Table des matières

QUESTIONS ET RÉPONSES 3

Les renseignements personnels 3

Qu'est-ce qu'un renseignement personnel? 3

Est-ce que le renseignement personnel est confidentiel? 3

Quelles sont les conséquences de la confidentialité des renseignements personnels? 3

Qu'est-ce qu'un renseignement personnel sensible? 3

Est-ce que le degré de confidentialité des renseignements personnels sensibles est plus élevé que celui des renseignements personnels? 3

Qu'est-ce qu'un renseignement à caractère public? 3

Est-ce que le renseignement personnel à caractère public est confidentiel? 3

La nouvelle «Loi 25» 3

Quelle est la portée de la Loi 25? 3

Quels sont les organismes visés par la Loi 25? 3

Le cycle de vie des renseignements personnels 4

Qu'est-ce que la collecte des renseignements personnels? 4

Est-ce que la conservation du renseignement personnel est nécessaire pour considérer qu'il y a une collecte de renseignement personnel? 4

Quelles sont les obligations lors de la collecte? 4

Comment évaluer la nécessité de la collecte des renseignements personnels? 4

Qu'est-ce que l'utilisation des renseignements personnels? 4

Quelles sont les obligations lors de l'utilisation? 5

Qu'est-ce que la communication des renseignements personnels? 5

Quelles sont les obligations lors de la communication? 5

Qu'est-ce que la conservation des renseignements personnels? 5

Quelles sont les obligations lors de la conservation? 5

Qu'est-ce que la destruction des renseignements personnels? 5

Quelles sont les obligations lors de la destruction? 5

Est-ce qu'il est possible d'anonymiser les renseignements plutôt que les détruire? 6

Qu'est-ce qu'un renseignement personnel anonymisé? 6

Comment anonymiser les renseignements personnels? 6

Quelles sont les conséquences de l'anonymisation des renseignements? 6

Quelle est la distinction entre une renseignement anonymisé et un renseignement dépersonnalisé? 6

Quelles sont les conséquences de la dépersonnalisation des renseignements? 6

Responsable de la protection des renseignements personnels (ci-après « Responsable de la PRP ») 6

Qui est le Responsable de la PRP? 6

Est-il possible de déléguer la fonction de Responsable de la PRP? 6

Quelles sont les formalités à accomplir pour se conformer à la Loi 25? 7

Quelles sont les tâches du Responsable de la PRP? 7

Quelles seraient les bonnes pratiques pour assurer la conformité? 7

Les politiques et pratiques de protection des renseignements personnels 8

Quelles sont les politiques à mettre en place en matière de gouvernance et de protection des renseignements personnels? 8

Quelles sont les formalités pour mettre en place les politiques en matière de gouvernance et de protection des renseignements personnels? 8

Quelles seraient les bonnes pratiques pour assurer la conformité? 8

L'évaluation des facteurs relatifs à la vie privée (ci-après « EFVP») 8

Qu'est-ce que l'évaluation des facteurs relatifs à la vie privée? 9

Quand faire une évaluation des facteurs relatifs à la vie privée? 9

Quelles seraient les bonnes pratiques pour assurer la conformité? 9

Le signalement des incidents de confidentialité 9

Qu'est-ce qu'un incident de confidentialité? 9

Est-ce que les incidents de confidentialité doivent être déclarés? 9

Comment évaluer la notion de « risque de préjudice sérieux »? 9

Que faire s'il a un « risque de préjudice sérieux »? 9

Quels sont les renseignements devant être notifiées à la CAI? 10
Que doit contenir le registre des incidents? 11
Quelles seraient les bonnes pratiques pour assurer la conformité?..... 11
L'obligation d'information et de transparence 12
Que comprend l'obligation de transparence lors de la collecte?..... 12
Quelles seraient les bonnes pratiques pour assurer la conformité?..... 12
Les nouvelles exigences en matière de consentement.....13
Quels sont les critères de validité du consentement? 13
Quels sont les modalités pour obtenir le consentement des mineurs?..... 13
Quelles sont les situations permettant la communication de renseignements personnels sans le consentement? 13
Quels sont les exceptions pour la réutilisation d'un renseignement sans le consentement? 14
Les nouveaux mécanisme de mise en œuvre 15
Quelles sont les sanctions possibles en cas de non-conformité à la Loi? 15
Quelles sont les sanctions administratives pécuniaires?..... 15
Quelles sont les sanctions pénales?..... 15
Qu'est-ce que les dommages punitifs? 15
LIENS PRATIQUES 16
Planification et mise en œuvre de la Loi 25 16
Liste pour se conformer aux nouvelles exigences de la loi..... 16
Cycle de vie d'un renseignement personnel 16
Liste d'informations à transmettre lors d'une collecte..... 16
Schéma sur les nouveautés liées au consentement 16
Schéma des étapes de la communication de renseignements 16
Gouvernance 16
Gabarit de directive sur la gestion des renseignements personnels..... 16
Gabarit de politique sur la protection des renseignements personnels..... 16
Gabarit de registre des communications de renseignements personnels 16
Guide d'application concernant les règles encadrant la gouvernance à l'égard des renseignements personnels..... 16
Outil pour faciliter la rédaction d'une politique de confidentialité 16
Application du règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique 16
Liste de vérification préalable à la publication d'une politique de confidentialité 17
Incident de confidentialité 17
Schéma du processus qui détermine si une atteinte constitue un événement de sécurité ou un incident de confidentialité 17
Schéma sur le traitement d'un incident de confidentialité..... 17
Détail pour la transmission d'avis et la tenue d'un registre pour les incidents de confidentialité 17
Modèle de lettre d'avis d'incident de confidentialité 17
Liste d'éléments devant apparaitre dans un avis lors d'un incident de confidentialité qui présente un risque de préjudice sérieux 17
Modèle de registre des incidents de confidentialité..... 17
BIBLIOGRAPHIE..... 18
ANNEXES 20
Annexe I Classification des renseignements.....20
Annexe II Tableau des infractions précises 22
Annexe III Aspects procéduraux.....23

QUESTIONS ET RÉPONSES

LES RENSEIGNEMENTS PERSONNELS

**Consulter la classification des renseignements en annexe I **

QU'EST-CE QU'UN RENSEIGNEMENT PERSONNEL?

Un renseignement personnel est : «tout renseignement qui permet d'identifier une personne physique, directement ou indirectement»[1].

