivate the functions (s. 8.1).	Although a data controller must be transparent about the existence of automated decision-making, including profiling, and provide meaningful information about the logic involved (Art. 13, 2(f)), Bill 64's "deactivation right" appears broader than GDPR's right of objection (Art. 21).	Quebec-based enterprises will be required to incur costs and dedicate resources to implement and manage a deactivation right that is broader than under the GDPR. Technology businesses based outside Quebec will be required to create versions of their products and services that are customized for Quebec to meet these specific requirements.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Take-down, De-indexing and Re-indexing	Bill 64 provides individuals with the right to require cessation of dissemination or de-indexing (s.28.1) if the dissemination contravenes the law or a court order, where certain conditions are met. Bill 64 provides individuals with the right to require re-indexation in the same circumstances where a person may require cessation of dissemination or de-indexing of hyperlinks (Bill 64, s. 28.1). Bill 64 does not provide any exceptions to the rights of cessation of dissemination, de-indexing, and re-indexing.	The GDPR provides individuals with rights of restriction (Art. 18) and objection (Art. 21) and a right of erasure or "right to be forgotten" (Art. 17). The GDPR does not include a right of re-indexation. Under the GDPR, the rights of objection and restriction and erasure are subject to exceptions where the request is manifestly unfounded or excessive, particularly because of its repetitive character. The right of erasure contains further exceptions where processing is necessary for the rights of freedom of expression and information, public health reasons, the performance of a public interest task, and other enumerated reasons (Art. 17).	Enterprises who are subject to the Quebec Privacy Act that have established policies, procedures and practices to comply with GDPR will need to take a series of additional steps and incur material costs to operationalize their compliance with the more stringent take-down, de-indexing and re-indexing provisions under Bill 64.
Data Retention	Prescribed Minimum Retention Period: Bill 64 requires data controllers to retain personal information at least one (1) year where the personal information is used to make a decision (s. 11). Limitation on Retention Period: Bill 64 permits the retention of personal information after the original purpose of the personal information processing is achieved only "where a preservation period is provided for by an Act" (s. 23).	Prescribed Minimum Retention Period: The GDPR does not provide any minimum (or other prescriptive) retention period for personal data and only requires personal data to be retained for "no longer than necessary" (Rec.39; Art.5(1)(e)).	Enterprises that are subject to the Quebec Privacy Act, and that have already established policies, procedures and practices to comply with the GDPR, will need to take a series of additional steps and incur material costs to operationalize their compliance with Bill 64's more stringent data retention requirements.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
	Anonymization: Where an organization anonymizes personal information after the information is no longer required, the organization must anonymize the data in accordance with "generally accepted best practices" (s. 23). Bill 64 defines "anonymize" in an absolute and stringent fashion as "irreversibly no longer allows the person to be identified directly or indirectly" (s. 23). Transparency of Retention Period: Bill 64 requires that on request an individual must be informed of the duration of the period of time their personal information will be kept (s. 8).	Limitation on Retention Period: The GDPR more flexibly permits data controllers to retain personal data for a broader set of purposes beyond the purposes for which such personal data was initially processed, specifically for purposes that are compatible with such purposes, as well as other specified purposes (see Rec.39; Art.5(1)(e)). Anonymization: The GDPR does not prescribe any standards for anonymization, and the GDPR's definition of "anonymization" appears less stringent than Bill 64 as "anonymous" information for the purposes of the GDPR is information which does not relate to an identified or identifiable natural person, or is rendered anonymous in such a manner that the data subject is no longer identifiable (Rec. 26). Transparency of Retention Period: The GDPR more flexibly requires that when personal data is collected from a data subject, the data controller shall provide the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Art.13(2)(a)).	

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Accountability	An enterprise's CEO or president is required to approve governance policies and practices regarding personal information (s. 3.2) and be directly involved in response to requests for access, rectification and ceasing dissemination or de-indexing (s. 35).	There are no corresponding express obligations on an enterprise's CEO or president.	This accountability provision may significantly raise the personal risk for the CEO or president of an enterprise, as the Quebec Act currently provides that an individual who orders or authorizes an act or omission that constitutes an offense of the data controller under the statute, is deemed to be a party to the offence and is personally liable to prescribed penalties under the Act.
Security Breach Notification	Bill 64 contains a mandatory breach notification obligation to the Commissioner and individuals of "confidentiality incidents" that present a "risk of serious injury" (s. 3.5). Bill 64 defines a "confidentiality incident" to include the communication of personal information "not authorized by law" and (more broadly) "any other breach in the protection of such information."	The notification trigger under the GDPR may set a higher threshold for notification, both in terms of (i) the level of harm to individuals ("high risk" to individuals' rights and freedoms is the test under the GDPR, rather than "risk of serious injury" in Bill 64); and (ii) the definition of a "personal data breach" (which is the comparable term in the GDPR to the broader definition of "confidentiality incidents" in Bill 64) (Art.33).	Enterprises that are subject to the Quebec Privacy Act, and that have already established policies, procedures and practices to comply with the GDPR (or other privacy laws, including PIPEDA) will need to take a series of additional steps and incur material costs to operationalize their compliance with Bill 64's security breach notification requirements.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Standard for Information Security	Bill 64 contains an absolute requirement for organizations to "protect personal information held by a person", which requires data controllers to establish and implement governance policies and practices that "ensure" the protection of such information (i.e. there is no qualifying concept of reasonable or appropriate security measures) (s. 3.2). These provisions, however, are inconsistent with the qualified requirements set out in section 10, "reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored." (s. 10)	The GDPR's standard for safeguarding is less stringent, as it requires "appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (Art.5(1)).	A higher standard for information security in Quebec (combined with the other penalties included in Bill 64) will create incentives for enterprises to limit the personal information that is stored or processed in Quebec. It will also create an incentive for enterprises to move their operations to other jurisdictions.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.

Summary Comparison of Bill 64 and the GDPR

Issue	Bill 64	GDPR	Examples of Anticipated Impacts
Penalties	Bill 64 effectively creates no-fault liability under which an enterprise is automatically liable (subject to establishing force majeure) for an injury resulting from the unlawful infringement of rights created by the Quebec Privacy Act or the rights of reputation and privacy set out in the Civil Code of Quebec (s. 93.1). When combined with the Standard for Information Security (s. 3.2), Bill 64 potentially creates a strict liability regime for data breaches. Bill 64 imposes a minimum quantum of punitive damages for intentional or gross fault – $1,000 (s. 93.1). Bill 64's maximum fine may be 8% of worldwide turnover, which is twice the maximum in the EU, notwithstanding that Quebec's population is 2% of the population of EU member countries (s. 92.1). Bill 64 does not cap fines for multiple infringements of different provisions resulting from the same or linked processing activities.	The GDPR does not create strict liability for data breaches. The GDPR does not impose a minimum quantum of punitive damages. The GDPR does not double fines for subsequent offences (e.g., doubling fines from 4% of worldwide turnover to 8% of worldwide turnover). The GDPR caps fines for multiple infringements of different provisions resulting from the same or linked processing activities.	The penalty provisions under Bill 64 is likely to result in significantly more privacy-related litigation in Quebec, including class actions. Quebec-based businesses will need to evaluate whether the increased risk of litigation, and the creation of financial penalties that lack proportionality to the size of the Quebec market, warrant giving serious consideration to relocating the businesses' operation to another jurisdiction.

Osler, Hoskin & Harcourt LLP
This document is provided for general information purposes only and does not constitute legal or other professional advice.