JOURNÉE PROFESSIONNELLE

Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

6 octobre 2021
Session A – 9 h à 12 h | Session B – 13 h à 16 h

aapi.qc.ca

AAPI Association des professionnels en accès à l'information et en protection de la vie privée

PRÉSENTATION DES DISPOSITIONS DE LA LOI 95, *Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives*.

- ***Objectif : Faire état des enjeux dans l'application de la Loi 95 aux fins de la valorisation des données numériques dans le respect des obligations de la vie privée.***

Formatrice AAPI : Me Marie-Claude Daraiche, avocate, responsable de l'ADPRP, Direction du Bureau de la sous-ministre et du Secrétariat général, ministère de la Justice

Plan de présentation

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

Introduction

Réalité des organismes publics

- Composent avec plusieurs environnements (sites web, infonuagique, applications web, appareils intelligents connectés à Internet, comptes de médias sociaux, etc.).

Enjeu actuel

- La sécurité des données emmagasinées ou qui circulent dans ces environnements est susceptible d'être compromise et les menaces prennent diverses formes (virus, rançongiciels, logiciels de détournement, etc.).

Objectif gouvernemental

- Rehausser considérablement la cybersécurité et rendre la gestion des données plus efficiente (un communiqué a été publié le 10 juin 2021 par le cabinet du ministre délégué à la Transformation numérique gouvernementale).

Introduction

Plusieurs outils accompagnent le virage numérique que prend l'administration publique :

- Stratégie de transformation numérique gouvernementale 2019-2023
  - Le gouvernement souhaite « tirer profit du numérique pour offrir de meilleurs services et accroître leur efficience et leur transparence ».
- Création du Centre gouvernemental de cyberdéfense (2019)
  - Vise à solidifier l'expertise du gouvernement dans la gestion des cyberattaques et des menaces.
- Politique gouvernementale de cybersécurité (2020)
  - Vise à mobiliser les organismes afin que tous soient proactifs et adoptent des comportements sécuritaires. L'un des objectifs de la Politique est de mettre à jour la législation et de réviser les cadres de gouvernances existants.

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

1. Changements législatifs (PL nº 95)

Entrée en vigueur

Les nouvelles dispositions sont entrées en vigueur le 10 juin 2021.

Objet de la loi

Le projet de loi nº 95 modifie d'abord l'objet de la Loi.

On y retrouve de nouveaux éléments :

- Offrir des services aux citoyens qui s'appuient sur les technologies de l'information (TI) dont les technologies numériques;
- Assurer la protection adéquate des ressources informationnelles (RI);
- Instaurer une gouvernance et une gestion optimales des données numériques gouvernementales;
- Coordonner les initiatives en transformation numérique.

1. Changements législatifs (PL nº 95)

Le projet de loi nº 95 intervient sur les quatre volets suivants :

1. **Sécurité de l'information (articles 12.2 et s.);**
2. **Données numériques gouvernementales (articles 12.10 et s);**
   - Dispositions particulières aux renseignements personnels (articles 12.14 à 12.17);
3. **Transformation numérique (articles 12.8 et 12.9);**
   - Production d'un plan de transformation numérique pour avoir une vision globale des projets en cours dans les organismes publics (ce volet ne sera pas traité aujourd'hui);
4. **Signature électronique**
   - Une modification apportée à la Loi concernant le cadre juridique des technologies de l'information (RLRQ, c. c-1.1) (ce volet ne sera pas traité aujourd'hui).

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

2. Sécurité de l'information (SI) (articles 12.2 et s.)

Cette nouvelle section réitère que :

- Tous les organismes publics doivent assurer la protection des ressources informationnelles (RI) et de l'information détenue;
- Tous les organismes publics doivent se plier aux exigences gouvernementales et aux instructions écrites données par le Dirigeant principal de l'information (DPI);
  - Dans le PL nº 95, on emploi le terme « indications d'application »;
- Tous les organismes publics (OP) doivent prendre toutes les mesures pour corriger les impacts dus à un bris de sécurité ou à en réduire le risque.