EST-CE QUE LE RENSEIGNEMENT PERSONNEL EST CONFIDENTIEL?

Oui. Le renseignement personnel est confidentiel.

QUELLES SONT LES CONSÉQUENCES DE LA CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS?

Nul ne peut communiquer à un tiers les renseignements personnels qu'il détient sur autrui, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie[2].

QU'EST-CE QU'UN RENSEIGNEMENT PERSONNEL SENSIBLE?

Un renseignement personnel sensible est : «un renseignement qui, par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée»[3].

EST-CE QUE LE DEGRÉ DE CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS SENSIBLES EST PLUS ÉLEVÉ QUE CELUI DES RENSEIGNEMENTS PERSONNELS?

Oui. Le consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible[4].

QU'EST-CE QU'UN RENSEIGNEMENT À CARACTÈRE PUBLIC?

«Un renseignement personnel est public lorsque la loi ou un règlement l'indique expressément»[5].

EST-CE QUE LE RENSEIGNEMENT PERSONNEL À CARACTÈRE PUBLIC EST CONFIDENTIEL?

Non. Le renseignement personnel à caractère public n'est pas confidentiel[6].

LA NOUVELLE «LOI 25»

QUELLE EST LA PORTÉE DE LA LOI 25?

La *Loi sur le privé* s'applique à toutes les organisations qui « exploitent une entreprise » au sens de l'article 1525 du Code civil du Québec[7].

La Loi 25 s'applique donc :

- À toutes organisations privées qui collectent des renseignements personnels ou opèrent au Québec ;
- Aux organismes à but non lucratifs qui collectent des renseignements personnels ou opèrent au Québec ; et
- À toutes organisations internationales disposant d'un siège social dans un autre pays ou province que le Québec qui collectent des renseignements personnels au Québec.

QUELS SONT LES ORGANISMES VISÉS PAR LA LOI 25?

Plusieurs organismes sont visés par la Loi 25 notamment :

---

[1] CAI, Qu'est-ce qu'un renseignement personnel?

[2] Art. 13 al.1 *Loi sur le privée*

[3] CAI : «Qu'est-ce qu'un renseignement personnel?»

[4] Art. 13 al.2 *Loi sur le privé*

[5] Université de Montréal https://vie-privee.umontreal.ca/gerer-les-renseignements-personnels/reconnaitre/#:~:text=Un%20renseignement%20personnel%20est%20public,n'est%20donc%20pas%20confidentiel.

[6] *Id.*

[7] Art. 1 al.1 *Loi sur le privée*

- Les ministères et les organismes gouvernementaux;
- Les municipalités et les organismes qui en relèvent, les communautés métropolitaines, les municipalités régionales de comté;
- Les centres de services scolaires, les commissions scolaires, les établissements privés subventionnés, les cégeps, les universités;
- Les établissements de santé et de services sociaux;
- Les ordres professionnels, dans la mesure prévue par le Code des professions (en ce qui concerne les documents détenus dans le cadre du contrôle de l'exercice de la profession)»[8].

LE CYCLE DE VIE DES RENSEIGNEMENTS PERSONNELS

QU'EST-CE QUE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS?

La collecte est le moment pendant lequel le renseignement personnel est recueilli, créé, inféré, c'est-à-dire déduit à partir d'autres renseignements[9].

EST-CE QUE LA CONSERVATION DU RENSEIGNEMENT PERSONNEL EST NÉCESSAIRE POUR CONSIDÉRER QU'IL Y A UNE COLLECTE DE RENSEIGNEMENT PERSONNEL?

Non. le fait de voir un renseignement personnel, comme ceux contenus sur une pièce d'identité, constitue une collecte, même s'il n'y a pas de conservation par la suite[10].

QUELLES SONT LES OBLIGATIONS LORS DE LA COLLECTE?

L'organisme doit[11] :

- Déterminer les fins et les objectifs de la collecte;
- Limiter la collecte de renseignements personnels à ceux qui sont nécessaires :
  - À l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion;
  - À l'exercice des attributions ou à la mise en œuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune;
- Recueillir les renseignements personnels par des moyens légaux et légitimes;
- Fournir certaines informations à la personne concernée lors de la collecte et, par la suite, sur demande.

**Faire section informations à fournir transparence **

** Voici un guide sur la collecte des pièces d'identité **

COMMENT ÉVALUER LA NÉCESSITÉ DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS?

Les conditions suivantes doivent être réunies :

- L'objectif poursuivi est légitime, important et réel;
- L'atteinte à la vie privée est proportionnelle à cet objectif, ce qui signifie plus précisément que :
  - La collecte des renseignements est rationnellement liée aux objectifs;
  - L'atteinte au droit à la vie privée est minimisée. Autrement dit, il n'existe pas d'autres moyens d'atteindre les mêmes objectifs d'une façon qui porte moins atteinte à la vie privée;
  - La collecte, l'utilisation ou la communication du renseignement est nettement plus utile à l'entreprise que préjudiciable à la personne concernée.

** Voir les décisions rendues dans la Section surveillance de la CAI **

QU'EST-CE QUE L'UTILISATION DES RENSEIGNEMENTS PERSONNELS?

[8] CAI : «Organismes publics et documents visés par la Loi»

[9] CAI : «Collecte des renseignements personnels»

[10] *Id.*

[11] CAI : «Champ d'application de la Loi»

L'utilisation est : «la période pendant laquelle le renseignement personnel est utilisé par les personnes autorisées au sein de l'organisme public»[12].

QUELLES SONT LES OBLIGATIONS LORS DE L'UTILISATION?

L'organisme doit [13]:

- Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de l'organisme public lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions;
- Limiter l'utilisation des renseignements personnels. À moins d'une exception prévue par la Loi, l'organisme doit obtenir le consentement de la personne concernée pour utiliser ses renseignements à une autre fin que celles pour lesquelles il a été recueilli.

QU'EST-CE QUE LA COMMUNICATION DES RENSEIGNEMENTS PERSONNELS?

La communication est : «la période pendant laquelle le renseignement personnel est communiqué, par exemple dans un système de prestation électronique de services, par courriel, au service à la clientèle ou par le biais de sites Web»[14].

QUELLES SONT LES OBLIGATIONS LORS DE LA COMMUNICATION?

L'organisme doit[15] :

- Obtenir le consentement des personnes concernées pour communiquer leurs renseignements à un tiers, à moins d'une exception prévue par la Loi;
- Respecter les obligations prévues par la Loi lorsqu'elle communique des renseignements personnels sans le consentement de la personne concernée;
- Respecter les obligations particulières applicables à la communication de renseignements personnels à l'extérieur du Québec.

