PROJET DE LOI 64 vs RGPD

Comparaison des mesures de protection des renseignements personnels dans le secteur privé

Tableau récapitulatif et comparatif du PL64 et du RGPD

Prudence AI Inc.

Cabinet d'avocats et multidisciplinaire en Intelligence Artificielle, Protection des Données, Analyse de risque, Vie Privée et Confidentialité, Éthique de l'IA et Cybersécurité.

Nous aidons les organisations de toutes tailles à développer, implanter ou utiliser des solutions d'IA responsables. Nous détenons également une grande expertise dans le secteur de la santé.

Hitachi Systems Security Inc.

Hitachi Systems Security Inc. est un fournisseur mondial de services de protection de la vie privée et de cybersécurité depuis 1999.

La mission de HISYS-SEC est de supporter la confiance dans l'économie numérique en développant des solutions Privacy+Security. Notre équipe d'experts aide nos clients dans plus de 50 pays, 24 heures sur 24 et 7 jours sur 7.

		Québec **Projet de loi (PL) n° 64** ***Loi sur la protection des renseignements personnels dans le secteur privé (Chapitre P-39.1)***	Union Européenne **Règlement Général sur la Protection des Données (RGPD)**
1. Champ d'application	1.1. Temporel	L'étude du projet de loi commencera à l'automne.	Pleinement applicable depuis le 25 mai 2018
	1.2. Territorial	Sur le territoire du Québec: ● Applicable au secteur privé : Toute entreprise qui recueille, détient, utilise ou communique des renseignements personnels ● Applicable au secteur public ● Applicable aux partis politiques	Applicable au secteur privé et public. Critère d'établissement : RT et ST établis dans l'UE ou l'EEE. Critère de ciblage : RT et ST établis hors de l'UE/EEE mais dont les activités de traitement sont liées: * à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou * au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.
	1.3. Matériel	- Champ d'application inchangé pour les entreprises. Spécificités: - Les renseignements personnels visés comprennent ceux recueillis par l'entreprise, même si leur conservation est assurée par un tiers - La LPRPSP ne viendra pas s'appliquer " aux renseignements personnels qui concernent l'exercice par la personne concernée d'une fonction au sein d'une entreprise, tel que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail."	Applicable aux traitements de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données personnelles appelées à figurer dans un fichier Non applicables - Aux traitements réalisés dans le cadre d'une activité strictement personnelle ou domestique - Aux informations anonymisées

2. Définitions	2.1. Renseignement personnel	Tout renseignement qui concerne une personne physique et permet de l'identifier. Quel que soit le support ou format utilisé. Vise également les employés et candidats à un emploi. Les coordonnées d'affaires sont exclues du champ d'application de la loi.	Les «*données à caractère personnel*» sont définies comme toutes informations se rapportant à une personne physique identifiée ou identifiable. Est réputée être une «*personne physique identifiable*» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale
	2.2. Traitement	Il est fait au sein du PL64 davantage référence à la notion de "collecte" avant tout. Cependant dans la note explicative, il est souligné qu'une attention particulière doit être apportée à "tout projet de système d'information ou de prestation électronique de services impliquant la **collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.**	Toute opération ou tout ensemble d'opérations effectués ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction
3. Cadre général du traitement des données	3.1. Grands principes relatifs au traitement des renseignements personnels	Deux grands principes, prévus au préambule du projet, viennent gouverner le texte: - Une confidentialité accrue, remettant au cœur de l'activité commerciale le respect de la vie privée des personnes - Une plus grande sévérité quant au recueil du consentement de la personne, central pour tout traitement de données personnelles	Les données doivent être : - Traitées de manière licite, loyale et transparente au regard de la personne concernée ; - Collectées pour des finalités limitées (i.e. déterminées à l'avance, explicites et légitimes) ; - Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités (principe de minimisation) ; - Exactes et, si nécessaire, tenues à jour ;

			- Conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités ; - Traitées de façon à garantir une sécurité appropriée des données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle
	3.2. Protection des données par conception et par défaut	– Le plus haut niveau de confidentialité doit être assuré par défaut (Privacy by default), sans aucune intervention de la personne concernée. – Le représentant de la protection des renseignements personnels doit être consulté dès le début du projet et peut intervenir à tout moment pour suggérer des mesures de protection des renseignements personnels.	– Mise en œuvre de moyen de protection de la vie dès la détermination et la conception du traitement et par défaut.
4. Fondements juridiques pouvant justifier de la licéité d'un traitement de renseignements personnels	4.1. Consentement	Le consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé. Le consentement n'est pas nécessaire – Lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli – Lorsque son utilisation est manifestement au bénéfice de la personne concernée. – Lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production statistiques et qu'il est dépersonnalisé. Le recueil du consentement des personnes concernées n'est pas nécessaire dans le cadre d'une transaction commerciale si elle est nécessaire aux fins de la	Le consentement est l'une des 6 bases juridiques permettant de justifier le traitement des données personnelles des personnes concernées. Le consentement doit être libre, spécifique éclairé et univoque, sous une forme compréhensible et accessible et ne vaut que pour les finalités déterminées. Il doit être explicite pour certaines catégories et retirable à tout moment.