2. Sécurité de l'information (articles 12.2 et s.)

Le DPI et les dirigeants de l'information (DI) ont de nouvelles fonctions :

Articles 7.1 et 12.6	Articles 9.1 et 12.7
Le DPI agit à tire de « Chef gouvernemental de la sécurité de l'information ». Il doit : • Diriger l'action gouvernementale en matière de SI; • Fournir un modèle pour déterminer le niveau de sécurité requis par les données numériques gouvernementales; • Signifier des attentes en matière de SI et fournir des règles écrites aux OP; • Surveiller la mise en œuvre des obligations par les OP et évaluer les mesures prises.	Le DI agit à tire de « Chef délégué de la sécurité de l'information ». Il doit : • Appuyer le Chef gouvernemental de la SI; • Appliquer les règles en matière de SI; • Assurer la protection des RI et de l'information, notamment en ce qui concerne : o la gestion des risques et des vulnérabilités; o la mise en œuvre de mesure contre toutes les formes d'atteintes (cyberattaques ou menaces); • Prendre des mesures en cas d'atteinte; • Formuler des règles pour son OP; • Surveiller la mise en œuvre des obligations par son OP et évaluer les mesures prises.

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

2. Sécurité de l'information (articles 12.2 et s.)

À retenir :

- Les modifications apportées démontrent la volonté d'avoir une **vision globale** en matière de RI au sein l'appareil gouvernemental;
  - D'ailleurs, il est souhaité de surveiller davantage les mesures concrètement déployées dans les OP;
- L'accent est également mis sur la **gestion des incidents** qui se doit d'être plus soutenue, plus efficace;
  - À ce compte, on autorise le partage rapide d'informations lorsque vient le temps de gérer un tel incident (article 12.2 à 12.4).

2. Sécurité de l'information (articles 12.2 et s.)

À retenir (suite) :

- Le DPI et les DI pourront formuler des **règles en matière de ressources informationnelles (RI), incluant la SI** (au niveau gouvernemental pour le DPI et au sein de l'organisme pour les DI);
  - Règlement d'application à venir pour encadrer le partage rapide d'informations lors d'une atteinte (articles 12.2 à 12.4, 22.1.1);
  - Indications d'application en RI à venir (articles 12.6 à 12.7).

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

2. Sécurité de l'information (articles 12.2 et s.)

Rôle du responsable de la protection des renseignements personnels (PRP)

- Le DPI et les DI doivent formuler des règles et surveiller la mise en œuvre de celles-ci.
  - *Quel est l'impact sur le rôle du responsable de la PRP?*
- De nouvelles dispositions autorisent la communication de renseignements, personnels ou non, lorsque cela est nécessaire pour gérer un incident de sécurité.
  - *Quel est l'impact sur le rôle du responsable de la PRP?*

3. Données numériques gouvernementales (articles 12.10 et s)

L'objectif de cette section est de favoriser la **mobilité** et la **valorisation** des données numériques gouvernementales à **des fins administratives ou de services** publics tout en assurant le droit à la vie privée (article 12.10).

- ***Mobilité*** *: communication ou transmission de données entre organismes publics.*
- ***Valorisation*** *: la mise en valeur d'une donnée numérique gouvernementale, excluant sa vente ou toute autre forme d'aliénation.*
- ***Fins administratives ou de services publics*** *: l'une ou l'autre des fins énoncées à l'article 12.10 par exemple, la vérification de l'admissibilité d'une personne à un programme ou à une mesure.*

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

3. Données numériques gouvernementales (articles 12.10 et s)

Dans le mémoire accompagnant le projet de loi nº 95, il est indiqué que « les données numériques gouvernementales permettent de comprendre et d'anticiper les besoins de la population, d'assurer une prestation optimale des services publics et de mettre en œuvre avec efficacité et efficience les politiques publiques. Pour ce faire, il importe que les organismes publics agissent de manière concertée à l'intérieur d'un cadre de gestion propre aux données numériques gouvernementales ».

3. Données numériques gouvernementales (articles 12.10 et s)

Qu'est-ce que les données numériques gouvernementales?