QU'EST-CE QUE LA CONSERVATION DES RENSEIGNEMENTS PERSONNELS?

La conservation est : «la période durant laquelle un organisme public garde des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non»[16].

QUELLES SONT LES OBLIGATIONS LORS DE LA CONSERVATION?

L'organisme doit[17] :

- Assurer la qualité des renseignements personnels en veillant à ce que les renseignements personnels qu'il détient soient à jour et exacts au moment où il les utilise pour prendre une décision relative à la personne concernée;
- Prendre des mesures propres à assurer la sécurité des renseignements personnels.

QU'EST-CE QUE LA DESTRUCTION DES RENSEIGNEMENTS PERSONNELS?

«Le cycle de vie du renseignement personnel se termine lors de sa destruction».

QUELLES SONT LES OBLIGATIONS LORS DE LA DESTRUCTION?

À cette étape, sauf exception, l'organisme doit[18] :

- Détruire les renseignements personnels de manière sécuritaire dès que la finalité pour laquelle ils ont été collectés est

---

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

accomplie, sous réserve de la Loi sur les archives ou du Code des professions.

- Mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures sont raisonnables compte tenu notamment de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels;
- Permettre l'exercice des droits d'accès et de rectification et répondre avec diligence, dans les 30 jours, aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées. L'absence de réponse dans ce délai équivaut à un refus. Un citoyen peut contester un refus ou une réponse jugée insatisfaisante en exerçant son droit de recours devant la Commission.

EST-CE QU'IL EST POSSIBLE D'ANONYMISER LES RENSEIGNEMENTS PLUTÔT QUE LES DÉTRUIRE?

Oui. La Loi 25 prévoit une alternative à la destruction des renseignements personnels. Suivant l'accomplissement de la finalité de leur collecte, il est possible de les conserver en procédant à leur anonymisation pour les utiliser à des fins sérieuses et légitimes.

QU'EST-CE QU'UN RENSEIGNEMENT PERSONNEL ANONYMISÉ?

«Un renseignement concernant une personne physique est 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 cette personne»[19].

COMMENT ANONYMISER LES RENSEIGNEMENTS PERSONNELS?

«L'anonymisation est un processus complexe qui doit suivre les meilleures pratiques généralement reconnues et selon les critères et les modalités déterminés par règlement du gouvernement»[20].

QUELLES SONT LES CONSÉQUENCES DE L'ANONYMISATION DES RENSEIGNEMENTS?

«Un renseignement anonymisé cesse d'être qualifié de renseignement personnel et n'est plus soumis aux règles applicables en cette matière. Il peut donc être utilisé, communiqué, diffusé et conservé sans autre obligation»[21].

QUELLE EST LA DISTINCTION ENTRE UNE RENSEIGNEMENT ANONYMISÉ ET UN RENSEIGNEMENT DÉPERSONNALISÉ?

Un renseignement personnel est dépersonnalisé : «quand il ne permet plus d'identifier directement la personne concernée»[22].

QUELLES SONT LES CONSÉQUENCES DE LA DÉPERSONNALISATION DES RENSEIGNEMENTS?

Un renseignement dépersonnalisé demeure un renseignement personnel soumis à la Loi sur le privé en cette matière.

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (CI-APRÈS « RESPONSABLE DE LA PRP »)[23]

QUI EST LE RESPONSABLE DE LA PRP?

La Loi 25 prévoit que, par défaut, la personne ayant la plus haute autorité au sein de l'entreprise (en l'occurrence le président) doit veiller au respect de la mise en œuvre de la loi et exercer la fonction du Responsable de la PRP[24].

EST-IL POSSIBLE DE DÉLÉGUER LA FONCTION DE RESPONSABLE DE LA PRP?

---

[19] CAI : «Conservation et destruction des renseignements personnels»

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] Article 3.1 *Loi sur le privé*

[24] Art. 3.1 al. 2 *Loi sur le privé*

Oui, la fonction de Responsable de la PRP peut être délégué, par écrit, en tout ou en partie, à toute personne[25], qu'il s'agisse d'une personne à l'interne ou d'un tiers.

QUELLES SONT LES FORMALITÉS À ACCOMPLIR POUR SE CONFORMER À LA LOI 25?

1. «Envoyer un avis de l'identité de son responsable dans les meilleurs délais, par écrit, à la Commission d'accès à l'information (ci-après « CAI »).
    a. L'avis écrit doit contenir :
        i. Le nom de la personne responsable;
        ii. Le titre de la personne responsable;
        iii. Les coordonnées de la personne responsable;
        iv. La date de son entrée en fonction.
2. Publier sur le site internet[26] ou, à défaut, rendre accessible par tout autre moyen approprié, les éléments suivants :
    a. Le titre de la personne responsable;
    b. Les coordonnées de la personne responsable»[27].

** Consulter l'avis de désignation d'une personne responsable et délégation de responsabilité **

QUELLES SONT LES TÂCHES DU RESPONSABLE DE LA PRP?

- «Approuver les politiques et pratiques en matière de renseignements personnels à établir et mettre en œuvre[28];
- Participer aux évaluations des facteurs relatifs à la vie privée concernant certains systèmes d'information ou de prestation électronique de services [29] et suggérer des mesures afin d'assurer la protection des renseignements personnels traitées dans le cadre de ces systèmes[30];
- Consigner toute communication (faite sans consentement) à une entreprise ou organisme public susceptible de diminuer le préjudice causé par un incident de confidentialité[31] et prendre part à l'évaluation du préjudice causé par un incident de confidentialité[32];
- Recevoir et répondre aux demandes d'accès et de rectification ainsi qu'aux demandes liées à la portabilité des données et au droit à l'oubli[33]»[34].

QUELLES SERAIENT LES BONNES PRATIQUES POUR ASSURER LA CONFORMITÉ?

- «Déterminer les qualifications requises pour exercer le rôle de responsable de la PRP;
    - Déterminer s'il est nécessaire de recruter une personne supplémentaire pour exercer cette fonction.
    - Déterminer s'il est nécessaire de déléguer cette fonction.
- Établir une description des rôles et responsabilités du responsable de la PRP;
- Désigner, par écrit, une personne à titre de responsable de la PRP;
- Prévoir un programme de formation pour le responsable de la PRP;
- Publier les coordonnées du responsable de la PRP sur le site Internet ou à défaut, rendre accessible par tout autre moyen approprié»[35].

