Adoption finale du projet de loi n° 64 – Principales exigences pour les entreprises

Le 21 septembre 2021, l'Assemblée nationale du Québec a adopté le projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* qui introduit des modifications importantes à la législation en matière de protection des renseignements personnels dans le secteur privé et public.

Cet article porte sur les modifications apportées à la *Loi sur la protection des renseignements personnels dans le secteur privé* (*Loi sur le secteur privé*) et résume les principaux impacts du projet de loi n° 64 pour les entreprises. Dans la Partie 1, nous présentons les plus importantes exigences introduites à la *Loi sur le secteur privé* dans l'ordre qui correspond à leur date d'entrée en vigueur. Il convient de noter que le délai d'entrée en vigueur des nouvelles dispositions commence à compter du 22 septembre 2021, soit la date de la sanction de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. Dans la Partie 2, nous proposons un résumé des nouvelles sanctions qui visent à assurer le respect de la Loi.

Nous vous invitons à consulter notre version amendée de la *Loi sur le secteur privé* pour connaître le texte précis de ces amendements.

1 Nouvelles exigences introduites à la Loi sur le secteur privé

Les exigences suivantes entreront en vigueur dans un an

Exigence	Description
Désignation d'un responsable de la protection des renseignements personnels (art. 3.1)	• Par défaut, le PDG de chaque organisation exerce la fonction de « responsable de la protection des renseignements personnels ». • Le responsable de la protection des renseignements personnels veille à assurer le respect et la mise en œuvre de la *Loi sur le secteur privé*. • La fonction de responsable de la protection des renseignements personnels peut être déléguée par écrit à toute personne. • Les coordonnées du responsable de la protection des renseignements personnels doivent être publiées sur le site Web de l'organisation.
Signalement des incidents de confidentialité (art. 3.5 à 3.8)	• Les organisations doivent aviser la Commission d'accès à l'information (CAI) et les personnes concernées de tout incident de confidentialité qui présente un risque de préjudice sérieux. • Le « risque de préjudice sérieux » est évalué à l'aide de facteurs similaires à ceux prévus par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), à savoir la sensibilité des renseignements concernés, es conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables. • Les organisations doivent tenir un registre des incidents de confidentialité qui doit être communiqué à la CAI sur demande.

Les exigences suivantes entreront en vigueur dans **deux ans**

Exigence	Description
Politiques et pratiques (art. 3.2)	• Les organisations doivent établir et mettre en œuvre des politiques et des pratiques encadrant leur gouvernance à l'égard des renseignements personnels. • Ces politiques et pratiques doivent : – Prévoir des règles applicables à la conservation et à la destruction des renseignements personnels; – Prévoir les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels; et – Prévoir un processus de traitement des plaintes relatives à la protection des renseignements personnels. • Les organisations doivent publier de l'information détaillée au sujet de ces politiques et de ces pratiques sur leur site Web.
Évaluation des facteurs relatifs à la vie privée (EFVP) (art. 3.3 et 3.4)	• Les organisations doivent procéder à une évaluation des facteurs relatifs à la vie privée (EFVP) de tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. • Une EFVP doit être « proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support ».
Traitement automatisé de renseignements personnels (art. 12.1)	• Les organisations doivent informer la personne concernée lorsqu'elle fait l'objet d'une décision fondée exclusivement sur un traitement automatisé de ses renseignements personnels. • Les organisations doivent également, à la demande de la personne concernée, l'informer de : – les renseignements personnels utilisés pour rendre la décision; – les raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision; et – son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision. • Les organisations doivent également donner à la personne concernée l'occasion de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision.
Transferts à l'extérieur du Québec (art. 17)	• Les organisations doivent effectuer une EFVP avant de communiquer des renseignements personnels à l'extérieur du Québec afin de déterminer si les renseignements bénéficieront d'une protection « adéquate » au regard notamment des « principes de protection des renseignements personnels généralement reconnus ». • Cette EFVP doit notamment tenir compte de : – la sensibilité des renseignements; – la finalité de leur utilisation; – les mesures de protection, y compris celles qui sont contractuelles, dont les renseignements bénéficieraient; et – le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables. • La communication devra faire l'objet d'une entente écrite qui tient compte des résultats de l'EFVP et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés par l'EFVP.

Les exigences suivantes entreront en vigueur dans **deux ans**

Exigence	Description
Impartition (art. 18.3)	• Les organisations qui transfèrent des renseignements personnels à un fournisseur de services doivent conclure une entente écrite avec ce dernier qui doit prévoir : – Une description des mesures prises par le fournisseur de services pour assurer la protection du caractère confidentiel des renseignements personnels communiqués (ex. une description des mesures de sécurité); – Une obligation pour le fournisseur de services de n'utiliser les renseignements qu'aux fins de la prestation des services et de ne pas conserver ces renseignements après l'expiration du contrat; et – Une obligation pour le fournisseur de services d'informer sans délai le responsable de la protection des renseignements personnels de toute violation ou tentative de violation d'une obligation relative à la confidentialité des renseignements et de permettre au responsable de la protection des renseignements personnels d'effectuer toute vérification relative aux exigences de confidentialité.
Transparence (art. 8 et 8.2)	• Les organisations doivent fournir les renseignements suivants aux personnes concernées au moment de recueillir leurs renseignements personnels : – les fins de la collecte; – les moyens de la collecte; – les droits d'accès et de rectification; et – le droit des personnes concernées de retirer leur consentement. • Lorsqu'applicable, les renseignements suivants doivent également être fournis : – le nom du tiers pour qui la collecte est faite; – les catégories de tiers à qui il est nécessaire de communiquer les renseignements pour accomplir les fins de la collecte (ex. fournisseurs de services); et – la possibilité que les renseignements soient communiqués à l'extérieur du Québec. • Les organisations doivent publier une politique de confidentialité sur leur site Web si elles recueillent des renseignements personnels par un moyen technologique. • La politique de confidentialité doit être rédigée en termes simples et clairs.
Transparence – Technologies de profilage, de localisation et d'identification (art. 8.1)	• Les organisations doivent informer les personnes concernées lorsqu'elles recueillent des renseignements personnels en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage. • Les organisations doivent également informer les personnes concernées des moyens offerts pour activer ces fonctions. • Le « profilage » s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.

