CONSEIL
INTERPROFESSIONNEL
DU QUÉBEC

LOI 25

GUIDE D'ACCOMPAGNEMENT POUR LES ORDRES PROFESSIONNELS

LES NOUVELLES RESPONSABILITÉS DES ORDRES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Juin 2022

COMPOSITION DU GROUPE DE TRAVAIL ET DE RÉDACTION

Jennifer Assogba, avocate
Contentieux
Direction des enquêtes et du contentieux
Chambre des notaires du Québec

Linda Bélanger, avocate, LL.B., MBA, ASC
Directrice et secrétaire adjointe
Direction des affaires juridiques
Collège des médecins

Catherine Bolduc, notaire
Notaire-Conseil, Services juridiques
Direction Secrétariat, Services juridiques, Relations institutionnelles et Gouvernance
Chambre des notaires du Québec

France Gauthier, avocate
Conseillère juridique et secrétaire du conseil de discipline
Direction de l'admission, du tableau, des services juridiques,
des greffes et des technologies de l'information
Ordre des dentistes du Québec

Sonia Godin, notaire
Directrice générale et secrétaire
Ordre des psychoéducateurs et psychoéducatrices du Québec

Marco Laverdière, avocat
Secrétaire et directeur général
Ordre des optométristes du Québec

Marie Paré, avocate
Direction, Affaires juridiques
Ordre des infirmières et infirmiers du Québec

Ouafa Younes, avocate
Coordonnatrice aux affaires juridiques
Ordre des technologues professionnels du Québec

REMERCIEMENT

Le CIQ et le groupe de travail souhaitent remercier M^e^ Cynthia Chassigneux de Langlois Avocats pour sa collaboration, le partage de son expertise sur la question et sa disponibilité dans l'élaboration du présent guide.

TABLE DES MATIÈRES

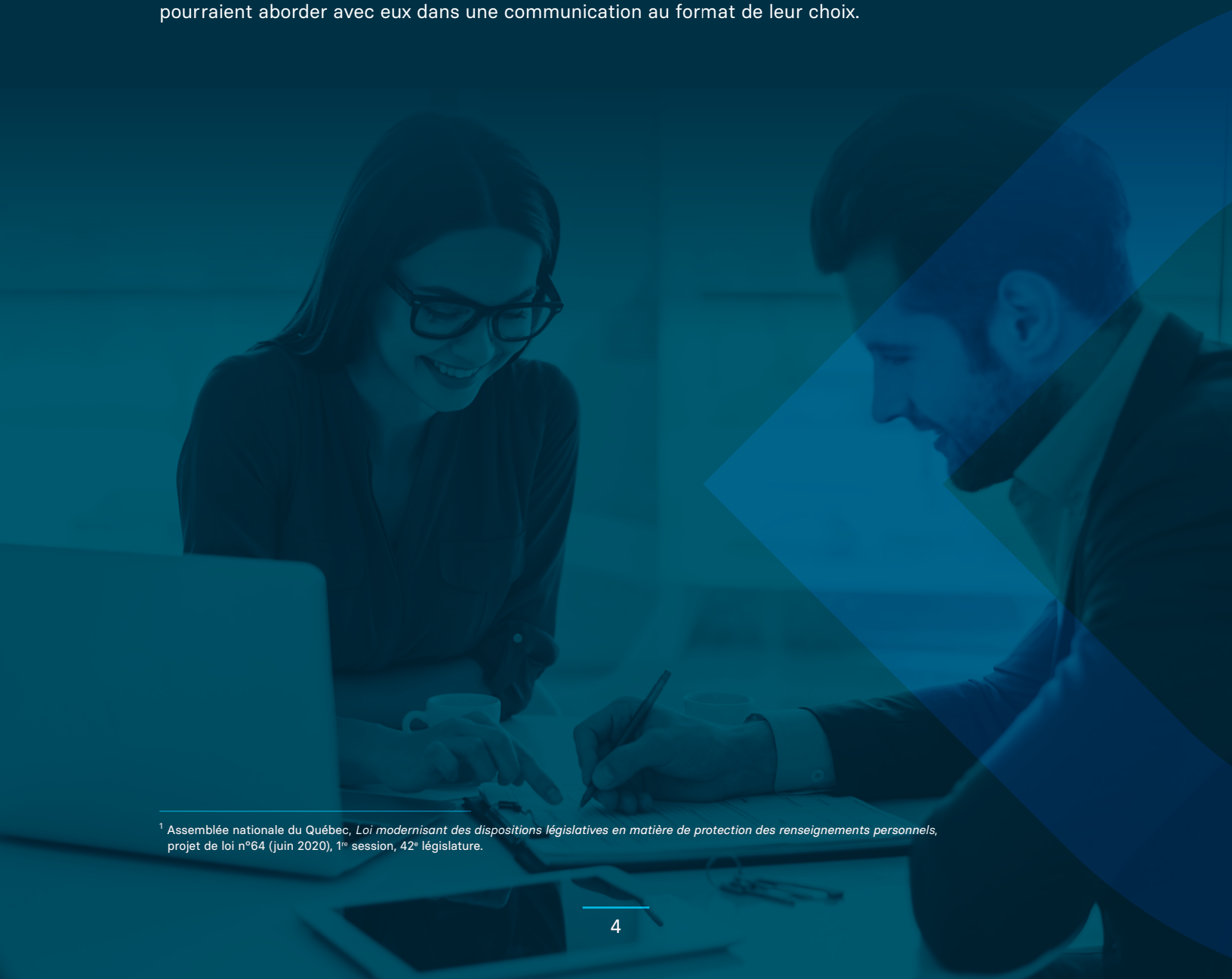
LISTE DES FIGURES

QU'EST-CE QUE LA LOI 25 ET POURQUOI UN GUIDE À L'INTENTION DES ORDRES PROFESSIONNELS?

La « **Loi 25** », ou *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[1], constitue une réforme majeure du cadre juridique relatif à l'accès et à la protection des renseignements personnels au Québec. Elle vise à répondre aux préoccupations croissantes des citoyens en cette matière, en introduisant de nouvelles obligations, tant pour les organismes et entreprises du secteur public que du secteur privé. Il s'agit notamment de favoriser une transparence ainsi qu'une protection de la vie privée accrues pour les citoyennes et les citoyens, en tenant compte des réalités technologiques actuelles. Le Québec suit ainsi beaucoup d'autres juridictions et s'inspire particulièrement du règlement général sur la protection des données (RGPD) du Parlement européen.

Tout en offrant certains outils et références pour s'adapter à cette nouvelle réalité, ce guide est une première référence générale qui explique la nouvelle Loi 25 et recense les dispositions spécifiques applicables aux ordres professionnels, lesquelles, sauf indication contraire, entrent en vigueur le 22 septembre 2022. D'autres documents, concernant les mesures devant entrer en vigueur en 2023 et 2024, seront proposés ultérieurement.

La Loi 25 affectera également les membres des ordres professionnels. À cet effet, la section **Outils préparés à l'intention des ordres professionnels** du présent guide propose une liste de sujets que les ordres pourraient aborder avec eux dans une communication au format de leur choix.



[1] Assemblée nationale du Québec, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi n°64 (juin 2020), 1re session, 42e législature.

RÉGIME HYBRIDE APPLICABLE À UN ORDRE PROFESSIONNEL

Dispositions légales pertinentes :

Art. 108.1 à 108.10 du Code des professions (RLRQ, c. C-26, le « **CP** » ou le « **Code** »);

Art. 1.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1, « **Loi sur l'accès** » ou la « **LAI** »);

Art. 1 de la Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ, c. P-39.1, « **Loi sur le secteur privé** » ou la « **LPRP** »).

Afin de bien identifier les impacts de la Loi 25 sur les ordres professionnels, il importe de faire un léger survol du régime qui les encadre en matière d'accès aux documents et de protection des renseignements personnels.