- Article 12.10 : toute information portée par un support technologique, incluant un support numérique, détenue par un organisme public, à l'exclusion :

  a. d'une information sous le contrôle d'un tribunal judiciaire ou d'un autre organisme public lorsqu'il exerce des fonctions juridictionnelles;

  b. d'une information déterminée par règlement du gouvernement ou faisant partie d'une catégorie déterminée par un tel règlement, notamment une information visée par une restriction au droit d'accès en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1).

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

3. Données numériques gouvernementales (articles 12.10 et s)

Le gouvernement peut, par décret, désigner un organisme pour agir comme **source officielle de données numériques gouvernementales** (article 12.13).

Conditions :

- Recommandation du Président du Conseil du trésor et du ministre responsable de l'organisme visé;
  - La recommandation vient du ministre de la Santé et des Services sociaux lorsque les données proviennent d'un organisme sous sa responsabilité;
- Énoncer les données concernées dans le décret;
- Énoncer les finalités dans le décret.

3. Données numériques gouvernementales (articles 12.10 et s)

Qu'est-ce qu'une **source officielle de données numériques gouvernementales**?

- *Un organisme qui « recueille, utilise ou communique des données numériques gouvernementales ou recueille auprès de toute personne des renseignements, incluant des renseignements personnels, lorsque cela est nécessaire à une fin administrative ou de services publics » (article 12.13).*

Le gouvernement peut également déterminer les organismes publics qui doivent recueillir ces données auprès de la source et les utiliser ou qui doivent les communiquer à cette dernière.

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

3. Données numériques gouvernementales (articles 12.10 et s)

Le DPI et les DI ont de nouvelles fonctions :

Article 7.1, 12.11 et 12.18	Article 9.2 et 12.12
Le DPI agit à titre de « Gestionnaire des données numériques gouvernementales ». Il doit : • Conseiller le président du Conseil du trésor; • Maintenir à jour un inventaire des données; • Élaborer des stratégies de mobilité ou de valorisation des données; • Autoriser la mobilité ou la valorisation des données; • S'assurer que le niveau de sécurité et les normes de qualité des données soient conformes aux cadres établis; • Contrôler la qualité des données et les mesures assurant leur sécurité; • Veiller à l'application des règles prises en vertu de l'article 12.19; • Soutenir les OP et les DI • Toute autre tâche attribuée par le SCT; • Déterminer les sources officielles de données de référence (article 12.18) – Données ouvertes.	Le DI agit à titre de « Gestionnaire délégué aux données numériques gouvernementales ». Il doit : • Soutenir son organisation dans l'application de ces obligations; • Appuyer le gestionnaire des données numériques gouvernementales (DPI); • Appliquer les règles émises par le DPI ou le gouvernement.

3. Données numériques gouvernementales (articles 12.10 et s)

Dispositions particulières en matière de protection des renseignements personnels (PRP)

- Autorisation de communiquer à une source officielle (article 12.14) :
  - Nécessité;
  - Intérêt public ou au bénéfice des personnes;
  - Dépersonnaliser les données, si possible.
- Exigences (articles 12.15 et 12.16) :
  - Évaluation des facteurs relatifs à la vie privée;
  - Déterminer des règles de gouvernance;
  - Remettre un rapport à la Commission d'accès à l'information.

AAPI Association des professionnels en accès à l'information et en protection de la vie privée
JOURNÉE PROFESSIONNELLE EN PVP| 6 octobre 2021
Les enjeux des changements législatifs et jurisprudentiels sur vos pratiques professionnelles en protection de la vie privée

3. Données numériques gouvernementales (articles 12.10 et s)

Rôle du responsable de la protection des renseignements personnels (PRP)

- Certains organismes publics seront des sources officielles de données numériques gouvernementales et/ou des sources officielles de données de référence.
  - *Quel est l'impact sur le rôle du responsable de la PRP?*

Merci pour votre attention!

AAPI Association des professionnels en accès à l'information et en protection de la vie privée

COMPLÉMENT D'INFORMATION DANS LE CADRE DE LA PRÉSENTATION SUR LES DISPOSITIONS ET LES ENJEUX D'APPLICATION DE LA LOI 22, Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives (L.Q. 2021, c. 22)

Avertissement : Le lecteur est prié de se référer au texte officiel publié par l'Éditeur officiel

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2021C22F.PDF

OBJECTIF : État des enjeux dans l'application de la Loi 22 aux fins de la valorisation des données numériques dans le respect des obligations de la vie privée.