		conclusion d'une transaction commerciale à laquelle elle entend être partie.	
	4.2. Consentement du mineur	– Âge du consentement du mineur : 14 ans. Avant 14 ans, il convient de recueillir le consentement du titulaire de l'autorité parentale, sauf si le traitement des renseignements personnels est manifestement pour le bénéfice du mineur.	– Âge minimal de 16 ans pour le consentement des mineurs, sauf si le titulaire de l'autorité parentale donne son autorisation – Possibilité pour les États de prévoir un âge inférieur à 16 ans, sans que celui-ci ne puisse aller au deçà de 13 ans
	4.3. Autre fondement juridique d'un traitement	– Le traitement des renseignements personnelles sans consentement est autorisé aux fins de l'exécution d'un contrat.	En dehors du consentement, 5 autres bases juridiques justifient le traitement de données personnelles : – L'existence d'une obligation légale – L'exécution d'un contrat ou de clauses précontractuelles – La sauvegarde des intérêts vitaux de la personne concernée – L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique – L'intérêt légitime poursuivis par le responsable du traitement
5. Renseignements sensibles	5.1. Définition des renseignements sensibles	Article 12 du projet de loi : "*lorsque, de par sa nature 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.* ».	Données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

	5.2. Régime d'exploitation	Article 102 du projet de loi "*le consentement nécessaire à certaines utilisations ou communications d'un renseignement personnel sensible doit être manifesté de façon expresse*" Dès lors que le renseignement personnel est considéré comme sensible, un consentement expresse est requis	Interdiction de principe de traiter des données personnelles à caractère sensible Par exception, traitement rendu possible si : ➢ Consentement explicite de la personne concernée; ➢ Nécessaire aux fins de l'exécution des obligations légales en droit du travail ; ➢ Nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ; ➢ Effectué, dans le cadre des activités légitimes d'une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ; ➢ Concerne des données manifestement rendues publiques par la personne concernée ; ➢ Nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ; ➢ Nécessaire pour des motifs d'intérêt public important ; ➢ Nécessaire aux fins médico-sociales ; ➢ Nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ; ➢ Nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques
	5.3. Renseignements relatifs aux condamnations pénales et aux infractions	Traitement possible si consentement expresse	Traitement possible à condition d'être effectué sous le contrôle de l'autorité publique

6. **Droits des personnes**	6.1. Transparence et information	Information obligatoire des personnes : – Politiques disponibles sur le site internet de l'organisme – Information des personnes concernée lors de la collecte de leurs renseignements personnels	Droit à l'information sur le traitement de données personnelles, que la collecte soit effectuée directement ou indirectement auprès de la personne concernée.
	6.2. Droits sur les données	– Droit d'accès – Droit de suppression – Droit de rectification – Droit à la notification de transfert de données personnelles – Droit de désindexation – Droit de s'objecter à un traitement automatisé	– Droit d'accès – Droit de rectification – Droit à l'effacement – Droit à la limitation du traitement – Droit de portabilité – Droit d'opposition – Droit de ne pas faire l'objet d'une décision individuelle automatisée, y compris le profilage, produisant des effets juridiques ou similaires
7. **Rôles associées à la gestion de la conformité**	7.1. Responsable de traitement	Pas de définition propre du responsable de traitement; "Toute personne qui exploite une entreprise est responsable de la protection des renseignements personnels qu'elle détient." "La personne ayant la plus haute autorité au sein d'un organisme public veille à y assurer le respect et la mise en œuvre" de cette loi. " Division possible dans la responsabilité de traitement entre les fonctions de : – Responsable de l'accès aux documents – **Responsable de la protection des renseignements personnels** – Responsable de la sécurité de l'information – Responsable de la gestion documentaire	Le responsable de traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement Le responsable du traitement est responsable du respect du RGPD et doit être en mesure de démontrer que celui-ci est respecté (principe d'*accountability*) **Responsabilité conjointe :** Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

	7.2. Sous-traitant	Aucune mention/obligation spécifique	Le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Le responsable de traitement doit vérifier que son sous-traitant présente des garanties suffisantes en matière de protection des données. Le traitement réalisé par le sous-traitant doit être régi par un contrat. Le sous-traitant peut engager sa propre responsabilité en cas de manquement à ses obligations contractuelles et manquement au régime de protection des données.
	7.3. Délégué à la protection des données	La fonction de responsable de la protection des renseignements personnels est assurée par la personne ayant la plus haute autorité dans l'entreprise. Cette fonction peut être déléguée par écrit, en tout ou en partie, à un membre du personnel.	Le Délégué à la protection des données est la personnes (physique ou morale) chargée de mettre en œuvre la conformité au RGPD au sein de l'organisme qui l'a désigné, s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.
8. **Mesures de gestion de la conformité**	8.1. Tenue d'un registre	Registre uniquement pour les incidents de confidentialité, (public ou privé)	Le responsable de traitement doit tenir un registre des activités de traitement effectuées sous sa responsabilité. Le sous-traitant doit également tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement.

	8.2. Analyse d'impact sur la protection des données / Évaluation des facteurs relatifs à la vie privée	**Évaluation des facteurs relatifs à la vie privée** Obligatoire notamment pour l'introduction d'une technologie pour tout système d'information ou de prestation de services électroniques ou encore lorsque des renseignements personnels doivent être communiqués à l'extérieur du Québec.	Le Responsable de traitement a pour obligation de réaliser une **Analyse d'impact sur la protection des données** lorsque le traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.
9. Sécurité des renseignements personnels	9.1. Obligation de sécurité	Mise en place des mesures de sécurités propres à assurer la protection des renseignements personnels et qui sont raisonnables au regard de la sensibilité, de la finalité, dans la quantité, de la répartition et des supports de ces renseignements personnels	Le responsable de traitement et le sous-traitant ont pour obligations de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque que représente les traitements de données personnelles.
	9.2. Violations de données / Incident de confidentialité	En cas d'incident de confidentialité qui présente un risque de préjudice sérieux, l'entreprise à l'obligation d'aviser avec Diligence : – La CAI – Toute personne dont un renseignement personnel est concerné – Toute personne ou organisme susceptible de diminuer ce risque L'entreprise a l'obligation de maintenir un registre des incidents de confidentialité et de le transmettre à la CAI sur demande.	En cas de violation de données à caractère personnel : – Obligation de notifier la violation à l'autorité de contrôle compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. – Obligation de communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque celle-ci est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

10. **Transferts internationaux**		– En cas de transferts en dehors du Québec, une évaluation des facteurs relatifs à la vie privée est obligatoire (voir ci-dessus). – Lors de cette évaluation, l'*équivalence* doit être établie et le traitement doit reposer sur un contrat écrit qui traite des résultats de l'évaluation et des mesures en place permettant d'assurer la protection des renseignements personnels. – Le gouvernement produira une liste des États considérées équivalent au Québec, en matière de législation sur la protection des renseignements personnels.	Les transferts de données personnelles en dehors des frontières de l'UE sont possibles à condition que des garanties appropriées soient mises en place pour assurer la sécurité du transfert : – Existence une "décision d'adéquation" dans le pays où a lieu le transfert de données personnelles – La mise en place de garanties appropriées telles que des règles d'entreprise contraignantes ou l'adoption de clauses contractuelles types entre agences...
11. **Contrôles et sanctions**	11.1. Autorité responsable	Commission d'Accès à l'Information du Québec avec pouvoirs renforcés. Exemples : – Possibilité d'émettre des avis de non-conformité. En cas de notification d'un incident de confidentialité, possibilité d'ordonner toute mesure visant à protéger les droits des personnes concernées telles que la remise ou la destruction des renseignements personnels.	**Niveau Européen :** Comité Européen à la Protection des Données (CEPD) **Niveau national** : Autorités de contrôle des États membres de l'UE. Missions d'informer, protéger, accompagner, conseiller, contrôler, sanctionner, anticiper… <u>Exemples de pouvoirs :</u> Pouvoir d'enquête Rappel à l'ordre de l'organisme lorsque les opérations de traitement ont entraîné une violation des dispositions du RGPD Imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement Etc.
	11.2. Coopération avec l'autorité de contrôle	Aucune mention/obligation spécifique	Le responsable du traitement et le sous-traitant doivent coopérer avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions.

	11.3. Sanctions administratives	**Sanctions administratives pécuniaires :** 50 000$ pour une personne physique 10 000 000$ pour une organisation ou 2 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé.	**Amendes administratives** : Selon la nature de l'infraction, jusqu'à 10 Millions d'€ ou 2% du chiffre d'affaires annuel mondial ou 20 Millions d'€ ou 4% du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu).
	11.4. Sanction civile/pénale	– 50 000 $ dans le cas d'une personne physique – 25 000 000 $ pour une organisation ou 4 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier montant est plus élevé. – En cas de récidive les amendes sont doublées.	– La personne ayant subi un dommage matériel ou moral a droit d'obtenir réparation du préjudice subi. – Les États membres de l'UE détermine le régime de sanction applicable en dehors des sanctions administratives précitées.