À la suite des modifications apportées au Code en 2007[2], les ordres professionnels sont soumis à un régime hybride en matière d'accès aux documents et de protection des renseignements personnels. De fait, selon la teneur des documents et renseignements personnels qu'ils détiennent, les ordres peuvent être soit soumis aux règles applicables aux organismes publics, soit aux règles applicables aux personnes qui exploitent une entreprise (secteur privé) ou, encore, à des règles spécifiques qui leur sont propres.

Ainsi, les articles 108.1 et 108.2 du Code prévoient que les lois suivantes s'appliquent aux ordres professionnels, en plus des dispositions spécifiques prévues par ce dernier[3]:

- La Loi sur l'accès, relativement aux documents détenus par un ordre dans le cadre du contrôle de l'exercice de la profession[4] par toute personne, en plus d'assurer la protection des renseignements personnels, comme si un ordre professionnel était un organisme public.
- La Loi sur le secteur privé, relativement aux renseignements personnels autres que ceux détenus dans le cadre du contrôle de l'exercice de la profession. Cette loi vise à assurer la protection des renseignements personnels et à en encadrer l'accès, sans instaurer un régime de transparence, comme celui du secteur public : la confidentialité des renseignements personnels y est érigée en principe, leur communication, en exception.

[2] *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives* (L.Q., 2006, c. 22 ou le projet de loi 86, adopté en 2006, mais dont les dispositions spécifiques concernant les ordres professionnels sont pour la plupart entrées en vigueur en 2007).

[3] Voir notamment les art. 108.3 à 108,10 CP.

[4] Voir l'alinéa 2 de l'article 108.1 CP pour des exemples de ce que le législateur considère comme des documents qui concernent le contrôle de l'exercice de la profession.

Ainsi, bien qu'elles n'entraînent pas de modifications visant spécifiquement le Code, les dispositions de la Loi 25 auront, dès leur entrée en vigueur par étapes entre septembre 2022 et septembre 2024[5], un impact important sur les ordres professionnels, tant en ce qui concerne les documents détenus dans le cadre du contrôle de l'exercice de la profession, qu'en ce qui concerne les autres documents ou renseignements personnels qu'ils peuvent détenir. Afin d'évaluer cet impact, il peut être utile pour les ordres de s'inspirer de la liste d'éléments à réaliser pour se conformer à la Loi 25, mise à la disposition des organismes publics par le gouvernement du Québec[6].

En bref :

- La Loi 25 constitue une réforme majeure du cadre juridique applicable en matière d'accès et de protection des renseignements personnels pour toutes les organisations et entreprises du Québec, autant celles du secteur public que du secteur privé.
- À cet égard, les ordres professionnels sont soumis à un « régime hybride » : ils sont visés par des règles spécifiques prévues par le Code; la Loi sur l'accès s'applique par ailleurs à ce qui relève du contrôle de l'exercice de la profession, alors que la Loi sur le secteur privé s'applique aux autres documents comme si l'ordre professionnel exploitait une entreprise.

[5] À ce sujet, voir notamment : Commission d'accès à l'information du Québec, « Espace évolutif – Projet de loi 64 - Principales modifications législatives », en ligne : https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/principales-modifications/.

[6] Gouvernement du Québec, Secrétariat à la réforme des institutions démocratiques, « Éléments qu'un organisme public doit réaliser pour se conformer aux modifications prévues par la loi modernisant des dispositions législatives en matière de protection des renseignements personnels », en ligne : https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/Outil_activitees_realiservf.pdf?1637878177

INVENTAIRE DES RENSEIGNEMENTS PERSONNELS DÉTENUS PAR UN ORDRE PROFESSIONNEL

Avant même de traiter des nouvelles obligations découlant de la Loi 25, il est primordial pour un ordre professionnel de connaitre les renseignements personnels qu'il détient, puisque la grande majorité de ces obligations les viseront directement ou indirectement. Bien que la préparation d'un inventaire des renseignements personnels détenus par un ordre professionnel ne soit pas une obligation prévue par la Loi 25 en tant que telle, elle en est le point de départ. Il s'agit en effet d'une étape préliminaire essentielle dont la réalisation devrait débuter dès maintenant.

Le présent guide propose un gabarit d'inventaire des renseignements personnels destiné à accompagner les ordres dans ce travail, qui peut être impressionnant de prime abord. Ce gabarit est disponible à la section : **Outils préparés à l'intention des ordres professionnels**. Il se veut une base de départ évolutive et peut être adapté à la réalité et au fonctionnement de chaque ordre professionnel (organigramme, secteurs d'activités et autres particularités). À titre d'exemple, dans l'élaboration de son propre inventaire, chaque ordre professionnel pourra préciser les lieux ainsi que les supports de conservation des renseignements personnels.

Il est à noter que la Loi 25 modifie la définition de « renseignement personnel » en précisant qu'un tel renseignement permet, *directement ou indirectement*, d'identifier la personne physique qu'il concerne[7].

En bref :

- Chaque ordre devrait dès à présent dresser l'inventaire des renseignements personnels qu'il détient.
- L'inventaire devrait inclure notamment la nature des renseignements, leur provenance, leur cycle de vie et leur accessibilité, etc.
- Ces renseignements peuvent concerner notamment les membres (incluant les anciens membres et les candidats à la profession), les étudiants, les employés, les membres des différents comités de l'ordre, les personnes dont les informations sont recueillies dans le cadre d'une enquête, à l'occasion d'évènements (colloques, formations, assemblée générale, etc.), en lien avec l'assurance de la responsabilité professionnelle, ou encore celles se rapportant aux affaires juridiques et contentieuses, etc.

[7] Art. 54 LAI et art. 2 LPRP

COMITÉ SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Dispositions légales pertinentes :

Art. 108.5 CP

Art. 8.1, 63.3, 63.5, 63.6 et 155 LAI

La Loi 25 introduit dans la Loi sur l'accès à l'information[8] le nouvel article 8.1. Ce dernier impose la création, au plus tard le 22 septembre 2022, d'un comité sur l'accès à l'information et la protection des renseignements personnels (le « **CAIPRP** »), lequel relève du directeur général de l'ordre.

La composition du CAIPRP

Le CAIPRP est composé « de la personne responsable de l'accès aux documents, de celle responsable de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise, incluant, le cas échéant, le responsable de la sécurité de l'information et le responsable de la gestion documentaire[9] » . On peut également songer, à titre de « personne dont l'expertise est requise », à la personne responsable de la gestion des risques, s'il ne s'agit pas du responsable de la sécurité de l'information, et/ou à un conseiller juridique, employé ou non de l'ordre. Le directeur général peut en effet faire appel à une ressource externe, s'il l'estime nécessaire.

Les personnes qui exercent au sein d'un ordre l'une ou l'autre des fonctions mentionnées à l'article 8.1 de la Loi sur l'accès sont, par voie de conséquence, membres du CAIPRP, et elles n'ont donc pas besoin d'être désignées à ce titre. Quant aux autres ressources internes ou externes, elles seront désignées par le directeur général, le cas échéant.

Plus spécifiquement, les personnes suivantes devraient siéger au CAIPRP :

- La présidence ou la(les) personne(s) désignée(s) conformément à l'article 108.5 CP afin d'agir comme responsable(s) de l'accès aux documents et de la protection des renseignements personnels ;
- Le syndic, à l'égard des documents et renseignements qu'il obtient ou détient de même que ceux qu'il communique au sein de l'ordre ;
- Le responsable de la sécurité de l'information (le « **RSI** ») ;
- Le responsable de la gestion documentaire ;
- Toute autre personne dont l'expertise est requise, telle que la personne responsable de la gestion des risques, s'il ne s'agit pas du RSI, et/ou un conseiller juridique.

La composition du CAIPRP sera à géométrie variable, selon le cumul des fonctions exercées par une même personne et selon les effectifs et ressources de chacun des ordres. Par exemple, le directeur général peut siéger au CAIPRP, mais la Loi sur l'accès ne l'exige pas.

La Loi sur l'accès ne précise pas à quelle fréquence le CAIPRP doit siéger. Compte tenu du rôle qui lui est confié, le fonctionnement du CAIPRP devrait offrir assez de souplesse pour lui permettre de se réunir aussi souvent que nécessaire, dès que son soutien ou son intervention est requis.