Ce complément d'information accompagne la présentation diffusée lors de la Journée professionnelle en PVP du 6 octobre 2021. L'analyse des dispositions et enjeux d'application de la Loi 22 a été réalisée, pour et au nom de l'AAPI, par M^e^ Marie-Claude Daraiche, avocate, responsable de l'ADPRP, Direction du Bureau de la sous-ministre et du Secrétariat général, ministère de la Justice. L'AAPI la remercie !

L'IMPLICATION DU RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (PRP)

Le Secrétariat du Conseil du trésor encadrera éventuellement les nouvelles responsabilités qui découlent des modifications législatives apportées dans la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03, ci-après nommée « LGGRI »). D'ici là, il est recommandé de mener une réflexion relative à ces responsabilités. Il faut notamment cibler les éléments du cadre normatif interne susceptible d'être mis à jour, d'identifier tous les actifs informationnels détenus et de cibler les banques de données susceptibles d'être des sources officielles de données numériques gouvernementales.

Responsabilités du responsable de la PRP

D'abord, rappelons que le responsable de la protection des renseignements personnels a les fonctions suivantes :

Fonctions légales	Fonctions administratives
• **Traiter les demandes d'accès aux renseignements personnels** • **Enregistrer certaines communications de renseignements personnels** o article 60 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, ci-après nommée « LAI ») • **Tenir un registre des communications en vue de prévenir un acte de violence**	• **Voir au respect qui incombe à l'organisme public en matière de PRP, dont :** o mettre en place les mesures* nécessaires pour permettre aux personnes d'exercer leurs droits d'accès et de rectification o classer les documents o diffuser systématiquement des documents ou renseignements dans un site Internet o mettre en place des mesures afin d'assurer la PRP o mettre en œuvre des mesures de gouvernance • **Sensibiliser le personnel en matière de PRP** • **Conseiller le personnel en matière de PRP**

Les principales mesures sont :

- ne recueillir que les renseignements personnels nécessaires à ses attributions (art. 64) et les recueillir de manière organisée et transparente (art. 65);
- prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support (art. 63.1);
- mettre en œuvre les mesures de protection des renseignements personnels édictées par règlement du gouvernement (art. 63.2);
- tenir les renseignements personnels à jour, complets et exacts, surtout au moment de leur utilisation (art. 72);
- verser dans un fichier de renseignements personnels tout renseignement personnel qui :
  - soit, est identifié ou se présente de façon à être retrouvé par référence au nom d'une personne ou à un signe ou symbole propre à celle-ci, ou
  - soit, lui a servi ou est destiné à lui servir pour une décision concernant une personne (art. 71);
  - en maintenir l'inventaire (art. 76).
- mettre en place les mesures nécessaires afin que seuls les employés ayant la qualité requise puissent accéder et utiliser les renseignements personnels, et ce, uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions (art. 62);
- n'utiliser les renseignements personnels qu'aux fins auxquelles ils ont été recueillis ou à une autre fin avec le consentement de la personne concernée ou sans son consentement lorsque cette autre utilisation est à des fins compatibles avec celles pour lesquelles ils ont été recueillis ou manifestement au bénéfice de la personne concernée ou nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi (art. 65.1);
- ne communiquer les renseignements personnels qu'avec le consentement de la personne concernée ou lorsque la loi l'autorise expressément (art. 53, 59, 59.1, 60.1, 66, 125 et 171);
- prendre une directive sur la communication de renseignements personnels en vue de prévenir un acte de violence (art. 59.1);
- s'assurer de la validité d'un consentement avant de communiquer les renseignements, c.-à-d. qu'il est manifeste, libre, éclairé, spécifique et limité dans le temps (art. 53);
- s'assurer, avant de communiquer des renseignements personnels à l'extérieur du Québec ou de confier à une personne ou un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, que ces renseignements bénéficieront d'une protection équivalant à celle prévue à la Loi sur l'accès (art. 70.1);
- conclure les ententes de communication de renseignements personnels requises par la loi, le cas échéant, et les faire approuver par la CAI ou le gouvernement (art. 68, 68.1 et 70);
- confectionner et tenir à jour un registre des communications (art. 67.3 et 67.4), des ententes de collecte de renseignements personnels (art. 64 par. 3) et de l'utilisation de renseignements personnels à d'autres fins (art. 65.1 par. 1 à 3);
- détruire les renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis ou utilisés sont atteintes, sous réserve des délais prévus au calendrier de conservation ou au *Code des professions* (art. 73) en utilisant des moyens sûrs préservant leur confidentialité (art. 63.1).

