

Entrée en vigueur du nouveau règlement sur l'anonymisation des renseignements personnels : Que faut-il retenir?

30 mai 2024

Le 15 mai 2024, le gouvernement du Québec a édicté un nouveau [Règlement sur l'anonymisation des renseignements personnels](#) (le « Règlement »). Ce règlement vient préciser les critères et les modalités du processus d'anonymisation des renseignements personnels au Québec. Il s'agit du premier texte réglementaire à venir encadrer l'anonymisation de renseignements personnels au Canada.

Contexte

Depuis l'entrée en vigueur de la Loi 25, tant la Loi sur la protection des renseignements personnels dans le secteur privé (« LPRPSP ») que la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (« Loi sur l'accès ») autorisent les organisations à anonymiser des renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis ou utilisés sont accomplies.

En vertu de cette disposition, les organisations doivent anonymiser les renseignements suivant les « meilleures pratiques généralement reconnues » et « selon les critères et modalités déterminés par règlement ». Un renseignement est considéré anonymisé lorsqu'il est « en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement » une personne.

Jusqu'à la publication récente du Règlement, des incertitudes persistaient quant aux « critères et modalités » devant être observés par les organisations lorsqu'elles souhaitent anonymiser des renseignements personnels. Particulièrement, la [Commission d'accès à l'information \(CAI\) avait indiqué sur son site Web](#) que les organisations ne pouvaient anonymiser des renseignements personnels en l'absence de règlement du gouvernement. La publication du Règlement met donc fin à plusieurs incertitudes¹.

Qui doit respecter le Règlement?

Tant les entreprises assujetties à la LPRPSP que les organismes publics assujettis à la Loi sur l'accès doivent respecter le Règlement. Les ordres professionnels sont également tenus de le respecter dans la mesure prévue par le Code des professions. Le Règlement emploie le terme « organisation » pour désigner l'ensemble des entités devant s'y conformer.

Quelle est sa date d'entrée en vigueur?

Le Règlement entre en vigueur le 30 mai 2024, à l'exception de l'article 9, portant sur l'obligation de consigner certaines informations dans un registre, qui entrera en vigueur le 1^{er} janvier 2025.

Contenu du Règlement

Voici un résumé des nouvelles exigences introduites par le Règlement afin d'encadrer le processus d'anonymisation. Les passages en italique désignent les nouveautés introduites depuis le projet de Règlement soumis en décembre 2023.

Période cible	Exigence	Description de l'exigence
Avant un processus d'anonymisation	Détermination des fins d'utilisation des renseignements anonymisés (art. 3)	Avant d'amorcer un processus d'anonymisation, l'organisation doit définir les fins pour lesquelles elle entend utiliser les renseignements anonymisés. Une entreprise doit s'assurer que ces fins soient « sérieuses et légitimes » alors qu'un organisme public doit veiller à ce que les renseignements anonymisés soient utilisés à des « fins d'intérêt public ». Le Règlement n'apporte pas de clarification sur la portée de ces notions.
Processus d'anonymisation		
En tout temps lors du processus d'anonymisation	Supervision du processus par une personne compétente en la matière (art. 4)	L'organisation doit s'assurer que l'anonymisation est réalisée sous la supervision d'une personne compétente. Pour se conformer à cette disposition, une organisation devrait sélectionner un professionnel qualifié en anonymisation et en protection des renseignements personnels

		<p>pour superviser le processus. Lorsque le personnel d'une organisation ne possède pas l'expertise requise pour superviser un tel processus, elle devrait faire appel aux services d'un fournisseur externe qui est qualifié en la matière.</p>
<p>Au début du processus d'anonymisation</p>	<p>Retrait des renseignements personnels qui permettent d'identifier directement les personnes concernées (art. 5)</p>	<p>L'organisation doit retirer tous les renseignements personnels qui permettent d'identifier directement la personne concernée (ex. : nom, numéro d'assurance sociale, identifiant unique) des renseignements qu'elle entend anonymiser.</p> <p>Les renseignements qui ne permettent plus d'identifier directement une personne sont considérés comme des renseignements dépersonnalisés au sens de LPRPSP et de la Loi sur l'accès.</p>
	<p>Analyse préliminaire des risques de réidentification (art. 5 al 2)</p>	<p>L'organisation doit par la suite effectuer une analyse préliminaire des risques de réidentification en considérant notamment :</p> <ol style="list-style-type: none"> 1. Le critère d'individualisation, soit le fait de ne pas être en mesure d'isoler ou de distinguer une personne dans un ensemble de données; 2. Le critère de corrélation, c.-à-d. le fait de ne pas être en mesure de relier entre eux des ensembles de données qui concernent une même personne; 3. Le critère d'inférence, soit le fait de ne pas être en mesure de déduire des renseignements personnels à partir