[8] Il n'y a aucune disposition au même effet dans la LPRP. Ainsi, l'exigence de constitution d'un CAIPRP n'est prévue que pour les organismes publics au sens de la LAI, dont les ordres professionnels.

[9] Art. 8.1 LAI

Le rôle du CAIPRP

Le CAIPRP sera chargé de soutenir l'ordre professionnel dans l'exercice de ses responsabilités et dans l'exécution des obligations, imposées par la Loi sur l'accès.

Ainsi, le CAIPRP devra, notamment :

- Approuver et mettre à jour périodiquement les règles encadrant la gouvernance que l'ordre doit adopter à l'égard des renseignements personnels (art. 63.3 LAI et art. 3.2 LPRP) ;
- Élaborer un plan de révision des processus de collecte, d'utilisation, de transmission, de conservation et de destruction des renseignements personnels (dresser un état de la situation ou réaliser un audit en gestion de la protection des renseignements personnels, réaliser une analyse comparative entre la situation actuelle et un cadre optimal, identifier et prioriser des pistes optimales pour tenir compte des principes et nouvelles règles, ainsi que des bonnes pratiques) ;
- Agir comme équipe de gestion des incidents de confidentialité en appliquant le plan prévu à cet effet ;
- Être consulté dès le début de tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant le cycle de vie des renseignements personnels, et suggérer des mesures de protection des renseignements personnels applicables à ce projet (art. 63,5 et 63.6 LAI, art. 3.3 et 3.4 LPRP).

Il importe de préciser que les règles entourant la gouvernance des renseignements personnels, dont le gouvernement peut déterminer le contenu par règlement, pourront prendre la forme d'une politique, d'une directive ou d'un guide, et qu'elles devront notamment prévoir les rôles et les responsabilités des membres du personnel de l'ordre professionnel tout au long du cycle de vie des renseignements personnels qu'il détient, de même qu'un processus de traitement des plaintes relatives à leur protection. Elles devront également inclure une description des activités de formation et de sensibilisation que l'ordre offre à son personnel en matière de protection des renseignements personnels.

En bref :

- L'obligation de mettre en place le CAIPRP entre en vigueur le 22 septembre 2022.
- Le CAIPRP d'un ordre professionnel relève de son directeur général.
- Outre la présence de la présidence (ou de son(sa) délégué(e)) et du syndic, la composition du CAIPRP sera à géométrie variable, selon le cumul des fonctions exercées par une même personne, et selon les effectifs et ressources de chacun des ordres.
- Les personnes qui exercent au sein d'un ordre l'une ou l'autre des fonctions mentionnées à l'article 8.1 (LAI) sont, par voie de conséquence, membres du CAIPRP.
- Le CAIPRP sera chargé de soutenir l'ordre professionnel dans l'exercice de ses responsabilités et dans l'exécution des obligations, imposées par la Loi sur l'accès, dont approuver les règles encadrant la gouvernance des renseignements personnels.

RESPONSABLES DE L'ACCÈS À L'INFORMATION, RESPONSABLES DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET PLUS HAUTE AUTORITÉ

Dispositions légales pertinentes :

Art. 80, 121.1, 108.1 et art. 108.5 CP

Art. 8.1, 17, 50, 53.1, 63.7, 63.9, 65 et art. 100 LAI

Art. 3.1 à 3.5, 3.7, 8, 14, 18.3, 28.1, 30, et art. 34 LPRP

Il est fréquent, au sein d'un ordre professionnel, que la présidence (ou son(sa) délégué(e)) cumule les fonctions de responsable de l'accès aux documents (communément appelé le responsable de l'accès à l'information ou « **RAI** ») et de responsable des demandes d'accès et de rectification faites en vertu du Code et de la Loi sur le secteur privé. Le syndic cumule ces responsabilités à l'égard des documents et renseignements qu'il obtient ou détient, de même que ceux qu'il communique au sein de l'ordre.

La fonction de RAI

La Loi 25 n'apporte aucun changement à la fonction de RAI. En effet, l'article 8 de la Loi sur l'accès ne s'applique toujours pas aux ordres professionnels en raison de l'article 108.1 du Code. Ainsi, le(la) président(e) de l'ordre ou le syndic, le cas échéant, agit comme RAI[10] en vertu de l'article 108.5 du Code.

La fonction de RPRP

Le nouvel article 3.1 de la Loi sur le secteur privé, quant à lui, s'applique aux ordres professionnels. Il prévoit qu'au sein de « l'entreprise », la personne ayant la plus haute autorité exerce la fonction de responsable de la protection des renseignements personnels (le « **RPRP** »). Pour les ordres professionnels, et en vertu de l'article 108.5 du Code, il s'agit encore une fois du président ou du syndic. En effet, les demandes d'accès ou de rectification faites en vertu de la Loi sur le secteur privé, prévues à l'article 108.5 du Code, sont adressées au RPRP[11]; il doit y répondre par écrit[12] et motiver son refus, le cas échéant[13].

La plus haute autorité au sein de l'ordre

Qu'en est-il des responsabilités, autres que celles de RAI et de RPRP, qui découlent de la Loi 25 pour la personne ayant la plus « haute autorité au sein de l'organisation » lorsqu'il s'agit d'un ordre professionnel ? Est-il possible d'affirmer hors de tout doute que le président ou le syndic, le cas échéant, est cette personne ? La Loi sur l'accès ne permet pas de franchir ce pas, faute d'applicabilité de son article 8 aux ordres professionnels.

L'article 3.1 de la Loi sur le secteur privé permet quant à lui de franchir le pas qu'il n'est pas possible de franchir avec la Loi sur l'accès : le président de l'ordre et le syndic, le cas échéant, seraient les personnes ayant la plus haute autorité au sein de l'ordre, selon leurs attributions respectives.

Toutefois, le rôle du syndic étant essentiellement orienté vers le contrôle de l'exercice de la profession, on le voit mal « veiller à assurer le respect et la mise en œuvre de la Loi sur le secteur privé » ; il ne détient pas de renseignements personnels dans un contexte « d'exploitation d'entreprise ». Il est donc permis d'avancer que la plus haute autorité au sein d'un ordre, en vertu de la Loi sur le secteur privé, serait son président.

[10] Par exemple, art. 43 et ss. LAI
[11] Art. 30 LPRP
[12] Art. 32 LPRP
[13] Art. 43 LPRP

Mais cette interprétation n'est pas totalement cohérente avec le rôle confié par le Code au président et au directeur général de l'ordre, le législateur ayant précisé que le président est un administrateur membre du conseil d'administration, pas un dirigeant[14]. De plus, le CAIPRP, dont il était question précédemment, relève du directeur général de l'ordre[15].

Cela dit, la « plus haute autorité au sein d'un ordre » peut-elle être différente en fonction de la loi applicable, soit en fonction de la nature des documents et renseignements personnels dont il est question ? Cela parait difficilement imaginable. Faut-il plutôt, par analogie avec la Loi sur le secteur privé, considérer que le président est la personne ayant la plus haute autorité au sein de l'ordre en vertu de la Loi sur l'accès ? Cette hypothèse est plausible, mais il faudra sans doute attendre que les tribunaux se prononcent sur la question.

La délégation des fonctions de RAI et de RPRP

La prudence est de mise avant de déléguer la fonction de RPRP du président ou du syndic « à toute personne », comme le permet l'article 3.1 précité. D'une part, les dispositions du Code à ce sujet ont été édictées bien avant les modifications que la Loi 25 apporte à la Loi sur l'accès et à la Loi sur le secteur privé[16]. D'autre part, contrairement au président, le syndic ne peut pas déléguer ses fonctions en vertu de l'article 108.5 du Code. Son indépendance doit d'ailleurs être préservée de toute ingérence de tiers[17]. Il est donc recommandé de limiter la délégation de la fonction de RAI ou de RPRP du président aux personnes visées par l'article 108.5 du Code et de considérer, comme le prévoit cet article, que le syndic ne peut toujours pas déléguer ses fonctions de RAI et de RPRP.