Sécurité de l'information (articles 12.2 à 12.7 LGGRI)

Comme énoncé dans la présentation PowerPoint, le Dirigeant principal de l'information et les Dirigeants de l'information doivent formuler des règles en matière de sécurité de l'information et surveiller la mise en œuvre de celles-ci. Cela requiert de s'organiser, mais aussi de prévoir des mécanismes de reddition de comptes et des indicateurs qui permettront d'évaluer la performance des organismes.

Non seulement les règles (politiques, directives, etc.) émises par le SCT en matière de ressources informationnelles, ce qui inclut la sécurité de l'information, seront probablement mises à jour, mais il y aura des « indications d'application » fournies par le Dirigeant principal de l'information. Les Dirigeants de l'information, quant à eux, devront mettre en place un processus de gestion des risques ainsi qu'un processus de gestion des incidents de sécurité si ce n'est déjà fait. Gérer les ressources informationnelles inclut forcément la gestion des renseignements personnels, donc les responsables de la PRP sont des acteurs clés.

Pistes de réflexion

Le responsable de la PRP doit participer à l'élaboration du cadre de gouvernance en matière de RI ou à sa mise à jour, et ce, afin de s'assurer que la PRP soit ou continue d'être prise en compte.

- Est-ce que le responsable de la PRP siégera sur plus de comités menés par les équipes responsables des ressources informationnelles?
- Est-ce que le responsable de la PRP devra être davantage consulté ou approuver des biens livrables?
- Est-ce que le responsable de la PRP devra participer à la reddition de comptes en matière de ressources informationnelles?
- Est-ce que le responsable de la PRP devra participer davantage au développement des outils mis en place pour respecter les règles qui seront émises par le Secrétariat du Conseil du Trésor?

Le responsable de la PRP doit également s'assurer que les règles en matière de ressources informationnelles, incluant la sécurité de l'information, permettent d'assurer la PRP.

- Est-ce que le bon niveau de sécurité est appliqué pour protéger les renseignements personnels qui sont parfois sensibles?
- Est-ce que les droits d'accès aux renseignements personnels sont octroyés selon la nécessité pour les employés d'y avoir accès afin d'accomplir leur travail?
- Est-ce que les environnements numériques sont classés de façon à permettre aux citoyens d'exercer leur droit d'accès aux renseignements personnels et de rectification?
- Est-ce que les environnements numériques contiennent des renseignements personnels? Sont-ils à jour?
- Est-ce que les renseignements personnels contenus dans les environnements numériques sont utilisés uniquement pour les finalités connues et justifiées?
- Est-ce que les renseignements personnels contenus dans les environnements numériques sont transmis à des tiers?

De plus, ces nouvelles dispositions permettent aux organismes publics, lorsqu'il y a une atteinte à la confidentialité, à la disponibilité ou à l'intégrité d'une ressource informationnelle, de communiquer des renseignements, dont des renseignements personnels, à un autre organisme public ou au Dirigeant principal de l'information (articles 12.2 et 12.3 LGGRI). Aussi, le président du Conseil du Trésor pourra utiliser tous les renseignements concernant un incident pour soutenir les organismes publics concernés. Il pourra aussi conclure des ententes avec toute personne ou des organismes au Canada ou à l'étranger lorsque cela s'avère nécessaire pour assurer la sécurité des données.

- Est-ce que le responsable de la PRP doit inscrire ces communications dans les registres prévus à l'article 67.3 LAI?
- Est-ce que ces communications sont prévues dans les processus de gestion des incidents de l'organisme public?
- Est-ce que des moyens sécuritaires de transmettre les renseignements personnels sont prédéterminés?
- Est-ce seulement la responsabilité du Secrétariat du Conseil du Trésor de s'assurer que les exigences de l'article 70.1 LAI sont respectées s'il y a entente avec un organisme à l'étranger ?
    - Éventuellement, il faudra tenir compte des modifications apportées à l'article 70.1 par le Projet de loi no 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.