---

[25] Art. 3.1 al. 2 *Loi sur le privé*

[26] Art. 3.1 al. 3 *Loi sur le privé*

[27] P. 7 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[28] Art. 3.2 al. 1 *Loi sur le privé*

[29] Art. 3.3 al. 2 *Loi sur le privé*

[30] Art. 3.4 *Loi sur le privé*

[31] Art. 3.5 al. 2 *Loi sur le privé*

[32] Art. 3.7 *Loi sur le privé*

[33] Art. 32, 34, 35 *Loi sur le privé*

[34] P.6 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[35] *Id.*

LES POLITIQUES ET PRATIQUES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS[36]

QUELLES SONT LES POLITIQUES À METTRE EN PLACE EN MATIÈRE DE GOUVERNANCE ET DE PROTECTION DES RENSEIGNEMENTS PERSONNELS?

Les politiques doivent prévoir l'encadrement applicable à :

- La conservation et la destruction des renseignements personnels;
- Les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels;
- Un processus de traitement des plaintes relatives à la protection des renseignements personnels[37].

QUELLES SONT LES FORMALITÉS POUR METTRE EN PLACE LES POLITIQUES EN MATIÈRE DE GOUVERNANCE ET DE PROTECTION DES RENSEIGNEMENTS PERSONNELS?

Les informations détaillées au sujet de ces politiques et de ces pratiques doivent être publiées sur leur site Internet en termes simples et clairs[38].

QUELLES SERAIENT LES BONNES PRATIQUES POUR ASSURER LA CONFORMITÉ?

- «Effectuer un inventaire des politiques, directives, pratiques et procédures en place relativement à la protection des renseignements personnels tout au long de leur cycle de vie;
- Effectuer un exercice de cartographie des données afin de documenter les pratiques de l'entreprise en matière de gestion des renseignements personnels;
- Mettre à jour ou établir les politiques et procédures suivantes, lesquelles doivent établir les rôles et responsabilités des employés de l'entreprise tout au long du cycle de vie des renseignements.
- Mettre en œuvre les politiques et procédures suivantes (ou les intégrer dans un cadre interne relatif à la gestion des renseignements personnels) :
    - Politique établissant les principes généraux relatifs à la collecte, l'utilisation et la communication de renseignements personnels.
    - Politique de conservation des données et calendrier de conservation.
    - Procédure relative aux méthodes de destruction des renseignements personnels et d'anonymisation, le cas échéant.
    - Politique et procédures relatives à la réception et le traitement de plaintes et de demandes d'individus souhaitant exercer leurs droits.
    - Politiques et procédures relatives à la sécurité des données.
    - Politique de gestion des incidents de confidentialité et plan de réponse aux incidents.
    - Politiques particulières en fonction des activités de l'entreprise, par exemple : politique sur l'utilisation des caméras de surveillance, politique sur l'utilisation de systèmes biométriques, politique sur l'utilisation de renseignements personnels pour la recherche et l'intelligence artificielle, etc.
- Développer un programme de formation sur les règles relatives à la protection des renseignements personnels pour les employés qui gèrent ou ont accès à des renseignements personnels;
- Faire approuver les politiques et pratiques par le responsable de la PRP;
- Publier de l'information détaillée au sujet des politiques et pratiques sur le site Internet de l'entreprise»[39].

L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (CI-APRÈS « EFVP »)[40]

[36] Art. 3.2 *Loi sur le privé*

[37] Art. 3.2 al.1 *Loi sur le privé*

[38] Art. 3.2 al. 2 *Loi sur le privé*

[39] Page 7 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[40] Art. 3.3. et 3.4 *Loi sur le privé*

** Consulter le guide d'accompagnement pour réaliser une EFVP**

QU'EST-CE QUE L'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE?

«L'EFVP est une démarche préventive qui vise à mieux protéger les renseignements personnels et à respecter davantage la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auraient des conséquences positives et négatives sur le respect de la vie privée des personnes concernées»[41].

QUAND FAIRE UNE ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE?

Une EFVP doit être effectué préalablement pour tout projet d'acquisition, de développement ou 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[42].

QUELLES SERAIENT LES BONNES PRATIQUES POUR ASSURER LA CONFORMITÉ?

- «Développer une procédure interne sur les EFVP. La procédure devrait, notamment :
  - Définir les critères déclenchant l'obligation d'effectuer une EFVP.
  - Définir un processus pour s'assurer que les projets qui requièrent une EFVP soient identifiés dès le début du projet.
- Communiquer la procédure au sein de l'entreprise.
  - Les responsables devraient informer le responsable de la PRP dès le début d'un projet nécessitant une EFVP.
- Développer un gabarit pour la réalisation d'une EFVP.
  - Former le personnel approprié sur la façon de compléter une EFVP»[43].

LE SIGNALEMENT DES INCIDENTS DE CONFIDENTIALITÉ[44]

QU'EST-CE QU'UN INCIDENT DE CONFIDENTIALITÉ?

Un incident de confidentialité est l'accès, l'utilisation ou la communication non autorisée par la loi d'un renseignement personnel, la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un renseignement personnel[45].

EST-CE QUE LES INCIDENTS DE CONFIDENTIALITÉ DOIVENT ÊTRE DÉCLARÉS?

Oui, «tous les incidents de confidentialité devront faire l'objet d'un processus d'évaluation du « risque de préjudice sérieux », afin de déterminer si l'incident en question devra être notifié à la CAI et aux individus concernés»[46].

COMMENT ÉVALUER LA NOTION DE « RISQUE DE PRÉJUDICE SÉRIEUX »?

Les principaux facteurs à considérer pour évaluer le niveau de gravité du risque du préjudice sont :

- «La sensibilité des renseignements en cause.
- Les conséquences appréhendées de leur utilisation.
- La probabilité qu'ils soient utilisés à des fins préjudiciables»[47].

QUE FAIRE S'IL A UN « RISQUE DE PRÉJUDICE SÉRIEUX »?

«Si l'organisation détermine que l'incident présente un risque de préjudice sérieux pour les individus touchés, elle doit aviser la CAI ainsi

---

[41] P. 4 Guide de EFVP

[42] Art. 3.3 al. 1 *Loi sur le privé*

[43] Page *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[44] Art. 3.5 à 3.8 *Loi sur le privé*

[45] Art. 3.6 *Loi sur le privée*

[46] P.32 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[47] Art. 3.7 *Loi sur le privé*; CAI :«Incidents de confidentialité et mesures de sécurité»

que tout individu concerné par l'incident, à défaut de quoi la CAI pourra lui ordonner de le faire[48].