Compétence du RAI et du RPRP

Il est à noter que certaines compétences sont nécessaires pour occuper la fonction de RAI ou de RPRP. Ces compétences devraient inclure des connaissances de l'environnement juridique et techniques en matière d'accès à l'information et en protection des renseignements personnels, ainsi que du système professionnel.

Au-delà des compétences requises, le RAI ou le RPRP d'un ordre devrait suivre une formation spécifique sur les changements apportés par la Loi 25. Il est prévu qu'une telle formation générale soit offerte par le Conseil interprofessionnel du Québec (CIQ) aux employés des ordres à l'été 2022.

Par ailleurs, l'ordre doit s'assurer que le titre et les coordonnées du RPRP sont publiés sur son site Internet[18]. De plus, un ordre doit informer toute personne concernée les coordonnées du RPRP, lorsqu'elle en formule la demande[19].

La Commission d'accès à l'information (« CAI ») a l'obligation de diffuser et de mettre à jour un répertoire contenant le titre et les coordonnées des personnes qui exercent les fonctions de RAI et de RPRP dans un ordre[20]. Malgré cela, l'ordre devrait également publier le titre et les coordonnées de son RAI sur son site Internet.

[14] Art. 80 et art. 101.1 CP.
[15] Art. 8.1 LAI.
[16] 1973, 1982 et 1993 respectivement.
[17] Art. 121.1 CP.
[18] Art. 3.1, al. 3 LPRP.
[19] Art. 65 LAI et art. 8 LPRP.
[20] Art. 17 LAI.

La Loi 25 confie essentiellement les responsabilités suivantes au RAI et au RPRP :

A. Responsabilités communes au RAI et au RPRP

- Siéger au CAIPRP ;
- Être membre de l'équipe de gestion des incidents de confidentialité, le cas échéant ;
- Recevoir l'avis sur une violation ou tentative de violation par une personne de l'une ou l'autre des obligations relatives à la confidentialité d'un renseignement communiqué, et effectuer toute vérification relative à cette confidentialité dans le cadre de l'exécution d'un mandat ou d'un contrat de service ou d'entreprise (art. 67.2 LAI et art 18.3 LPRP).

B. Responsabilité exclusive au RAI

- Recevoir les demandes d'accès aux documents et prêter assistance au requérant qui a besoin d'aide pour comprendre la décision d'accès à l'information rendue (art. 43 et art. 50 LAI).

C. Responsabilités exclusives au RPRP

- Voir à la conformité des consentements recueillis par l'ordre et assister la personne concernée pour assurer sa compréhension de la portée du consentement qui lui est demandé (art. 53.1 LAI, art. 14 LPRP) ;
- Enregistrer la communication de renseignements personnels à toute personne ou tout organisme susceptible de diminuer le risque de préjudice sérieux causé par un incident de confidentialité (art. 63.7 LAI et art. 3.5 LPRP) ;
- Participer à l'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité (art. 63.9 LAI et art. 3.7 LPRP) ;
- Recevoir les demandes d'accès et de rectification des renseignements personnels, prêter assistance au demandeur afin d'identifier les renseignements recherchés et l'aider à comprendre la décision rendue à cet égard (art. 94 et ss. LAI, art. 30 et 34 LPRP) ;
- Participer, avec le CAIPRP, à l'établissement et à la mise en œuvre des politiques et des pratiques encadrant la gouvernance de l'ordre à l'égard des renseignements personnels et propre à assurer la protection de ces derniers (art. 63.3 LAI et art. 3.2 LPRP) ;
- Participer, avec le CAIPRP, aux évaluations des facteurs relatifs à la vie privée (art. 63.5 LA et art. 3.3 et 3.4 LPRP) ;
- Répondre aux demandes de cessation de diffusion d'un renseignement personnel, de désindexation et de réindexation d'hyperliens (art. 28.1 LPRP).

En bref :

- Le président de l'ordre, ou son(sa) délégué(e), et le syndic exercent les fonctions de RAI et de RPRP.
- Il faut prévoir un plan de formation si la personne pressentie pour être RAI ou RPRP ne possède par l'expertise nécessaire avant son entrée en fonction.
- Un ordre doit s'assurer que le titre et les coordonnées du RPRP sont publiés sur son site Internet.
- Un ordre doit informer toute personne concernée des coordonnées du RPRP lorsqu'elle en formule la demande.

INCIDENTS DE CONFIDENTIALITÉ

Dispositions légales pertinentes :

Art. 108.5 CP

Art. 8.1, 63.3, 63.7 à 63.10 et 63.1 LAI

Art. 3.1, 3.2, 3.6, 3.7 et 10 LPRP

Lorsqu'il est question de la protection des renseignements personnels et de leur sécurité, il faut se demander « Quand un incident de confidentialité aura-t-il lieu ? » et « Est-ce que nous serons prêts à y faire face ? ». La Loi 25 oblige les ordres à mettre en place une série de mesures afin de se préparer au mieux pour répondre à ces questions.

On peut définir un incident de sécurité comme un incident affectant la disponibilité, l'intégrité ou la confidentialité d'un actif informationnel d'une organisation.

La Loi 25, quant à elle, définit ce qu'est un incident de confidentialité (« **IC** »), soit :

- **l'accès, l'utilisation, ou la communication non autorisée par la loi de renseignements personnels, la perte de renseignements personnels ou toute autre atteinte à la protection de renseignements personnels**[21]**.**

Un IC est donc un incident de sécurité, alors que l'inverse n'est pas nécessairement vrai.

Un incident ayant les conséquences prévues par la Loi 25 sur des renseignements qui ne sont pas personnels au sens de la Loi 25 constituera un incident de sécurité, mais pas un IC. Ainsi, les dispositions légales traitant des IC ne trouveront pas application. Cependant, cela ne signifie pas qu'un tel incident de sécurité soit sans conséquence sur la réputation et d'autres aspects de l'ordre, de sorte que l'équipe de gestion des IC, dont il est question ci-dessous, pourrait quand même devoir être impliquée.

L'IC peut résulter d'un geste volontaire ou involontaire commis par une personne de l'interne (employé, membre d'un comité, administrateur de l'ordre, etc.) ou de l'externe (sous-traitant, prestataire de services, pirate informatique, etc.).

Parmi les différents types d'IC, on retrouve **l'hameçonnage**, le déploiement de **logiciels malveillants**, les attaques par **rançongiciel**, les **botnets**, les **attaques par force brute**, l'envoi de renseignements personnels à une mauvaise adresse courriel, la perte d'une enveloppe par le service de courrier, etc.[22].

[21] Art. 63.8 LAI et art. 3.6 LPRP. Au fédéral, il s'agit d'une « atteinte aux mesures de sécurité », définie à l'article 2 de la *Loi sur le secteur privé et les documents électroniques* (L.C., ch. 32).

[22] Voir Borden Ladner Gervais, « Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises », novembre 2021, page 45, en ligne : https://www.blg.com/fr/insights/2021/11/quebec-privacy-law-reform-a-compliance-guide-for-organizations.

Constituer une équipe de gestion des incidents de confidentialité

L'équipe de gestion des IC d'un ordre professionnel doit être formée d'un noyau de personnes internes et, le cas échéant, de l'externe, dont le nombre peut varier en fonction de la taille de l'ordre. Idéalement, ces personnes entretiennent de bonnes relations, connaissent bien le système professionnel et sont en mesure de communiquer entre elles, 24 h sur 24, 7 jours sur 7 et 365 jours par année, car les IC se produisent habituellement en dehors des heures de travail d'un ordre.

Quoique leur présence dans l'équipe ne soit pas absolument essentielle, les personnes extérieures à l'ordre seront sollicitées pour leur expertise particulière en matière d'IC, ce qui permet de gagner un temps précieux en situation de crise. Elles pourront également prêter main-forte au personnel de l'ordre qui pourrait momentanément surcharger de travail. Enfin, la collaboration d'un notaire ou d'un avocat expérimenté présente l'avantage non négligeable de soumettre les communications de l'ordre en matière de IC au secret professionnel du conseiller juridique, protégé par les chartes et le code de déontologie de ces professionnels.