		<p>d'autres renseignements disponibles;</p> <p>4. Les risques que d'autres renseignements <i>raisonnablement</i> disponibles, notamment dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne.</p> <p><i>Le terme « raisonnablement » a été ajouté à l'article 5 depuis la publication du Projet de règlement.</i></p> <p>Les critères d'individualisation, de corrélation et d'inférences se rapprochent des critères employés par les autorités européennes de protection des données, notamment la CNIL en France. Les ressources publiées par ces autorités peuvent fournir des pistes d'interprétation en l'absence d'une publication formelle par la CAI.</p>
	<p>Établir les techniques d'anonymisation à utiliser (art. 6)</p>	<p>En fonction des risques de réidentification identifiés, l'organisation doit établir les techniques d'anonymisation à utiliser, lesquelles doivent être conformes aux meilleures pratiques généralement reconnues.</p> <p>Techniques d'anonymisation : Les autorités européennes de protection des données distinguent deux grandes familles de techniques d'anonymisation, soit la randomisation et la généralisation. Le Règlement invite donc les organisations à identifier les techniques appropriées issues de ces deux</p>

		<p>approches afin de protéger son ensemble de données face aux risques d'individualisation, de corrélation et d'inférence.</p> <p>Meilleures pratiques généralement reconnues : À l'heure actuelle, la notion de « meilleures pratiques généralement reconnues » n'est pas clairement définie. Ainsi, par précaution, les organisations peuvent se référer aux pratiques qui sont internationalement reconnues pour anonymiser les renseignements personnels. Par exemple, la norme ISO/IEC 27559:2022.</p>
	<p>Établir des mesures de protection et de sécurité raisonnables pour diminuer les risques de réidentification (art. 6)</p>	<p>L'organisation doit aussi établir des mesures de protection et de sécurité <i>raisonnables</i> pour diminuer les risques de réidentification.</p> <p><i>Le terme « raisonnables » a été ajouté à l'article 5 depuis la publication du Projet de règlement.</i></p> <p>À noter que cette disposition fait écho à l'obligation prévue dans la LPRPSP et la Loi sur l'accès à l'accès pour les organisations qui utilisent des renseignements dépersonnalisés de prendre des mesures raisonnables pour limiter les risques que quiconque procède à l'identification d'une personne physique à partir de ces renseignements.</p>
Mise en œuvre des techniques d'anonymisation et des mesures de sécurité		
<p>Après la mise en œuvre des techniques d'anonymisation</p>	<p>Analyse des risques de réidentification (art. 7)</p>	<p>Après avoir mis en œuvre les techniques d'anonymisation et les mesures de sécurité, l'organisation doit effectuer une analyse des risques de</p>

		<p>réidentification de son ensemble de données.</p> <p>Éléments à considérer : L'organisation doit considérer les éléments suivants lors de l'analyse :</p> <ul style="list-style-type: none"> • Les circonstances liées à l'anonymisation des renseignements personnels, incluant les fins pour lesquelles l'organisation entend utiliser les renseignements anonymisés • La nature des renseignements • Le critère d'individualisation, le critère de corrélation et le critère d'inférence • Les risques que d'autres renseignements <i>raisonnablement</i> disponibles, notamment dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne <p style="text-align: center;"><i>Le terme raisonnablement a également été ajouté à ce paragraphe, tout comme à l'article 5.</i></p> <ul style="list-style-type: none"> • Les moyens nécessaires pour réidentifier les personnes, notamment en considérant les efforts, les ressources et le savoir-faire requis pour mettre en œuvre ces moyens. <p>Résultats de l'analyse :</p> <p>Les résultats de l'analyse doivent démontrer qu'il est « en</p>
--	--	---

		<p>tout temps, raisonnable de prévoir dans les circonstances que les renseignements produits à la suite d'un processus d'anonymisation ne permettent plus, de façon irréversible, d'identifier directement ou indirectement une personne. » Le Règlement précise que ce critère n'exige pas la démonstration d'un risque nul. Cependant, les résultats de l'analyse doivent démontrer, en tenant compte notamment des éléments ci-dessus, que <i>les risques résiduels</i> de réidentification sont très faibles.</p> <p><i>La notion de risque résiduel a été mise au pluriel depuis la publication du Projet de règlement</i></p> <p>Toujours dans l'attente d'une publication de la CAI sur l'anonymisation, nous sommes d'avis que les organisations peuvent s'inspirer de la méthode décrite par le Commissaire à l'information et à la protection de la vie privée de l'Ontario pour évaluer de façon quantitative les risques de réidentification.</p>
<p>À la fin du processus d'anonymisation et après</p>	<p>Évaluation périodique des renseignements anonymisés (art. 8)</p>	<p>L'organisation doit <i>périodiquement</i> évaluer les renseignements qu'elle a anonymisés afin de s'assurer qu'ils le demeurent.</p> <p><i>Le terme « périodiquement » remplace celui de « régulièrement » qui était prévu dans le Projet de règlement. Le troisième alinéa qui a été rajouté à l'article 8 fournit des précisions utiles sur la périodicité des évaluations qui est</i></p>