Il est également prévu que l'entreprise peut, à sa discrétion, aviser toute personne ou organisme susceptible de réduire le risque de dommage, mais en ne lui communiquant que les renseignements personnels nécessaires à cette fin (sans le consentement de l'individu concerné). Dans ce dernier cas, le responsable de la protection des renseignements personnels doit enregistrer la communication»[49].

QUELS SONT LES RENSEIGNEMENTS DEVANT ÊTRE NOTIFIÉES À LA CAI?

1. «Le nom de l'organisation ayant fait l'objet de l'incident de confidentialité et, le cas échéant, le numéro d'entreprise du Québec qui lui est attribué en vertu de la Loi sur la publicité légale des entreprises;
2. Le nom et les coordonnées de la personne à contacter au sein de l'organisation relativement à l'incident ;
3. Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description ;
4. Une brève description des circonstances de l'incident et, si elle est connue, sa cause ;
5. La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période ;
6. La date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident ;
7. Le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres ;
8. Une description des éléments qui amènent l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables ;
9. Les mesures que l'organisation a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, en application du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé, de même que la date où les personnes ont été avisés ou le délai d'exécution envisagé ;
10. Les mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé ;
11. Le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident»[50].

** Consulter l'avis à la CAI concernant un incident de confidentialité impliquant des renseignements personnels et qui présente un risque sérieux **

Que doit contenir l'avis aux personnes concernées?

- «Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- Une brève description des mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

[48] Art. 3.5 al. 2 *Loi sur le privé;* CAI :«Incidents de confidentialité et mesures de sécurité»

[49] P.32 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[50] P.33 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

- Les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
- Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident»[51].

QUE DOIT CONTENIR LE REGISTRE DES INCIDENTS?

- «Une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- La date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
- Le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
- Une description des éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
- Si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant;
- Une brève description des mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé»[52].

QUELLES SERAIENT LES BONNES PRATIQUES POUR ASSURER LA CONFORMITÉ?

- «Définir une structure organisationnelle prévoyant des rôles et responsabilités clairs en matière de prévention, de gestion et de réponse aux incidents.
- Élaborer et le cas échéant mettre à jour la politique de gestion des incidents de l'entreprise de manière à y inclure les nouvelles obligations, et
    - Élaborer un plan de réponse aux incidents détaillé et basé sur les standards de l'industrie ;
    - Faire tester et approuver ce plan par des experts en réponse aux incidents.
- Réviser les contrats avec des fournisseurs de service afin d'y inclure les nouvelles obligations de notification des incidents de manière à s'assurer que :
    - Tous les incidents impliquant des renseignements personnels sont communiqués à l'entreprise rapidement.
    - Les clauses reflètent la nouvelle définition d'un incident de confidentialité.
    - Le fournisseur est en mesure de communiquer à l'entreprise toutes les informations requises pour lui permettre d'évaluer le risque de préjudice sérieux.
- Définir un programme de formation en matière de prévention et de gestion des incidents.
- Tenir un registre au sein de l'entreprise de tous les incidents de confidentialité et ce, même s'ils ne comportent pas de risque de préjudice sérieux. Ce registre devrait comprendre au minimum :
    - Le responsable de l'enquête.
    - Les circonstances de l'incident.
    - La date ou la période où il y a eu un incident.
    - La nature des renseignements personnels visés par l'incident, pour autant qu'elle soit connue.
    - La raison pour laquelle l'entreprise juge que l'incident ne comporte pas de préjudice sérieux pour les individus concernés»[53].

---

[51] CAI :«Incidents de confidentialité et mesures de sécurité»

[52] *Id.*

[53] Page 31 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

L'OBLIGATION D'INFORMATION ET DE TRANSPARENCE[54]

QUE COMPREND L'OBLIGATION DE TRANSPARENCE LORS DE LA COLLECTE[55]?

- Informer l'individu :
  - (i) des fins auxquelles ces renseignements sont recueillis
  - (ii) des moyens par lesquels les renseignements sont recueillis
  - (iii) des droits d'accès et de rectification prévus par la loi
  - (iv) de son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis ; et le cas échéant :
  - (v) du nom du tiers pour qui la collecte est faite ;
  - (vi) du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins auxquelles ces renseignements sont recueillis ; et
  - (vii) de la possibilité que les renseignements soient communiqués à l'extérieur du Québec»[56].

QUELLES SERAIENT LES BONNES PRATIQUES POUR ASSURER LA CONFORMITÉ?

- «Réviser et mettre à jour les politiques de confidentialité (celle visant les clients ainsi que celle visant les employés) et les formulaires et processus d'obtention de consentement. S'assurer que les éléments suivants sont inclus en termes simples et clairs:
  - Fins auxquelles et moyens par lesquels les renseignements personnels sont recueillis. Droits d'accès, de rectification et de retrait du consentement.
  - Nom du tiers pour qui la collecte est faite (le cas échéant).
  - Catégories des fournisseurs de services (le cas échéant).
  - Transfert des renseignements à l'extérieur du Québec (le cas échéant).
- Développer et mettre en place un processus visant à répondre aux questions et aux demandes d'information suivantes des clients ou des employés :
  - Nature des renseignements personnels recueillis par l'entreprise.
  - Catégories d'employés qui pourraient avoir accès aux renseignements personnels.
  - Durée de conservation applicable aux renseignements recueillis auprès de l'individu.
  - Coordonnées du responsable de la PRP.
  - Source des renseignements recueillis auprès d'une autre entreprise (sauf si les renseignements ont été recueillis dans le cadre d'une enquête visant à prévenir, détecter ou réprimer un crime ou une infraction à la loi).
- Faire l'inventaire des technologies utilisées pour recueillir des renseignements personnels et déterminer si elles comportent des fonctions permettant de profiler, de localiser ou d'identifier un individu.
  - Le cas échéant, pour chaque fonction vérifier si des processus adéquats sont en place pour informer les individus, au moment de la collecte, de l'utilisation de la technologie et des moyens d'activer la fonction. Le cas échéant, envisager de mettre en place de nouveaux processus pour demander à l'utilisateur d'activer la fonction.
- Déterminer si des renseignements personnels (de clients ou d'employés) sont collectés par l'entremise de moyens technologiques. Le cas échéant :
  - Faire l'inventaire de ces moyens technologiques.
  - Publier une politique de confidentialité (en termes simples et clairs) sur le site Internet de l'entreprise détaillant ces collectes par l'entremise de moyens technologiques.
  - Diffuser la politique de confidentialité par tout moyen approprié pour atteindre les individus concernés par la collecte de renseignements personnels par des moyens technologiques.
  - Mettre en place une procédure pour mettre à jour la politique de confidentialité afin de s'assurer qu'elle reflète bien les pratiques de l'entreprise et que les

[54] Art. 8 à 8.2 *Loi sur le privé*

[55] Art. 8 al. 1 et 2 *Loi sur le privé*

[56] Page 10 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

individus sont adéquatement informés de ces changements»[57].