Considérant ce qui précède, il est recommandé que les personnes suivantes constituent le noyau de base de l'équipe de gestion des IC :

- Un membre de la direction (pour la prise de décisions) ;
- Une personne désignée parmi les employés de l'assureur en cyberrisques ;
- Les responsables de la sécurité des technologies de l'information interne et/ou externe ;
- Les conseillers juridiques internes et/ou externes ;
- Les responsables des communications internes et/ou externes.

Les membres ou une partie des membres du CAIPRP, ou du comité des mesures d'urgence, peuvent faire partie de l'équipe de gestion des IC, auquel cas les renseignements contenus dans le présent guide concernant le CAIPRP, les RAI et les RPRP s'appliqueront avec les adaptations nécessaires. Ainsi, le RAI, le RPRP (si l'incident touche des renseignements personnels) et le responsable de la gestion documentaire pourraient être membres de l'équipe de gestion des IC.

D'autres intervenants pourront se greffer à ce noyau de base, selon la nature et l'ampleur de l'IC :

- Un membre du conseil d'administration ;
- Le syndic, si l'incident concerne des documents et renseignements qu'il obtient ou détient, de même que ceux qu'il communique au sein de l'ordre ;
- Le responsable des ressources humaines et le président du syndicat (si des renseignements personnels d'employés ou des employés eux-mêmes sont impliqués dans l'IC) ;
- Le responsable des relations avec les clientèles (public, membres) ;
- Le responsable des relations institutionnelles et intergouvernementales ;
- Les partenaires corporatifs, sous-traitants, fournisseurs, etc.

Il est recommandé que les membres de l'équipe de gestion des IC soient nommés par le directeur général de l'ordre et que leurs fonctions soient identifiées dans une directive qui comprendra également le plan de gestion des incidents de sécurité à appliquer. Le rôle de l'équipe étant essentiellement opérationnel, la directive sera également adoptée par le directeur général (sans nécessiter d'approbation par le conseil d'administration) et communiquée à tous les employés.

La loi exige que le titre et les coordonnées du RPRP soient publiés sur le site Internet de l'ordre. Elle ne prévoit rien de particulier en ce qui a trait à l'équipe de gestion des IC. Toutefois, l'ordre doit publier sur son site Internet :

- les règles entourant sa gouvernance à l'égard des renseignements personnels ;
- les règles prévoyant les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie des renseignements personnels ;
- un processus de traitement des plaintes relatives à la protection des renseignements personnels ;
- une description des activités de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels.

L'équipe devrait se réunir chaque fois qu'un ordre a des motifs de croire qu'un incident de sécurité s'est produit, afin de déterminer s'il s'agit d'un IC impliquant des renseignements personnels. Les rencontres devraient avoir lieu aussi souvent que nécessaire pour prendre les mesures raisonnables afin de diminuer les risques de préjudice grave et de prévenir d'autres IC de même nature. En somme, les rencontres sont requises dès les premiers signaux d'un IC jusqu'au post mortem des opérations.

Afin de reconnaître les signaux précurseurs des principaux scénarios d'attaque, et de répondre promptement et efficacement à ces attaques, il est recommandé de suivre une formation et d'aiguiser les réflexes de l'équipe en testant l'application du plan de gestion des incidents de sécurité, avec l'assistance d'un expert.

De plus, les personnes susceptibles de répondre aux questions des médias devraient parfaire leurs techniques d'entrevues.

Quel est le rôle l'équipe de gestion des IC?

En amont, l'équipe de gestion des IC participe, avec le directeur général, à l'élaboration d'un plan de gestion des incidents de sécurité (voir la section suivante), ainsi qu'à sa révision périodique.

Elle prendra immédiatement en charge les opérations conformément à ce plan. Si elle a des motifs de croire que l'incident de sécurité est un IC, elle doit prendre les mesures raisonnables pour diminuer les risques de préjudice et pour prévenir d'autres incidents de même nature.

L'équipe de gestion doit identifier la cause de l'incident de sécurité, déterminer s'il s'agit d'un IC, évaluer son ampleur, le documenter et mettre en branle diverses actions prévues au plan, au moment opportun, notamment :

- Mettre les systèmes hors service avec les messages appropriés ;
- Bloquer des accès, changer des mots de passe ;
- Déployer le plan de continuité des affaires ;
- Identifier les données et les personnes touchées (les propriétaires des renseignements personnels) ;
- Évaluer le préjudice potentiel et s'il peut être « sérieux » ;
- Aviser la CAI, les personnes touchées ou des tiers ;
- Déployer un plan de communication ;
- Prévenir les services policiers ;
- Mettre en place du soutien pour les personnes touchées (ligne téléphonique directe, surveillance du crédit, documentation pertinente…) ;
- Etc.

En bref :

L'équipe de gestion des IC doit être formée d'un noyau agile de personnes internes et, le cas échéant, externes.

- Les membres ou une partie des membres du CAIPRP, ou du comité des mesures d'urgence, peuvent faire partie de l'équipe de gestion des IC.
- L'équipe de gestion des IC participera, en amont, avec le directeur général, à l'élaboration d'un plan de gestion des incidents de sécurité, ainsi qu'à sa révision périodique.
- En cas d'incident de sécurité, l'équipe de gestion des IC prendra immédiatement en charge les opérations, conformément au plan.
- L'équipe doit être constituée dès à présent puisque les obligations légales relatives à la gestion des incidents de confidentialité entrent en vigueur le 22 septembre 2022.

ÉTABLISSEMENT D'UN PLAN DE GESTION DES INCIDENTS DE SÉCURITÉ

Dispositions légales pertinentes :

Art. 59, 63.7 à 63.10 LAI

Art. 3.5 à 3.8 LPRP

Il est nécessaire d'établir un plan de gestion des incidents de sécurité afin d'en effectuer l'analyse et de déterminer les actions à prendre selon les circonstances. À ce propos, un modèle de plan et de grille d'analyse est mis à votre disposition sous forme de directive dans la section : **Outils préparés à l'intention des ordres professionnels**.

Évaluation du risque de préjudice sérieux

Dans l'éventualité où l'équipe de gestion des IC a des motifs de croire que l'incident de sécurité est un IC[23] au sens de la Loi 25, elle doit évaluer s'il y a un risque qu'un préjudice sérieux soit causé. Pour cela, elle doit prendre en considération certains éléments, tels que la sensibilité des renseignements concernés[24], les conséquences appréhendées de leur utilisation, et la probabilité qu'ils soient utilisés à des fins préjudiciables[25].

En attendant que la CAI se prononce sur ces notions et, à titre indicatif, il est utile de souligner que la *Loi sur le secteur privé et les documents électroniques* (L.C., ch. 32, art. 10), précise ce qu'est un « risque réel de préjudice grave » (par opposition à « sérieux » dans la Loi 25)[26] :

> « [...] ***préjudice grave*** vise notamment la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles. »

[23] Voir la section précédente du présent guide pour en savoir davantage sur les IC.
[24] Art. 59 LAI et art. 12 LPRP.
[25] Art. 63.7 et 63.9 LAI, art. 3.5 et 3.7 LPRP
[26] Art. 10.1 (7) LPRPDE

Obligation d'aviser

À compter du 22 septembre 2022, et en cas de risque de préjudice sérieux, l'ordre professionnel doit aviser la CAI, ainsi que toute personne dont un renseignement personnel est concerné par l'incident, et ce, avec *diligence*. Au surplus, toute personne ou tout organisme susceptible de diminuer le risque peut être avisé[27].