Les exigences suivantes entreront en vigueur dans **deux ans**

Exigence	Description
Consentement (art. 8.3, 12 et 14)	• Toute personne qui fournit ses renseignements personnels après avoir été informée par une politique de confidentialité adéquate consent à leur utilisation et à leur communication aux fins indiquées dans cette politique. • Le consentement doit être manifeste, libre et éclairé et être donné à des fins spécifiques. Il doit être demandé pour chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. • Les organisations doivent obtenir un consentement formulé de manière expresse dès qu'une utilisation secondaire de renseignements personnels concerne un renseignement personnel sensible. • Un renseignement personnel est considéré sensible lorsque de par sa nature notamment médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée. • Le consentement d'un mineur de moins de 14 ans doit être donné par le titulaire de l'autorité parentale ou par son tuteur. • Les organisations bénéficieront des nouvelles exceptions au consentement.
Protection de la vie privée par défaut (art. 9.1)	• Les organisations qui recueillent des renseignements personnels en offrant au public un produit ou un service technologique qui dispose paramètres de confidentialité doivent s'assurer que ces paramètres assurent le plus haut niveau de confidentialité par défaut. • Cette exigence ne s'applique pas aux témoins de connexion (cookies).
Conservation et destruction (art. 23)	• Les organisations doivent détruire les renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis ou utilisés sont accomplies. • Les organisations peuvent également anonymiser les renseignements personnels, selon les meilleures pratiques généralement reconnues, pour les utiliser à des fins sérieuses et légitimes.
Droit à la désindexation (art. 28.1)	• Les personnes concernées peuvent demander aux organisations de cesser de diffuser leurs renseignements personnels et de désindexer tout hyperlien rattaché à leur nom qui donne accès à ces renseignements si cette diffusion contrevient à la loi ou à une ordonnance judiciaire.

L'exigence suivante entrera en vigueur dans **trois ans**

Exigence	Description
Droit à la portabilité (art. 27)	• Une personne peut demander que les renseignements personnels recueillis à son sujet lui soient communiqués (ou à une autre organisation qu'elle désigne) dans un format technologique structuré et couramment utilisé. • Ceci exclut les renseignements créés ou inférés par l'organisation à partir de l'analyse des renseignements personnels de la personne concernée. • L'organisation n'est pas tenue de détruire les renseignements personnels qu'elle détient après avoir traité une demande de portabilité.

2 Nouvelles sanctions introduites à la Loi sur le secteur privé

La *Loi sur le secteur privé* comptera désormais trois mécanismes visant à assurer la conformité des organisations.

1. Des sanctions administratives pécuniaires (SAP) imposées directement par la Commission d'accès à l'information (CAI).
2. De nouvelles infractions pénales associées d'amendes salées.
3. Un droit privé d'action permettant aux individus de poursuivre une organisation en dommages-intérêts.

Le tableau suivant présente un résumé des principales infractions susceptibles d'être sanctionnées dans le cadre de ce nouveau régime d'application de la loi qui entrera en vigueur dans deux ans.

Violation		Infraction pénale	SAP	Droit privé d'action
Collecte, utilisation, communication ou destruction de renseignements personnels en contravention à la loi	→	X	X	X
Conservation de renseignements personnels en contravention à la loi	→		X	X
Défaut de fournir aux personnes concernées les informations requises pour procéder à la collecte des renseignements personnels	→		X	X
Défaut d'aviser la CAI ou les personnes concernées d'un incident de confidentialité qui présente un risque de préjudice sérieux	→	X	X	X
Défaut d'informer la personne visée par une décision automatisée ou ne pas lui donner l'occasion de présenter ses observations	→		X	X
Refuser ou négliger de se conformer, dans le délai fixé, à une demande de production de documents émise par la CAI	→	X		
Contrevenir à une ordonnance de la CAI	→	X		
Sanction (Montant maximal)		**25 M$ ou 4 % du chiffre d'affaires mondial**	**10 M$ ou 2 % du chiffre d'affaires mondial**	**Montant des dommages octroyés**

Prochaines étapes

BLG publiera bientôt un guide complet pour aider les entreprises à se conformer aux nouvelles exigences en matière de protection des renseignements personnels introduites à la *Loi sur le secteur privé*.

Pour toute question sur les récents développements concernant le cadre juridique régissant la protection des renseignements personnels au Québec, veuillez communiquer avec l'un des principaux contacts ci-dessous ou avec un membre de l'équipe Respect de la vie privée et protection des renseignements personnels de BLG.

Éloïse Gratton
Associée
T 514.954.3106
egratton@blg.com

Elisa Henry
Associée
T 514.954.3113
ehenry@blg.com

François Joli-Coeur
Avocat principal
T 514.954.3144
fjolicoeur@blg.com

Simon Du Perron
Avocat
T 514.954.2542
sduperron@blg.com

Max Jarvie
Avocat principal
T 514.954.2628
mjarvie@blg.com

Julie Gauthier
Avocate-conseil
T 514.954.2555
jugauthier@blg.com

Andy Nagy
Avocat
T 514.395.2714
anagy@blg.com

Borden Ladner Gervais