LES NOUVELLES EXIGENCES EN MATIÈRE DE CONSENTEMENT[58]

QUELS SONT LES CRITÈRES DE VALIDITÉ DU CONSENTEMENT?

«Pour être valide, le consentement d'une personne doit être :

- Manifeste : évident et donné d'une façon qui démontre la volonté réelle de la personne concernée;
- Libre : impliquant un réel choix et donné sans contraintes et sans pression indue;
- Éclairé : précis, donné en toute connaissance de cause et avec toutes les informations nécessaires pour comprendre la portée du consentement;
- Spécifique : donné dans un objectif précis et clairement circonscrit;
- Temporaire : valide seulement pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé;
- Granulaire : demandé pour chaque fin spécifique;
- Compréhensible : demandé en termes simples et clairs;
- Distinct : demandé distinctement de toute autre information, lorsque la demande est faite par écrit»[59].

QUELS SONT LES MODALITÉS POUR OBTENIR LE CONSENTEMENT DES MINEURS?

- «Si le mineur a moins de 14 ans, le consentement à l'utilisation ou à la communication de ses renseignements personnels doit être donné par le parent ou le titulaire de l'autorité parentale;
- Si le mineur a 14 ans ou plus, le consentement peut être donné par le mineur lui-même ou par le parent ou le titulaire de l'autorité parentale;
- Si cette collecte est manifestement au bénéfice du mineur, les entreprises peuvent toutefois procéder à cette collecte sans consentement parental»[60].

QUELLES SONT LES SITUATIONS PERMETTANT LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS SANS LE CONSENTEMENT?

- «Situations mettant la vie, la santé ou la sécurité d'une personne en danger;
  - Communiquer les renseignements personnels de cette personne sans son consentement à toute personne à qui cette communication doit être faite;
  - Inscrire la communication dans le registre prévu à cet effet.
- Prévention d'un acte de violence présentant un risque sérieux de mort ou de blessures graves;
  - Communiquer uniquement aux personnes exposées à ce danger, à leur représentant et à toute personne susceptible de leur porter secours.
  - Inscrire la communication dans le registre prévu à cet effet.
- Exécution d'un contrat;
  - Dans la mesure où la communication de renseignements personnels est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise que vous avez conclu :
    - Communiquer ces renseignements sans le consentement des personnes concernées.
- Incident de confidentialité;
  - Un organisme public peut aviser toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux à la suite d'un incident de confidentialité. Seuls les renseignements personnels nécessaires peuvent alors être communiqués sans le consentement de la personne concernée. Le

[57] Page 12 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[58] Art. 8.3, 12 et 14 *Loi sur le privé*

[59] CAI : «Consentement des personnes concernées»

[60] *Id.*

responsable de la protection des renseignements personnels doit enregistrer cette communication.

- Fins judiciaires ou d'enquête
  - Communiquer :
    - Au procureur de votre organisme si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi que votre organisme est chargé d'appliquer;
    - Au directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;
    - Au procureur de votre organisme (y compris le procureur général, s'il s'agit de lui) si le renseignement est nécessaire aux fins d'une autre procédure judiciaire que celles mentionnées ci-dessus;
    - À une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;
    - À un autre corps de police si votre organisme est lui-même un corps de police;
    - À une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police ou par une personne ou un organisme agissant en application d'une loi qui exige un rapport de même nature s'il s'agit d'un renseignement sur l'identité de toute autre personne impliquée dans ce même événement (sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement)»[61].

QUELS SONT LES EXCEPTIONS POUR LA RÉUTILISATION D'UN RENSEIGNEMENT SANS LE CONSENTEMENT?

- «Les objectifs de son utilisation sont compatibles avec ceux pour lesquels il a été recueilli. Pour être compatibles, ces nouveaux objectifs doivent avoir un lien pertinent et direct avec les objectifs initiaux;
- Son utilisation est manifestement au bénéfice de la personne concernée. Par exemple l'octroi d'une subvention ou d'une aide financière;
- Son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit prévue expressément par la loi ou non. Par exemple, un organisme pourrait utiliser des renseignements personnels afin de verser une aide financière pour des procédures de recouvrement contre une personne ayant commis une fraude;
- Son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques au sein de votre organisme et qu'il est dépersonnalisé. Dans ce cas, vous devez prendre les mesures raisonnables pour minimiser les risques qu'une personne physique soit réidentifiée à partir de renseignements dépersonnalisés»[62].

Quelles seraient les bonnes pratiques pour assurer la conformité?

1. «Faire l'inventaire des renseignements personnels collectés, utilisés et communiqués par l'entreprise (clients et employés) afin de déterminer :
   a. Ceux qui sont de nature sensible.
   b. Ceux relatifs à des mineurs.
   c. Ceux qui sont exclus du champ d'application de la loi (c.-à-d. coordonnées d'affaires).
2. Faire l'inventaire des formulaires de consentement ou autres documents utilisés pour obtenir le consentement des individus concernés (clients ou employés) et les réviser afin de s'assurer que :
   d. Tout consentement obtenu est manifeste, libre, et éclairé.
   e. Tout consentement est donné à des fins spécifiques en termes simples et clairs.

[61] CAI : «Utilisation et communication de renseignements personnels»

[62] *Id.*

f. Lorsque la demande de consentement est faite par écrit, elle est présentée distinctement de toute autre information communiquée à l'individu.
g. Le consentement du mineur de moins de 14 ans est obtenu par le titulaire de l'autorité parentale ou par le tuteur.
h. Le consentement du mineur de 14 ans et plus est obtenu par le mineur, le titulaire de l'autorité parentale ou alors par le tuteur.