Données numériques gouvernementales (articles 12.10 à 12.19 LGGRI)

Cette nouvelle activité, qui est de désigner les sources officielles de données numériques gouvernementales, implique des collectes et/ou des communications de renseignements, incluant les renseignements personnels, entre organismes publics. Les organismes publics sont autorisés à partager les renseignements qu'ils détiennent. Cela dit, plusieurs conditions et obligations sont prévues et le responsable de la PRP doit être impliqué.

Pistes de réflexion

D'abord, le critère de nécessité demeure un élément important à considérer.

- Est-ce que le responsable de la PRP participera à l'évaluation de la nécessité lorsque des renseignements personnels sont impliqués, et ce, afin de s'assurer que l'atteinte à la vie privée soit ou continue d'être minimale?

Aussi, le responsable de la PRP peut se demander :

- Est-ce que le nombre de demandes d'accès à des renseignements personnels augmentera si l'organisme public devient une source officielle de données numériques gouvernementales?
- Est-ce que toutes les communications faites devront être inscrites dans les registres prévus à l'article 67.3 LAI?
- Si l'organisme public collecte désormais les renseignements personnels auprès d'une source officielle plutôt qu'auprès des citoyens, quels processus devront être modifiés?
  - Est-ce que des ententes de communications deviendront caduques?
  - Dans le mémoire accompagnant le projet de loi nº 95, il est indiqué que les communications désormais permises en vertu de la LGGRI se basent sur l'article 67 LAI. En principe, il n'y a pas d'obligation de faire une entente, mais est-ce qu'une entente dite « administrative » continuera d'être nécessaire pour établir les responsabilités de chaque organisme impliqué et les façons de faire?
- Est-ce que devenir une source officielle implique de gérer un plus grand volume de données? Si oui, est-ce qu'il faut changer les processus en place (façon de communiquer, type de fichier, systèmes d'information, etc.)?
  - Est-ce que devenir une source officielle implique de revoir la catégorisation des actifs informationnels (qu'est-ce que je détiens?, pourquoi?, niveau de sensibilité, etc.)?
  - Est-ce que devenir une source officielle expose davantage l'organisme public aux cyberattaques?
- Est-ce que l'évaluation des risques organisationnels doit être mise à jour?
  - Est-ce que l'inventaire des fichiers de renseignements personnels doit être mis à jour?
  - Comment fonctionnera la mise à jour des données numériques gouvernementales?
- Est-ce que l'organisme public devant communiquer des renseignements incluant des renseignements personnels à la source officielle devra participer?
- Est-ce les organismes publics agissant à titre de sources officielles auront l'obligation de détenir des renseignements personnels à jour, exacts et complets (article 72 LAI)?
  - Le responsable de la PRP participera-t-il à l'évaluation des facteurs relatifs à la vie privée?
  - Le responsable de la PRP sera-t-il interpellé si l'organisme reçoit un mandat en matière de données ouvertes, notamment pour identifier les risques possibles sur la vie privée des gens dans le cas où des renseignements personnels sont impliqués (article 12.18 LGGRI)?

- Est-ce que devenir une source officielle implique de sensibiliser les employés qui participeront à la gestion des données et à la production des biens livrables (par exemple, produire le rapport pour la Commission d'accès à l'information)?
- Ils doivent connaître les obligations et la portée des nouvelles responsabilités.
    - Est-ce que devenir une source officielle implique de veiller davantage à ce que les renseignements personnels soient utilisés uniquement pour les fins déterminées?
    - Est-ce que devenir une source officielle implique de revoir le calendrier de conservation?

IMPORTANT – L'arrimage avec les dispositions de la Loi 25 (L.Q. 2021, c. 25), Loi modernisant des dispositions législatives en matière de protection des renseignements personnels qui sont entrées en vigueur le 22 septembre 2021 devient nécessaire.

www.aapi.qc.ca