		<p><i>exigée.</i></p> <p>L'organisation doit mettre à jour <i>la dernière analyse</i> des risques de réidentification qu'elle a effectués. Cette mise à jour doit considérer les avancées technologiques qui peuvent contribuer à réidentifier une personne.</p> <p>Les résultats de la <i>mise à jour de cette analyse</i> doivent démontrer que les renseignements demeurent anonymisés conformément au critère prévu au deuxième alinéa de l'article 7 du Règlement. Dans la négative, les renseignements ne sont alors plus considérés comme anonymisés.</p> <p>La périodicité à laquelle une organisation doit évaluer les renseignements qu'elle a anonymisés est déterminée en fonction des risques résiduels identifiés lors de la dernière analyse des risques de réidentification effectuée.</p> <p><i>Ce dernier paragraphe a été ajouté dans la version finale du Règlement.</i></p>
	<p>Tenue d'un registre portant sur l'anonymisation (art. 9)</p> <p><i>Cette exigence devra être respect</i></p>	<p>Enfin, l'organisation qui anonymise des renseignements personnels doit consigner les informations suivantes dans un registre:</p> <ol style="list-style-type: none"> 1. Une description des renseignements personnels qui <i>ont été anonymisés</i>; 2. Les fins pour lesquelles elle entend utiliser ces renseignements anonymisés.

		<p>3. Les techniques d'anonymisation utilisées et les mesures de protection et de sécurité établies.</p> <p>4. La date à laquelle l'analyse des risques de réidentification a été complétée ainsi que toute date à laquelle sa mise à jour a été effectuée.</p> <p>En pratique, l'organisation devrait désigner une personne responsable pour assurer la tenue du registre. Le registre devrait être conservé aussi longtemps que requis pour démontrer la conformité de l'organisation.</p>
--	--	--

Pistes de conformité

Le principal constat qui émerge d'une lecture attentive du Règlement est que l'anonymisation des renseignements personnels au Québec est un processus rigoureux qui requiert que les organisations y consacrent le temps et les ressources nécessaires. En ce sens, nous sommes d'avis que les organisations souhaitant anonymiser des renseignements personnels peuvent mettre en branle les étapes suivantes dès maintenant :

- Impliquer vos équipes responsables des TI, de la gestion documentaire, de la conformité et le département juridique dans le projet d'anonymisation;
- Évaluer si votre organisation bénéficierait d'une expertise externe en matière d'anonymisation;
- Cartographier vos répertoires existants de données anonymisées afin d'évaluer s'ils respectent le Règlement;
- Formaliser votre processus d'anonymisation dans un document normatif interne, adapté à la réalité opérationnelle de vos équipes.

Communiquez avec nous

Le groupe [Cybersécurité, respect de la vie privée et protection des renseignements personnels](#) de BLG suit de près les développements susceptibles d'éclairer les organisations sur les exigences des lois de protection des données au Canada. N'hésitez pas à communiquer avec notre équipe si votre organisation souhaite être accompagnée dans la mise en place des mesures de conformité requises pour encadrer un processus d'anonymisation.

Notes de bas de page

¹ Le 20 décembre 2023, le gouvernement a publié le Projet de règlement sur l'anonymisation des renseignements personnels dans la Gazette officielle du Québec (155^e année, no 51). Depuis, le Projet de règlement a fait l'objet d'une consultation publique et des modifications à son texte ont été proposées. Le Règlement publié le 15 mai dernier diffère donc du Projet de règlement.

Par

[Patrick Laverty-Lavoie, Simon Du Perron](#)

Services

[Cybersécurité, respect de la vie privée et protection des renseignements personnels](#)

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

Les présents renseignements sont de nature générale et ne sauraient constituer un avis juridique, ni un énoncé complet de la législation pertinente, ni un avis sur un quelconque sujet. Personne ne devrait agir ou s'abstenir d'agir sur la foi de ceux-ci sans procéder à un examen approfondi du droit après avoir soupesé les faits d'une situation précise. Nous vous recommandons de consulter votre conseiller juridique si vous avez des questions ou des préoccupations particulières. BLG ne garantit aucunement que la teneur de cette publication est exacte, à jour ou complète. Aucune partie de cette publication ne peut être reproduite sans l'autorisation écrite de Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Si BLG vous a envoyé cette publication et que vous ne souhaitez plus la recevoir, vous pouvez demander à faire supprimer vos coordonnées de nos listes d'envoi en communiquant avec nous par courriel à desabonnement@blg.com ou en modifiant vos préférences d'abonnement dans blg.com/fr/about-us/subscribe. Si vous pensez avoir reçu le présent message par erreur, veuillez nous écrire à communications@blg.com. Pour consulter la politique de confidentialité de BLG relativement aux publications, rendez-vous sur blg.com/fr/ProtectionDesRenseignementsPersonnels.

© 2025 Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Borden Ladner Gervais est une société à responsabilité limitée de l'Ontario.