3. Mettre en place un processus afin de s'assurer que sur demande d'un individu (clients ou employés) :
   a. L'entreprise a une procédure en place afin de lui prêter assistance et l'aider à comprendre la portée du consentement demandé.
4. Mettre à jour la politique de classification ou de catégorisation de l'entreprise (ou tout autre document pertinent) afin d'y refléter :
   i. Les renseignements qui sont de nature sensible et ceux relatifs à des mineurs»[63].

LES NOUVEAUX MÉCANISME DE MISE EN ŒUVRE[64]

**Consulter tableau des infractions précises en annexe II **

QUELLES SONT LES SANCTIONS POSSIBLES EN CAS DE NON-CONFORMITÉ À LA LOI?

La Loi 25 prévoit (1) des sanctions administratives pécuniaires (2) des sanctions pénales et (3) un droit d'action privé pour assurer la conformité aux nouvelles exigences[65].

QUELLES SONT LES SANCTIONS ADMINISTRATIVES PÉCUNIAIRES?

Les sanctions administratives pécuniaires peuvent aller jusqu'à 10 000 000$ ou 2% du chiffre d'affaires mondial[66].

QUELLES SONT LES SANCTIONS PÉNALES?

La Cour du Québec peut imposer une amende pouvant aller jusqu'à 25 000 000$ ou 4 % du chiffre d'affaires mondial[67].

QU'EST-CE QUE LES DOMMAGES PUNITIFS?

Il est possible pour un individu de réclamer des dommages et intérêts punitifs d'au moins 1 000$ lorsqu'une atteinte illicite à un droit conféré par la Loi ou par les articles 35 à 40 C.c.Q. cause un préjudice et que cette atteinte est intentionnelle ou résulte d'une faute lourde[68].

---

[63] Page 13 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[64] Art. 90.1 à 93.1 *Loi sur le privé*

[65] Page 3 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

[66] Art. 90.1 à 90.17 *Loi sur le privé*

[67] Art. 91 à 93 *Loi sur le privé*

[68] Art. 93.1 *Loi sur le privé*

LIENS PRATIQUES

PLANIFICATION ET MISE EN ŒUVRE DE LA LOI 25

LISTE POUR SE CONFORMER AUX NOUVELLES EXIGENCES DE LA LOI
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/Outil_activitees_realiservf.pdf

CYCLE DE VIE D'UN RENSEIGNEMENT PERSONNEL

LISTE D'INFORMATIONS À TRANSMETTRE LORS D'UNE COLLECTE
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/Formulaire_Collecte-moyens.pdf

SCHÉMA SUR LES NOUVEAUTÉS LIÉES AU CONSENTEMENT
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/Napperon_consentement.pdf

SCHÉMA DES ÉTAPES DE LA COMMUNICATION DE RENSEIGNEMENTS
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sridail/protection-renseignements-personnels/SRIDAIL_Napperon_CommRP-EtudesRechercheProdStats.pdf

GOUVERNANCE

GABARIT DE DIRECTIVE SUR LA GESTION DES RENSEIGNEMENTS PERSONNELS
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/Gabarit_directive_gestion_rens_perso.pdf

GABARIT DE POLITIQUE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/Gabarit_politique_protect_rens_perso.pdf

GABARIT DE REGISTRE DES COMMUNICATIONS DE RENSEIGNEMENTS PERSONNELS
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/registre-communications.pdf

GUIDE D'APPLICATION CONCERNANT LES RÈGLES ENCADRANT LA GOUVERNANCE À L'ÉGARD DES RENSEIGNEMENTS PERSONNELS
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/Guide_application_Regles_gouvernance.pdf

OUTIL POUR FACILITER LA RÉDACTION D'UNE POLITIQUE DE CONFIDENTIALITÉ
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sridail/reforme/Outil_redaction_politique_confidentialite.pdf

APPLICATION DU RÈGLEMENT SUR LES POLITIQUES DE CONFIDENTIALITÉ DES ORGANISMES PUBLICS RECUEILLANT DES RENSEIGNEMENTS PERSONNELS PAR UN MOYEN TECHNOLOGIQUE

https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/Application_Reglement_Politique_Confidentialite.pdf

LISTE DE VÉRIFICATION PRÉALABLE À LA PUBLICATION D'UNE POLITIQUE DE CONFIDENTIALITÉ
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sridail/reforme/Liste_verification_activite_politique_confidentialite_avis.pdf

INCIDENT DE CONFIDENTIALITÉ

SCHÉMA DU PROCESSUS QUI DÉTERMINE SI UNE ATTEINTE CONSTITUE UN ÉVÉNEMENT DE SÉCURITÉ OU UN INCIDENT DE CONFIDENTIALITÉ
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/incidents-confidentialite/distinction-evenementsecurite-incidentconfidentialite.pdf

SCHÉMA SUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf

DÉTAIL POUR LA TRANSMISSION D'AVIS ET LA TENUE D'UN REGISTRE POUR LES INCIDENTS DE CONFIDENTIALITÉ
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/incidents-confidentialite/detail-transmission-avis-tenu-registre.pdf

MODÈLE DE LETTRE D'AVIS D'INCIDENT DE CONFIDENTIALITÉ
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/incidents-confidentialite/modele-lettre-avis-incident.pdf

LISTE D'ÉLÉMENTS DEVANT APPARAITRE DANS UN AVIS LORS D'UN INCIDENT DE CONFIDENTIALITÉ QUI PRÉSENTE UN RISQUE DE PRÉJUDICE SÉRIEUX
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/incidents-confidentialite/liste-verification-incident-confidentialite-prp.pdf

MODÈLE DE REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ
https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/acces-information/protection_des_renseignements_personnels/incidents-confidentialite/modele-registre-incident.pdf

BIBLIOGRAPHIE

Éloïse GRATTON, Elisa HENRY, François JOLI-CŒUR, Simon DU PERRON, Max JARVIE, Julie M. GAUTHIER, Andy NAGY, Daniel-Nicolas EL KHOURY, Anthony HÉMOND, Catherine LABASI-SAMMARTINO, *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*. Borden Ladner Gervais, 2022.