Un futur règlement précisera sans doute le contenu et les modalités des avis aux personnes dont un renseignement personnel est concerné par l'IC. Dans l'intérim, il est recommandé de consulter le *Règlement sur les atteintes aux mesures de sécurité* (DORS/2018-64), adopté en vertu de la LPRPDE, lequel précise notamment, à l'article 3, ce que doit contenir « l'avis relatif à une atteinte aux mesures de sécurité » :

a) les circonstances de l'atteinte ;

b) la date ou la période où il y a eu atteinte ou, si elle n'est pas connue, une approximation de la période ;

c) la nature des renseignements personnels visés par l'atteinte, pour autant qu'elle soit connue ;

d) les mesures que l'organisation a prises afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte ;

e) les mesures que peut prendre tout intéressé afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte ou afin d'atténuer un tel préjudice ;

f) les coordonnées permettant à l'intéressé de se renseigner davantage au sujet de l'atteinte.

Enfin, la CAI dispose, sur son site Web, d'un formulaire servant à l'aviser[28]. Lorsqu'un IC est porté à son attention, elle peut ordonner l'application de toute mesure visant à protéger les droits des personnes concernées pour le temps et aux conditions qu'elle détermine[29].

En bref :

- Tous les incidents de confidentialité devront faire l'objet d'un processus d'évaluation du « risque de préjudice sérieux ».
- S'il y a risque de préjudice sérieux, l'ordre doit aviser : la CAI, les personnes dont un renseignement personnel est concerné par l'incident et, au besoin, les tiers (ex. : police, agences de crédit, etc.) susceptibles de diminuer ce risque.

[27] Art. 63.7 LAI et art. 3.8 LPRP
[28] Commission d'accès à l'information du Québec, « Formulaires et lettres types pour les ministères et organismes », en ligne : https://www.cai.gouv.qc.ca/formulaires-et-lettres-types/pour-les-ministeres-et-organismes/
[29] Art. 127.2 LAI et art. 81.3 LPRP

REGISTRE DES INCIDENTS DE SÉCURITÉ

Dispositions légales pertinentes :

Art. 63.10 LAI

Art. 3.8 LPRP

Il est de la responsabilité d'un ordre de tenir un registre des incidents de sécurité, distinguant ceux qui constituent des IC au sens de la Loi 25. Le présent guide propose, à la section : **Outils préparés à l'intention des ordres professionnels**, un gabarit de registre conçu pour un ordre professionnel et adaptable à la réalité de chacun. Un tel registre doit être implanté avant le 22 septembre 2022.

Le registre doit contenir **tous** les incidents de sécurité, peu importe leur gravité, et ce, même s'ils ne comportent pas de risque de préjudice sérieux. En attendant le règlement sur la teneur du registre, le registre exigé en vertu de la LPRPDE doit être conservé « pendant vingt-quatre mois après la date à laquelle l'organisation conclut qu'il y a eu atteinte » et doit comporter « tout renseignement qui permet au commissaire [fédéral à la protection de la vie privée] de vérifier la conformité aux paragraphes 10.1(1) et (3) de la [LPRPDE] »[30], soit :

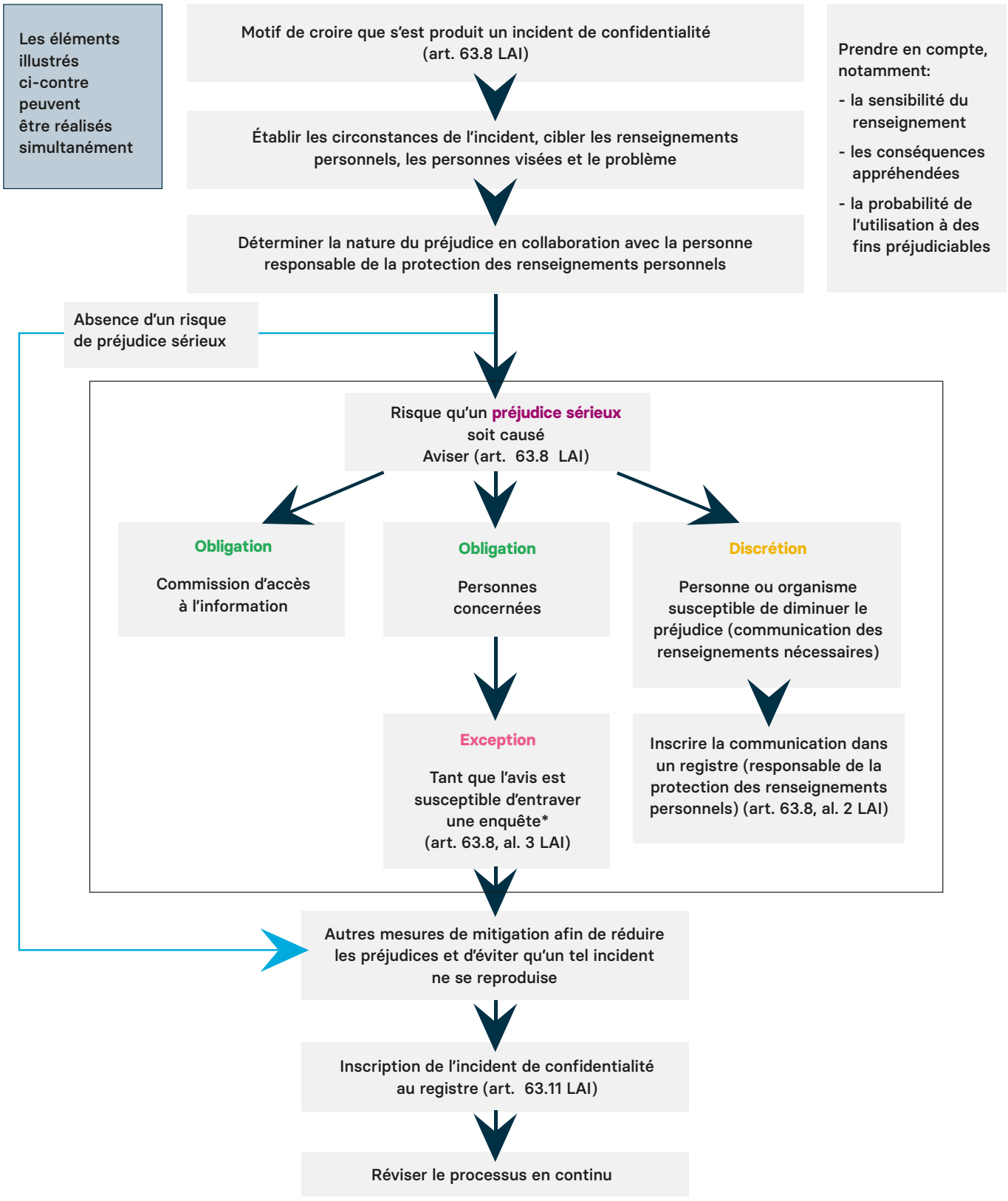
- Le responsable de l'enquête ;
- La description de l'incident ;
- La date ou la période où il y a eu un incident ;
- La nature des renseignements personnels visés par l'incident, pour autant qu'elle soit connue ;
- Le nombre de personnes concernées ;
- La déclaration de l'incident ou non à la CAI ;
- La raison pour laquelle l'ordre juge que l'incident ne comporte pas de préjudice sérieux pour les individus concernés ;
- Les mesures qui ont été prises ou qui peuvent être prises afin d'atténuer le risque ou le préjudice.

Dans la mesure où un ordre professionnel compte plus d'un RAI/RPRP et que son fonds d'assurance-responsabilité professionnelle a, tout comme le syndic, des enjeux de confidentialité qui diffèrent de ceux des autres directions de l'ordre, il est possible d'envisager la tenue de plus d'un registre des incidents de sécurité. Ce faisant, le registre n'aura pas l'effet indésirable de divulguer de l'information confidentielle à des personnes non autorisées au sein de l'ordre. Toutefois, si la CAI demande à consulter le registre de l'ordre, il faudra s'assurer de lui faire parvenir l'ensemble des registres.

[30] Voir les articles 10.3 LPRPDE et 6 (1) du Règlement sur les atteintes aux mesures de sécurité (DORS/2018-64).

FIGURE I : SCHÉMA SUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL

(Articles 63.8 à 63.11 de la Loi sur l'accès aux documents des organismes public et sur la protection des renseignements personnels (LAI))



Reproduction du document du gouvernement du Québec : « Schéma sur le traitement d'un incident de confidentialité impliquant un renseignement personnel (articles 63.8 à 63.11 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LAI)), en ligne : https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf?1637173195

COMMUNICATION À DES FINS D'ÉTUDE, DE RECHERCHE ET DE PRODUCTION DE STATISTIQUES

Dispositions légales pertinentes :

Art. 67.2.1 à 67.2.3 LAI

Art. 21 à 21.0.2 LPRP

Afin de communiquer des renseignements personnels, sans le consentement des personnes concernées à une personne, un organisme ou une entreprise qui souhaite les utiliser à des fins d'étude, de recherche ou de production de statistiques (les « FÉRPS »), un ordre professionnel devra effectuer une évaluation des facteurs relatifs à la vie privée (une « EFVP »).

La Loi 25 prévoit l'exigence d'effectuer une EFVP dans plusieurs circonstances[31], dont la première est la communication à des FÉRPS.

La CAI définit l'EFVP comme « une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée »[32]. Le guide sur les EFVP produit par la CAI,[33] ainsi que celui produit par le **Commissaire à la protection de la vie privée fédéral**, contiennent des informations pertinentes qui sauront vous orienter dans la réalisation d'une EFVP.

À noter également qu'une EFVP, en vertu de la Loi sur l'accès et la Loi sur le secteur privé, doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support[34].

Dans la mesure où les résultats de l'EFVP permettent la communication des renseignements personnels, cette communication devra être précédée d'une entente entre l'ordre et le destinataire des renseignements.

En bref :

- La première exigence de réalisation d'une EFVP est prévue pour le 22 septembre 2022, dans le cadre de la communication de renseignements personnels à des FÉRPS.
- D'autres EFVP devront être réalisées au fur et à mesure de l'entrée en vigueur de la Loi 25.

[31] Voir les EFVP des articles 63.5, 64, 68 et 70.1 de la LAI, et celles des articles 3.3 et 17 de la LPRP, dont l'entrée en vigueur n'est prévue que pour septembre 2023.
[32] Commission d'accès à l'information du Québec, « Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée », en ligne : https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf, document mis à jour le 10 mars 2021. À noter cependant l'avertissement de la CAI à l'effet qu'il pourrait être remanié en profondeur en raison de la Loi 25.
[33] *Ibid.*
[34] Art. 3.3 LPRP

RÉVISION DES ENTENTES, MANDATS ET CONTRATS DE SERVICE DE L'ORDRE

Dispositions légales pertinentes (année d'entrée en vigueur):

Art. 67.2.2,67.2.3 (2022 – traités dans la section précédente du guide) et 70.1 (2023) LAI

Art. 17, 18.3 (2023), 21 et 21.0.2 (2022) LPRP

La Loi 25 implique de nouvelles exigences contractuelles entre l'ordre et ses différents partenaires. Bien que ces exigences n'entrent pas toutes en vigueur en septembre 2022, il est recommandé que l'ordre effectue un inventaire de ses contrats afin de les mettre à jour et d'y prévoir le contenu exigé par la Loi 25.

Par la même occasion, l'ordre s'assurera veillera à mettre en place des dispositions exigeant de ses partenaires qu'ils se conforment à la Loi 25. En effet, la Loi sur le secteur privé énonce désormais clairement qu'elle s'applique aux renseignements personnels, et que leur conservation doit être assurée par l'entreprise ou par un tiers[35] (principe qui était d'ailleurs déjà prévu par la Loi sur l'accès[36] pour les organismes publics). Il pourrait s'agir de clauses qui prévoient, par exemple, l'obligation des partenaires d'aviser l'ordre en cas d'incident de sécurité, de collaborer dans la réalisation des EFVP ou des modalités dans le but d'atténuer les risques identifiés dans une EFVP, précédant une communication de renseignements personnels à l'extérieur du Québec.

Le groupe de travail offre un modèle de clauses contractuelles dans la section: **Outils préparés à l'intention des ordres professionnels.**

[35] Art. 1 LPRP
[36] Art. 1 LAI

APPLICATION DES LOIS, SURVEILLANCE ET SANCTIONS EN CAS D'INFRACTION

Dispositions légales pertinentes (date d'entrée en vigueur) :

Art. 158 à 167 LAI (2023)

Art. 90.1 à 93,1 LPRP (2023 ou entrée en vigueur à la date fixée par le gouvernement)

À l'instar des orientations prises en Europe avec le RGPD, le législateur souhaite, avec la Loi 25, lancer un message clair quant au caractère sérieux accordé à la protection des renseignements personnels. Pour ce faire, la Loi 25 introduit un nouveau régime de sanctions administratives pécuniaires, des sanctions pénales beaucoup plus importantes, ainsi que la reconnaissance d'action en droit privé pour les particuliers.

Sanctions administratives pécuniaires

La Loi 25 introduit dans la Loi sur le secteur privé un tout nouveau régime de sanctions administratives pécuniaires consistant en l'imposition par « une personne désignée par la CAI, mais qui n'est pas membre de l'une de ses sections » d'une amende pouvant aller jusqu'à 10 000 000 $ ou 2 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier est plus élevé.

Sanctions pénales

De nouvelles infractions, en vertu desquelles la CAI peut intenter des poursuites pénales, sont introduites dans la Loi sur le secteur privé. Désormais, ces infractions peuvent être sanctionnées par la Cour du Québec par l'imposition d'une amende pouvant aller jusqu'à 25 000 000 $ ou 4 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier est plus élevé. En cas de récidive, ces amendes seront portées au double.[37]

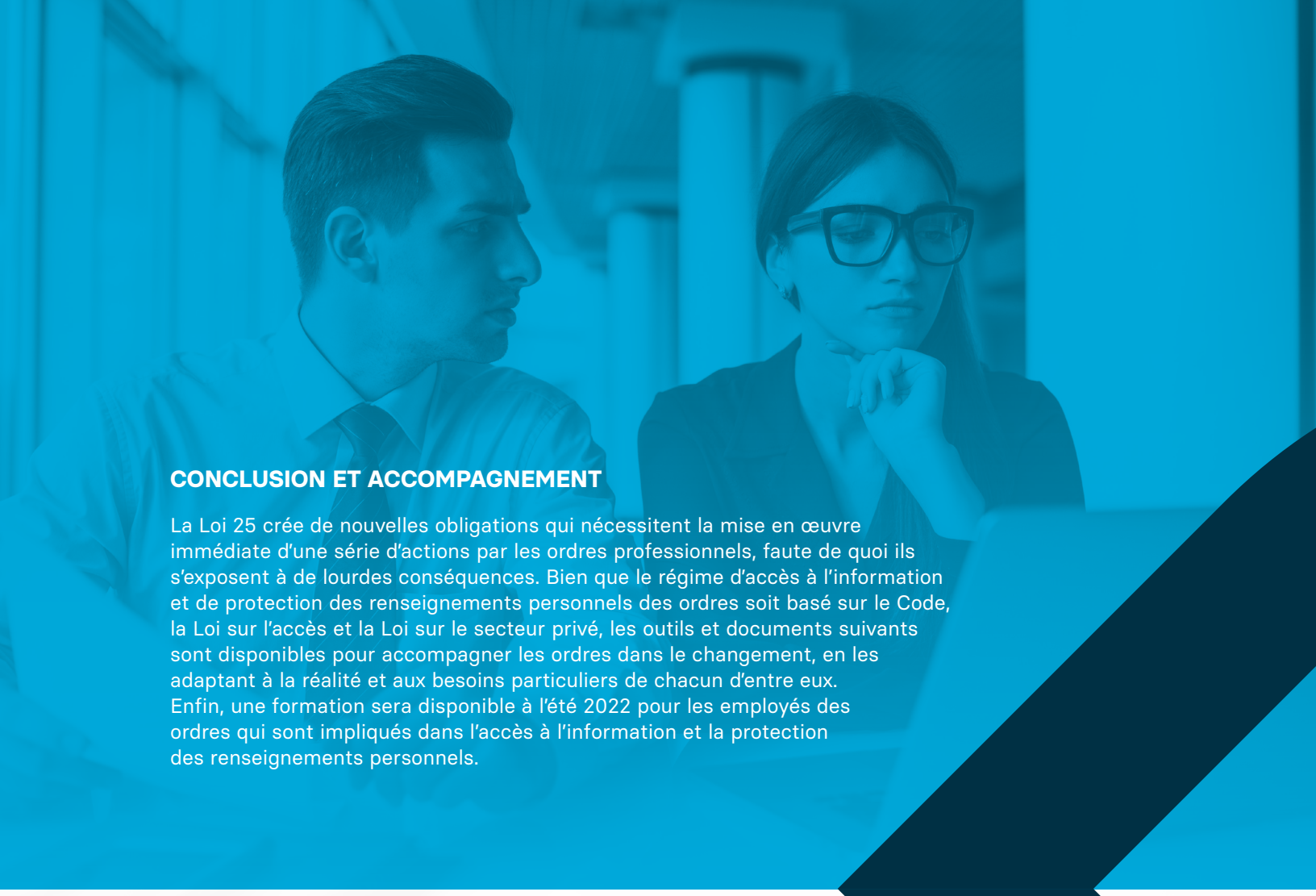
La Loi 25 a également pour effet de hausser le montant des amendes prévues à la Loi sur l'accès en cas d'infraction, amendes qui, en cas de récidive, sont portées au double[38].

Droit privé d'action

La Loi sur le secteur privé permet désormais à une personne de réclamer des dommages-intérêts punitifs d'au moins 1 000 $ en cas d'une atteinte à un droit conféré par cette loi ou en vertu des articles 35 à 40 du Code civil du Québec. Pour cela, l'atteinte doit être intentionnelle ou résulter d'une faute lourde.

Il en va de même de la Loi sur l'accès, en cas d'atteinte à un droit reconnu au chapitre III qui concerne la protection des renseignements personnels.

[37] Art. 92.1 LPRP
[38] Art. 164.1 LAI



CONCLUSION ET ACCOMPAGNEMENT

La Loi 25 crée de nouvelles obligations qui nécessitent la mise en œuvre immédiate d'une série d'actions par les ordres professionnels, faute de quoi ils s'exposent à de lourdes conséquences. Bien que le régime d'accès à l'information et de protection des renseignements personnels des ordres soit basé sur le Code, la Loi sur l'accès et la Loi sur le secteur privé, les outils et documents suivants sont disponibles pour accompagner les ordres dans le changement, en les adaptant à la réalité et aux besoins particuliers de chacun d'entre eux. Enfin, une formation sera disponible à l'été 2022 pour les employés des ordres qui sont impliqués dans l'accès à l'information et la protection des renseignements personnels.

OUTILS PRÉPARÉS À L'INTENTION DES ORDRES PROFESSIONNELS

- **Proposition de sujets à traiter dans une communication des ordres à leurs membres**
- **Gabarit d'inventaire des renseignements personnels détenus par un ordre professionnel**
- **Registre des incidents de sécurité**
  Incluant les incidents de confidentialité* et les atteintes aux mesures de sécurité**
- **Modèles de clauses contractuelles**
- **Plan de gestion de risque de sécurité et grille d'analyse**

FIGURE II : LIGNE DU TEMPS : PLANIFICATION DE L'ENTRÉE EN VIGUEUR DE LA LOI 25

SEPTEMBRE 2022

- Rôle et responsabilités de la personne ayant la plus haute autorité et fonctions de responsable
- Mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels
- Principe de responsabilité d'un organisme public
- Incident de confidentialité
- Communication à des fins d'étude, de recherche ou de production de statistiques
- Changement à la structure de la Commission d'accès à l'information et octroi de certains pouvoirs
- Lignes directrices de la Commission d'accès à l'information

SEPTEMBRE 2023

- Adoption et diffusion de règles de gouvernance
- Politique de confidentialité
- Communication dans un processus de deuil
- Devoir d'assistance du responsable pour aider un requérant à comprendre sa décision
- Informations à fournir aux personnes dans le cadre d'une collecte
- Collecte en collaboration avec un autre organisme public
- Utilisation des renseignements dépersonnalisés
- Exigences pour une communication conforme à l'article 68 de la Loi sur l'accès
- Exigences pour une communication à l'extérieur du Québec
- Sanctions pénales
- Mandat ou contrat de services ou d'entreprise
- Anonymisation des renseignements personnels
- Critères de validité d'un consentement
- Collecte et consentement en lien avec les renseignements personnels d'un mineur
- Consentement exprès lors de certaines utilisations et communications de renseignements personnels sensibles
- Acquisition, développement et refonte de système d'information ou de prestation électronique de services (Protection de la vie privée dès la conception)
- Protection par défaut pour les produits ou services technologiques offerts au public disposant de paramètres de confidentialité
- Décision fondée exclusivement sur un traitement automatisé
- Utilisation d'une technologie comprenant des fonctions d'identification, de localisation ou de profilage

SEPTEMBRE 2024

- Droit à la portabilité

Adapté de la ligne du temps du gouvernement du Québec : « Planification de l'entrée en vigueur du projet de loi 64 modernisant des dispositions législatives en matière de protection des renseignements personnels », en ligne https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/LigneTemps_PL64.pdf?1632344059

ANNEXE I : DOCUMENTS DISPONIBLES POUR CONSULTATION

Espace évolutif – Projet de loi 64, Commission d'accès à l'information du Québec. On y retrouve notamment une version administrative de la Loi sur l'accès à l'information et de la Loi sur le secteur privé, tel qu'elles entreront en vigueur en septembre 2022, 2023 et 2024.

« Formulaire de déclaration d'un incident de sécurité portant atteinte à des renseignements personnels », Commission d'accès à l'information.

Guide d'accompagnement - Réaliser une évaluation des facteurs relatifs à la vie privée : Commission d'accès à l'information, 10 mars 2021.

Incidents de sécurité : Mieux vaut prévenir que guérir ! et Aide-mémoire, Commission d'accès à l'information, mai 2021.

Réagir en cas d'incident de sécurité et Que faire en cas de perte ou de vol de renseignements personnels (organismes et entreprises), Commission d'accès à l'information, 29 mars 2021.

Formulaire de désignation d'une personne responsable et délégation de responsabilités en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, Commission d'accès à l'information.

« Éléments qu'un organisme public doit réaliser pour se conformer aux modifications prévues par la loi modernisant des dispositions législatives en matière de protection des renseignements personnels », Gouvernement du Québec, Secrétariat à la réforme des institutions démocratiques.

« Schéma sur le traitement d'un incident de confidentialité impliquant un renseignement personnel », Gouvernement du Québec, Secrétariat à la réforme des institutions démocratiques.

« Ligne du temps – Planification de l'entrée en vigueur du projet de loi 64 modernisant des dispositions législatives en matière de protection des renseignements personnels », Gouvernement du Québec, Secrétariat à la réforme des institutions démocratiques.

Réforme des lois québécoises en matière de protection des renseignements personnels : Guide de conformité pour les entreprises, Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) , 23 novembre 2021, pages 45 et suivantes.

Protection et gouvernance des données : Opérationnalisation des nouvelles exigences et opportunités, KPMG, janvier 2022, page 17.

Dossier spécial du CAIJ : mis à jour en continu

Centre de ressources – Réforme des lois québécoises sur la protection des renseignements personnels, Fasken (dont le Bulletin numéro #24 intitulé « Projet de loi 64 : Quel est l'impact concret du projet de loi sur les ordres professionnels ? », paru le 23 novembre 2020)

Commissariat à la protection de la vie privée du Canada : voir particulièrement la section sur le signalement d'une atteinte à la vie privée au sein de votre entreprise.

CONSEIL
INTERPROFESSIONNEL
DU QUÉBEC

550, rue Sherbrooke Ouest, Tour ouest
bureau 2050, Montréal (Québec) H3A 1B9

Tél. : 514 288-3574 • Tél. : 514 288-3580

www.professions-quebec.org