Commission d'accès à l'information. Protection des renseignements personnels, 2024, en ligne : https://www.cai.gouv.qc.ca/

Coalition Inter-jeune. Loi 25 sur la protection des renseignements personnels, en ligne : https://interjeunes.org/loi-25/

Gouvernement du Québec, Outil en matière de la protection des renseignements personnels, 2024, en ligne : https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/outils

PRÉCISIONS IMPORTANTES

L'INFORMATION JURIDIQUE CONTENUE DANS CE GUIDE EST VALIDE EN DATE D'AVRIL 2025.

L'INFORMATION JURIDIQUE CONTENUE DANS CE GUIDE S'APPLIQUE SEULEMENT AU QUÉBEC ET NE PAS DOIT PAS ÊTRE CONSIDÉRÉE COMME UN AVIS JURIDIQUE.

CE GUIDE PEUT ÊTRE REPRODUIT À DES FINS NON COMMERCIALES.

Clé de vos droits UdS

Clinique juridique universitaire de l'Université de Sherbrooke, offrant gratuitement des services d'information juridique à la population.

ANNEXES

ANNEXE I CLASSIFICATION DES RENSEIGNEMENTS[69]

	Renseignements personnels	**Renseignements personnels sensibles**	**Renseignements personnels ayant un caractère public**

Renseignements d'identification	• Adresse civique personnelle
	• Adresse courriel personnelle
	• État civil
	• Lieu de naissance
	• Matricule employé
	• Nom de famille et prénom de l'enfant à charge
	• Nom de famille et prénom du conjoint
	• Nom de famille et prénom du parent
	• Numéro de téléphone personnel
	• Page Facebook, Instagram ou LinkedIn privée
	• Photographie d'identité
	• Signature
	• Identifiant (login)
	• Jour et mois d'anniversaire
		• Date de naissance
		• Numéro d'assurance-maladie
		• Numéro d'assurance sociale (NAS)
		• Numéro de passeport
		• Numéro de permis de conduire
		• Renseignement de géolocalisation
		• Statut au Canada / Citoyenneté
			• Adresse civique professionnelle
			• Adresse courriel professionnelle
			• Nom de famille et prénom
			• Numéro de téléphone professionnel
			
			Au sein des ministères et des organismes publics :
			• Adresse courriel :
			  ○ Des membres du conseil d'administration;
			  ○ Du personnel de direction;
			  ○ Du sous-ministre et ses adjoints;
			  ○ Du personnel d'encadrement.

Renseignements sur le genre, l'orientation sexuelle, les croyances religieuses	• Langue	• Identité et expression de genre • Orientation sexuelle • Origine ethnique • Premiers peuples (autochtones) • Convictions philosophiques • Opinions politiques • Opinions des participants à la recherche sur des sujets ou qui se trouvent dans des contextes qui pourraient porter préjudice • Religion	

[69] Basé sur le modèle de l'Université de Sherbrooke

Renseignements financiers		• Montant du don d'une personne physique (financier ou en nature) • Numéro de carte de paiement • Numéro de compte bancaire • Renseignement économique relatif à la retraite Revenu annuel	• Salaire des officiers
Renseignements relatifs à l'emploi	• Classification dans l'échelle de traitement • Horaire, absences, congés • Nom de l'ancien employeur	• Évaluation du rendement • Évaluation psychométrique	• Échelle de traitement d'un poste • Fonction/statut employé • Titre d'emploi • Unité de rattachement
Renseignements génétiques, biologiques ou biométriques		• ADN • Salive • Sang • Urine • Empreintes digitales • Reconnaissance faciale	
Renseignements sur le parcours économique		• Inscription à un cours • Inscription à une activité ou un service • Résultat académique • Scolarité, formation, diplôme	
Renseignements sur une enquête		• Allégation de manquement à la conduite responsable en recherche, en matière de harcèlement psychologique, ou de violence à caractère sexuel • Cas de différend • Cas de discipline universitaire (dossier étudiant ou académique) ou de travail • Plainte	
Renseignements liés à des projets de recherche		• Renseignements personnels inclus dans des données de recherche Informations protégées par un accord de non- divulgation • Renseignements financiers confidentiels	• Informations publiées sur le site Web de l'Université

ANNEXE II TABLEAU DES INFRACTIONS PRÉCISES[70]

Sanction pénale	**Sanction administrative pécuniaire**	**Dommages punitifs**
Montant maximal de la sanction		
25 000 000$ ou 4 % du chiffre d'affaires mondial de l'exercice financier précédant	10 000 000$ ou 2 % du chiffre d'affaires mondial de l'exercice financier précédent	Montant des dommages-intérêts punitifs
Facteurs de détermination		
• La nature, la gravité, le caractère répétitif et la durée de • l'infraction • La sensibilité des renseignements personnels concernés • Le fait que le contrevenant ait agi de façon intentionnelle ou avec négligence ou insouciance Le caractère prévisible de l'infraction ou le défaut d'avoir donné suite aux recommandations ou aux avertissements visant à la prévenir • Les tentatives du contrevenant de dissimuler l'infraction ou son défaut de tenter d'en atténuer les conséquences • Le fait que le contrevenant ait omis de prendre des mesures raisonnables pour empêcher la perpétration de l'infraction • Le fait que le contrevenant, en commettant l'infraction ou en omettant de prendre des mesures pour l'empêcher, ait accru ses revenus ou ait réduit ses dépenses ou avait l'intention de le faire • Le nombre de personnes • concernées par l'infraction et le risque de préjudice associé	• La nature, la gravité, le caractère répétitif et la durée du • Manquement • La sensibilité des renseignements personnels concernés • Le nombre de personnes concernées par le manquement et le risque de préjudice associé • Les mesures prises par la personne en défaut pour remédier au manquement ou en atténuer les conséquences • Le degré de collaboration offert à la CAI • La compensation offerte par la personne en défaut, à titre de dédommagement, à toute personne concernée • La capacité de payer de la personne en défaut	• Selon la jurisprudence

[70] P. 5 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*

ANNEXE III ASPECTS PROCÉDURAUX[71]

	Sanction pénale	**Sanction administrative pécuniaire**	**Dommages punitifs**
Délai de prescription	5 ans	2 ans	3 ans
Avis de non-conformité préalable	Optionnel	Oui	Non
Possibilité de conclure un engagement de conformité	Non	Oui	Non
Sanction imposée par :	Cour du Québec	Personne désignée par la CAI	Cour du Québec ou Cour supérieure
Révision administrative	Non	Oui	Non
Droit d'appel/contestation	Oui (Cour supérieure)	Oui (Cour du Québec)	Sur permission (Cour d'appel)

[71] Page 4 *Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé*