cyber eco

Guide Pratique : Application de la loi 25

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Mai 2022

Table des matières

Partie 1

Explication de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25)

1. Objectifs principaux de la Loi

La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels va apporter des modifications importantes aux lois sur la protection des renseignements personnels. Cette loi a pour objectif d'offrir un meilleur contrôle aux citoyens sur leurs renseignements personnels. Elle modernise le cadre législatif pour l'adapter à la réalité technologique d'aujourd'hui. Pour ce faire, plusieurs éléments déjà contenus au régime européen sont maintenant transposés à l'environnement québécois. L'adoption de cette loi fait d'ailleurs du Québec un précurseur au niveau de l'encadrement des technologies et de protection des renseignements personnels, car il s'agit de la première province du Canada à entreprendre une réforme de sa législation.

Sanctionnée en septembre 2021, cette loi entrera graduellement en vigueur, soit en trois phases. Ainsi, certaines dispositions entreront en vigueur le 22 septembre 2022, d'autres le 22 septembre 2023, puis les dernières le 22 septembre 2024. C'est d'ailleurs suivant ces différentes dates d'entrée en vigueur que le présent document est subdivisé, afin d'en faciliter la consultation.

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

1. 22 septembre 2022

1. Conformité et gouvernance

1. Désignation d'un responsable de la protection des renseignements personnels

Article 3.1 de la Loi sur la protection des renseignements personnels dans le secteur privé

La personne ayant la plus haute autorité de l'organisation devra veiller à assurer le respect et la mise en œuvre de la Loi. Cette personne exercera la fonction de « responsable de la protection des renseignements personnels ». Cependant, cette fonction pourra être déléguée par écrit, en tout ou en partie, à toute personne.

Le titre et les coordonnées du responsable devront être publiés sur le site web de l'entreprise ou, si elle n'a pas de site web, rendus accessibles par tout autre moyen approprié.

2. Obligations

1. Notification et consignation des incidents de confidentialité

Articles 3.5 à 3.8 de la Loi sur la protection des renseignements personnels dans le secteur privé

Un registre de tout incident de confidentialité devra également être tenu. Celui -ci devra être communiqué à la Commission d'accès à l'information (ci-après «CAI») sur demande.

À titre d'exemples, ces différentes situations pourraient, entre autres, se qualifier d'incidents de confidentialité :

a) l'accès non autorisé par la loi à un renseignement personnel;
b) l'utilisation non autorisée par la loi d'un renseignement personnel;
c) la communication non autorisée par la loi d'un renseignement personnel; ou
d) la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Au surplus, les organisations devront aviser la CAI **ET** les personnes concernées de tout incident de confidentialité si celui-ci implique un renseignement personnel qu'elles détiennent **ET** présente un risque de préjudice sérieux. À titre d'exemples, un préjudice sérieux pourrait être une atteinte à la réputation, une atteinte au dossier de crédit, un vol d'identité, etc.

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

2. 22 septembre 2023

1. Conformité et gouvernance

1. Adopter ou mettre à jour des politiques et des pratiques encadrant la gouvernance des renseignements personnels

   Article 3.2 de la Loi sur la protection des renseignements personnels dans le secteur privé

   Les entreprises devront établir et mettre en œuvre des politiques et des pratiques encadrant leur gouvernance à l'égard des renseignements personnels. Ces politiques doivent être proportionnées à la nature et à l'importance des activités de l'entreprise. Elles devront être rédigées en termes simples et clairs.

2. Prévoir l'encadrement applicable à la conservation, la destruction et l'anonymisation des renseignements personnels

   Article 3.2 de la Loi sur la protection des renseignements personnels dans le secteur privé

   Des règles permettant d'encadrer à la conservation et à la destruction des renseignements personnels devront être prévues aux politiques et pratiques. Des informations sur ces règles devront être exposées en termes simples et clairs et publiées au site internet de l'organisation (ou rendues autrement disponibles).

3. Se munir d'un processus de traitement des plaintes

   Article 3.2 de la Loi sur la protection des renseignements personnels dans le secteur privé

   Un processus de traitement des plaintes relatives à la protection des renseignements personnels devra être prévu aux politiques et pratiques. Ce processus devra être exposé en termes simples et clairs et publié au site web de l'organisation (ou rendu autrement disponible).

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

2. 22 septembre 2023

2. Obligations

1. Publication d'informations concernant les politiques et procédures sur le site web

   Article 3.2 de la Loi sur la protection des renseignements personnels dans le secteur privé

   Des informations portant sur les politiques, procédures et pratiques encadrant la gouvernance des renseignements personnels mises en place par l'entreprise devront être publiées sur son site web. Si elles n'ont pas de site web, les entreprises devront rendre accessible cette information par tout autre moyen approprié.

   Cela permet d'assurer la transparence des entreprises concernant les politiques et procédures qu'elles ont adoptées.

2. Réalisation d'Évaluations de Facteurs relatifs à la Vie Privée (EFVP) pour certains traitements de renseignements personnels

   Article 3.3 de la Loi sur la protection des renseignements personnels dans le secteur privé

   Pour tout nouveau projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services qui implique la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels, les entreprises devront réaliser une EFVP. L'EFVP devra être proportionnelle à la sensibilité des renseignements touchés par le projet, la finalité de leur utilisation, leur quantité, leur répartition et leur support. Tous ces éléments devront être pris en compte dans l'EFVP. D'ailleurs, il faudra consulter la personne responsable de la protection des renseignements personnels au sein de l'entreprise dès le début du projet. Cette personne pourra suggérer des mesures de protection des renseignements personnels à mettre en place dans la réalisation du projet en question.

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

2. 22 septembre 2023

2. Obligations

3. Modification des paramètres du consentement

Articles 4 et suivants de la Loi sur la protection des renseignements personnels dans le secteur privé

Le consentement est toujours exigé pour recueillir, détenir, utiliser ou communiquer des renseignements personnels. Il doit être manifeste, libre, éclairé et être donné à des fins spécifiques. L'exigence du consentement sera toutefois renforcée puisqu'il devra être demandé pour chacune de ces fins, en termes simples et clairs, et de façon distincte de toute autre information communiquée à la personne concernée.

De plus, lorsqu'une entreprise souhaite utiliser ou communiquer un renseignement personnel sensible, le consentement doit être manifesté de façon expresse. Cela implique que la personne pose un geste pour confirmer son consentement, par exemple en cochant une case. Un renseignement personnel est qualifié de sensible lorsqu'un haut degré d'attente raisonnable en matière de vie privée lui est lié, tels un numéro d'assurance social ou des informations médicales.

4. Destruction et anonymisation de renseignements personnels

Article 23 de la Loi sur la protection des renseignements personnels dans le secteur privé

Lorsque l'entreprise aura atteint les fins pour lesquelles elle a collecté des renseignements personnels auprès d'une personne concernée, deux choix s'offriront désormais à elle. Le premier est la destruction de ces renseignements personnels. Le second est l'anonymisation des renseignements personnels. Toutefois, l'anonymisation devra être faite dans l'objectif d'utiliser les renseignements anonymisés pour des fins sérieuses et légitimes. Ce choix ne pourra donc pas être fait sans raison le justifiant.

Il est important de préciser que pour qu'un renseignement personnel soit considéré comme anonymisé au sens de la loi, il ne doit plus permettre d'identifier directement ou indirectement une personne physique, et ce, de manière irréversible. Cette anonymisation devra être réalisée selon les meilleures pratiques généralement reconnues et selon des critères qui seront déterminés par règlement.

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

2. 22 septembre 2023

2. Obligations

5. Transfert de renseignements personnels à l'extérieur du Québec

Article 17 de la Loi sur la protection des renseignements personnels dans le secteur privé

Avant de communiquer des renseignements personnels à l'extérieur du Québec, les entreprises devront réaliser une EFVP qui devra prendre en considération les éléments suivants :

1) la sensibilité des renseignements personnels;
2) la finalité de leur utilisation;
3) les mesures de protection associées aux renseignements personnels faisant l'objet de la communication;
4) le régime juridique applicable à l'endroit où les renseignements personnels sont communiqués, plus précisément les principes de protection des renseignements personnels qui s'appliquent.

Une fois ces éléments évalués, les renseignements personnels pourront être communiqués si l'évaluation démontre que les renseignements bénéficieraient d'une protection qui est adéquate en fonction des principes de protection des renseignements personnels généralement reconnus. La communication devra également faire l'objet d'une entente écrite faisant état des conclusions de l'EFVP et, si nécessaire, des modalités convenues afin d'atténuer les risques identifiés dans l'EFVP.

Ces obligations seront également applicables lorsqu'une entreprise souhaite déléguer la tâche de recueillir, d'utiliser, de communiquer ou de conserver à sa place des renseignements personnels à une personne ou un organisme se trouvant hors du Québec.

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

2. 22 septembre 2023

2. Obligations

6. Mise en place d'un processus de destruction ou d'anonymisation, afin de mettre en œuvre la désindexation

Article 28.1 de la Loi sur la protection des renseignements personnels dans le secteur privé

Le droit à la désindexation permet à une personne de demander à une entreprise d'arrêter la diffusion d'un ou plusieurs de ses renseignements personnels ou que soit désindexé tout hyperlien rattaché à son nom qui permet d'accéder à ce renseignement. Cette demande peut être faite lorsque la diffusion du renseignement en question contrevient à la loi ou à une ordonnance judiciaire.

La personne peut également le demander lorsque toutes ces conditions sont réunies :

1) la diffusion du renseignement lui cause un préjudice grave en lien avec son droit au respect de sa réputation ou de sa vie privée;
2) ce préjudice est manifestement supérieur à l'intérêt du public d'accéder à ce renseignement ou à l'intérêt de toute personne de s'exprimer librement; et
3) les actions pour la cessation de la diffusion, la réindexation ou la désindexation demandée n'excède pas les mesures nécessaires pour que le préjudice cesse.

Pour valider si toutes les conditions sont réunies, l'entreprise tiendra compte des éléments suivants :

1) si la personne concernée est une personnalité publique;
2) si le renseignement concerne la personne alors qu'elle est mineure;
3) si le renseignement est à jour et exact;
4) la sensibilité du renseignement;
5) le contexte de la diffusion du renseignement;
6) le délai écoulé entre la diffusion du renseignement et la demande de la personne concernée; et
7) si le renseignement concerne une procédure criminelle ou pénale, de l'obtention d'un pardon ou de l'application d'une restriction à l'accessibilité des registres des tribunaux judiciaires.

Lorsqu'une telle demande est acceptée, le responsable de la protection des renseignements personnels devra attester, dans une réponse écrite, que le renseignement personnel en question n'est plus diffusé, que l'hyperlien est désindexé ou réindexé.

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

2. 22 septembre 2023

3. Sanctions

Articles 90.1 et suivants de la Loi sur la protection des renseignements personnels dans le secteur privé

Les entreprises qui ne se conformeront pas aux obligations prévues par la loi pourront se voir imposer différents types de sanctions.

1) **Sanctions administratives pécuniaires (SAP):**
   La Commission d'accès à l'information pourra imposer des SAP d'un montant maximal de 10 000 000$ ou de 2% du chiffre d'affaires mondial de l'entreprise.
2) **Sanctions pénales :**
   La Commission d'accès à l'information pourra également intenter des poursuites pénales. Ainsi, la Cour du Québec pourra imposer une amende d'un montant maximal de 25 000 000$ ou de 4% du chiffre d'affaires mondial de l'entreprise.
3) **Dommages-intérêts punitifs :**
   Les individus auront également un droit privé d'action envers les entreprises qui leur permettra de réclamer des dommages-intérêts punitifs lors d'une atteinte intentionnelle ou résultant d'une faute lourde.

2. Nouvelles obligations pour le secteur privé et leur entrée en vigueur

3. 22 septembre 2024

1. Obligations

1. Implanter des mesures facilitant le droit à la portabilité des données

Article 27 de la Loi sur la protection des renseignements personnels dans le secteur privé

Le droit à la portabilité des données permet à une personne d'obtenir une copie des renseignements personnels qu'une organisation détient à son sujet dans un format intelligible. Dans certains cas, ce droit permet également à la personne de demander le transfert de ses renseignements personnels d'une organisation à l'autre. L'un des objectifs principaux de ce droit est de permettre aux individus d'avoir plus de contrôle sur leurs renseignements personnels.

La loi prévoit que l'entreprise qui détient un renseignement personnel sur une personne devra, à sa demande, lui en confirmer l'existence et lui communiquer ce renseignement, tout en lui permettant d'en obtenir une copie. Cela s'applique pour un renseignement personnel informatisé. Il devra lui être communiqué sur demande dans un format technologique structuré et couramment utilisé. Enfin, ce renseignement devra être communiqué, toujours à sa demande, à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement.

Partie 2

Loi 25 - Plan d’actions suggéré

Loi 25 - Plan d'actions suggéré
2022 à 2024

À compléter pour **septembre 2022**

1. Désigner un responsable de la protection des renseignements personnels
2. Créer ou mettre à jour les politiques et les pratiques encadrant la gouvernance des renseignements personnels
3. Mettre en place un registre des incidents de confidentialité et un processus de notification
4. Avoir un inventaire des renseignements personnels de l'entreprise
5. Mettre en place un programme de formation sur la protection des renseignements personnels

À compléter pour **septembre 2023**

6. Mettre à jour les politiques et les pratiques encadrant la conservation, la destruction et l'anonymisation des renseignements personnels
7. Mettre en place un processus de traitement des plaintes relatives à la protection des renseignements personnels
8. Publier les éléments clés des règles de gouvernance encadrant la protection des renseignements personnels sur le site Web de l'entreprise
9. Mettre en place un politique et un processus d'évaluation des facteurs relatifs à la vie privée (EFVP) pour le traitement des renseignements personnels
10. Mettre en place un processus de cueillette du consentement pour recueillir, détenir, utiliser ou communiquer des renseignements personnels
11. Mettre en place un processus de désindexation

À compléter pour **septembre 2024**

12. Implanter des mesures facilitant le droit à la portabilité des données

Actions à compléter pour
Septembre 2022

1. Désigner un responsable de la protection des renseignements personnels
2. Créer ou mettre à jour les politiques et les pratiques encadrant la gouvernance des renseignements personnels
3. Mettre en place un registre des incidents de confidentialité et un processus de notification
4. Avoir un inventaire des renseignements personnels de l'entreprise
5. Mettre en place un programme de formation sur la protection des renseignements personnels

Désigner un responsable de la protection des renseignements personnels

Information chronologique

- **Requis le 22 septembre 2022 selon 2.1.1.1**
- **Prédécesseur :** Aucun, première activité à réaliser pour septembre 2022
- **Successeurs :** Créer ou mettre à jour les politiques et les pratiques encadrant la gouvernance des renseignements personnels et avoir un inventaire des renseignements personnels de l'entreprise

Sommaire

Le responsable de la protection des renseignements personnels est la pierre angulaire de votre programme. C'est la personne qui a la plus haute autorité de l'organisation et elle devra veiller à assurer le respect et la mise en œuvre de la Loi. Certaines tâches peuvent être déléguées, mais la responsabilité demeure toujours sous le responsable.

Activités clés

- Décrire les rôles et responsabilités de la personne responsable
- Déterminer de qui relèvera la personne responsable dans l'organisation
- Désigner les critères d'embauche pour la personne responsable
- Assurer la formation de la personne responsable
- Définir / modifier le modèle de gouvernance en fonction des rôles et responsabilités
- Publier les coordonnées de la personne responsable publiquement (ex. site web)

Désigner un responsable de la protection des renseignements personnels

Facteurs de planification

Cette phase requiert potentiellement un processus d'embauche et il faut donc prévoir suffisamment de temps pour cette activité surtout si la personne n'est pas déjà dans l'organisation. La formation peut également prendre un certain temps en fonction de l'écart de compétences entre la personne retenue et les compétences requises pour le poste.

Astuce

Cette première action est critique et est un prérequis à toutes les autres actions qui suivent. On ne saurait trop insister sur l'importance de compléter le tout sans délai.

Ressources disponibles

- https://www.caij.qc.ca/dossier/projet-de-loi-n-64-loi-modernisant-des-dispositions-legislatives-en-matiere-de-protection-des-renseignements-personnels
- https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/responsable-protection-renseignements-personnels

Créer ou mettre à jour les politiques et les pratiques encadrant la gouvernance des renseignements personnels

Information chronologique

- **Requis le 22 septembre 2023 selon 2.2.1.2**
- **Prédécesseur :** Désigner un responsable de la protection des renseignements personnels
- **Successeur :** Mettre en place un registre des incidents de confidentialité et un processus de notification

Sommaire

Les politiques et les pratiques encadrant la gouvernance des renseignements personnels sont des éléments critiques pour permettre une saine gestion des renseignements personnels. Cette activité, bien que requise seulement le 22 septembre 2023 dans la loi, doit être réalisée dès 2022 car ses extrants auront un impact sur les prochaines activités à réaliser pour septembre 2022.

Activités clés

- La personne responsable de la protection des renseignements personnels est la personne en charge de s'assurer de la mise en œuvre des politiques et des pratiques.
- Élaborer et mettre à jour les politiques et pratiques pour répondre aux questions suivantes :
  - Quelles informations sont collectées, conservées, communiquées et détruites?
  - Quel est le processus de rétention des données?
  - Quels sont les raisons, principaux facteurs et paramètres encadrant la prise de décisions fondées exclusivement sur un traitement automatisé de renseignements personnels? Qui a accès aux données?
  - Quel est le processus de destruction?
  - Qu'est-ce qui constitue un incident de confidentialité?
  - Quelle est la procédure de traitement d'un incident de confidentialité?
  - Qui sera avisé d'un incident (interne/externe)?
  - Quels sont les délais de notification pour les incidents?

Créer ou mettre à jour les politiques et les pratiques encadrant la gouvernance des renseignements personnels

Facteurs de planification

À initier dès que la personne responsable de la protection des renseignements personnels est embauchée.

Astuce

- Si l'entreprise n'a pas déjà mis en place des politiques et pratiques sur les renseignements personnels ou un inventaire, il faut prévoir des efforts plus importants pour les produire que de simplement mettre à jour des politiques existantes.
- Utiliser des gabarits simples de politiques et pratiques, alignés avec les autres politiques et pratiques de l'organisation.

Ressources disponibles

- https://www.priv.gc.ca/fr/protection-de-la-vie-privee-et-transparence-au-commissariat/pp/
- https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/politiques-pratiques-gouvernance/
- https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf?1637173195

Mettre en place un registre des incidents de confidentialité et un processus de notification

Information chronologique

- ***Requis le 22 septembre 2022 selon 2.1.2.1***
- **Prédécesseur :** Créer ou mettre à jour les politiques et les pratiques encadrant la gouvernance des renseignements personnels
- **Successeur :** Inventorier les renseignements personnels de l'entreprise

Sommaire

À compter du 22 septembre 2022, les organisations devront aviser la Commission d'accès à l'information et les personnes concernées de tout incident de confidentialité impliquant un renseignement personnel qu'elles détiennent et présentant un risque de préjudice sérieux.

Les organisations devront également tenir un registre des incidents de confidentialité qui devra être communiqué à la Commission sur demande.

Activités clés

- Mettre en place un registre pour capturer les détails des incidents de confidentialité.
- Mettre en place un registre des notifications en lien avec l'incident.
- Mettre en place un processus de mise à jour des registres.

Mettre en place un registre des incidents de confidentialité et un processus de notification

Facteurs de planification

Débuter la planification même si toutes les politiques et pratiques ne sont pas finalisées à 100%. Le requis d'avoir le tout en place pour septembre 2022 suggère de faire du parallélisme dans les activités dans la mesure du possible.

Astuce

- Avec l'aide de votre équipe légale et de votre responsable de la protection de renseignements personnels, effectuez l'analyse de l'existence d'un risque de préjudice sérieux pour connaître vos obligations légales de notification.
- Prendre connaissance d'exemples de registres disponibles sur le Web et en intégrant au processus de gestion des incidents existant.
- Mettre l'importance sur l'identification adéquate du niveau de sévérité d'un incident afin de déterminer si de l'aide externe sera nécessaire.
- Utiliser un gabarit simple de tableau / chiffrier qui rencontre les requis au sens de la loi.

Ressources disponibles

- https://www.cai.gouv.qc.ca/incident-de-securite-impliquant-des-renseignements-personnels/
- https://cybereco.ca/wp-content/uploads/2021/10/guide-de-gestion-des-incidents-pmes-pdf.pdf
- https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/incident-de-confidentialite

Avoir un inventaire des renseignements personnels de l'entreprise

Information chronologique

- ***Recommandé en lien avec l'opérationnalisation de la protection des renseignements personnels***
- **Prédécesseur :** Désigner un responsable de la protection des renseignements personnels.
- **Successeur :** Mettre en place un programme de formation sur la protection des renseignements personnels.

Sommaire

Ceci est requis afin d'une part avoir un inventaire des renseignements personnels de l'entreprise et d'autre part assurer que le registre des incidents de confidentialité tient compte de tous les renseignements personnels qui doivent être gardés confidentiels.

Activités clés

- Dresser un inventaire des renseignements personnels dans les systèmes TI et les différentes sources d'information de l'entreprise incluant ce qui est imparti:
  - Où sont les renseignements personnels?
  - Quels types d'informations sont stockés?
  - Quelles sont les informations collectées?
- Contrôler l'accès et le transfert des renseignements personnels en lien avec les politiques de l'entreprise:
  - Qui a accès aux renseignements personnels? Dans quel contexte?
  - Est-ce que les politiques de l'entreprise sont suivies?
  - Quels sont les renseignements personnels transférés vers des tiers?
- Être en mesure d'identifier le lien entre les renseignements personnels et les personnes concernées:
  - Si un incident survient; savons-nous quelles données sont impliquées et qui nous devrons notifier?

Avoir un inventaire des renseignements personnels de l'entreprise

Facteurs de planification

Cette activité peut être faite en parallèle à l'activité précédente (registre des incidents de confidentialité).

Astuce

- Il faut s'assurer d'avoir fait un inventaire complet, car il faudra par la suite s'en servir pour les activités requises pour septembre 2023 et en particulier pour les activités qui touchent les systèmes d'information.
- Il sera beaucoup moins coûteux d'éliminer dès que possible l'information non requise aux processus de l'entreprise que d'avoir à s'assurer de leur conformité.
- Prévoir un processus de mise à jour en continu (lors d'ajouts ou de modifications d'applications) et de révision annuelle.
- L'information et les endroits où elle est conservée doit être documenté.
- Ne pas hésiter à changer les pratiques lorsque de l'information hautement confidentielle est conservée dans un endroit inapproprié (ex. serveur, ordinateur portable).
- S'assurer qu'on collecte, utiliser et conserve seulement ce qui est requis (et pas plus).
- Avoir des solutions technologiques en place pour rendre l'inventaire des renseignements personnels le plus simple et efficace possible.

Ressources disponibles

- https://www.cai.gouv.qc.ca/diffusion-de-linformation/inventaire-des-fichiers-de-renseignements-personnels/
- https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/securite-des-renseignements-personnels/gd_rd_201406/

Mettre en place un programme de formation sur la protection des renseignements personnels

Information chronologique

- ***Recommandé en lien avec l'opérationnalisation de la protection des renseignements personnels***
- **Prédécesseur :** Avoir un inventaire des renseignements personnels de l'entreprise
- **Successeur :** Voir les activités pour septembre 2023

Sommaire

Cette activité sert à s'assurer que tout le personnel a reçu la formation requise afin de satisfaire les exigences de la 25 au sein de votre entreprise.

Activités clés

- Créer une présentation qui explique de manière simple et claire les changements en lien avec la protection des renseignements personnels et qui identifie les rôles et responsabilités du personnel tout au long du cycle de vie des renseignements personnels.
- Présenter les politiques et pratiques de l'entreprise aux employés suivant un calendrier de formation.
- S'assurer d'une mise à jour de la formation.
- Prévoir des formations plus spécifiques pour les employés qui joueront un rôle de premier plan dans la mise en œuvre du programme de protection des renseignements personnels de l'entreprise.
- S'assurer que les politiques et pratiques sont suivies par les employés et documenter les lacunes. Ajuster le plan de formation afin de remédier aux lacunes identifiées dans les comportements des employés.
- Notifier et réentraîner les employés qui ne respectent pas les obligations prévues aux politiques.

Mettre en place un programme de formation sur la protection des renseignements personnels (PRP)

Facteurs de planification

Il y a un effort pour assurer la production du matériel de formation. Il faut penser au type de session qui dépendra de l'audience à qui on s'adresse.

Astuce

- Utiliser un langage simple, standardisé à l'entreprise.
- Démontrer en quoi la PRP n'alourdit pas la tâche, les conséquences d'un incident et l'importance de se conformer à la politique de l'entreprise.
- Il est possible de former des personnes de référence qui formeront à leur tour des groupes afin de couvrir l'ensemble de l'entreprise.
- Utiliser des ressources existantes:
  - La Cybertrousse de Cybereco peut être utilisée pour certains aspects de sensibilisation.
  - Certains membres de Cybereco rendent disponibles des artefacts qui pourraient vous aider dans vos activités de sensibilisation.

Ressources disponibles

- Cybertrousse de Cybereco: https://cybereco.ca/cybertrousse/
- Conservation et retrait des renseignements personnels: https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/protection-des-renseignements-personnels-pour-les-entreprises/mesures-de-securite-et-atteintes/securite-des-renseignements-personnels/gd_rd_201406/

Actions à compléter pour
Septembre 2023

6. Mettre à jour les politiques et les pratiques encadrant la conservation, la destruction et l'anonymisation des renseignements personnels
7. Mettre en place un processus de traitement des plaintes relatives à la protection des renseignements personnels
8. Publier les éléments clés des règles de gouvernance encadrant la protection des renseignements personnels sur le site Web de l'entreprise
9. Mettre en place un politique et un processus d'évaluation des Facteurs relatifs à la vie privée (EFVP) pour le traitement des renseignements personnels
10. Mettre en place un processus de cueillette du consentement pour recueillir, détenir, utiliser ou communiquer des renseignements personnels
11. Mettre en place un processus de désindexation

Mettre à jour les politiques et les pratiques encadrant la conservation, la destruction et l'anonymisation des renseignements personnels

Information chronologique

- **Requis selon 2.2.1.2 le 23 septembre 2023**
- **Prédécesseur** : Avoir un inventaire des renseignements personnels de l'entreprise
- **Successeurs** : Mettre en place un processus de désindexation

Sommaire

Cette pratique permet de protéger la vie privée des personnes concernées en leur assurant que leurs renseignements personnels détenus par l'entreprise ne soient plus accessibles ni par l'entreprise ou par un tiers en ayant recours à la destruction ou à l'anonymisation. Elle est déclenchée lorsque les renseignements personnels ne servent plus selon leur finalité initiale et lorsque la période de conservation légalement prescrite est échue.

Activités clés

- S'informer sur les meilleures pratiques existantes, incluant les exigences réglementaires du gouvernement québécois.
- Définir les dispositions de la politique applicable de l'entreprise en matière de conservation et de destruction des renseignements personnels.
- Identifier les outils à implanter dans l'entreprise, idéalement par une personne dont l'expertise est reconnue en la matière.
- En conformité avec le calendrier de conservation déterminé par l'entreprise, établir les pratiques à mettre en place pour les renseignements personnels collectés par l'entreprise, tels qu'identifiés dans l'inventaire.
- Mettre en œuvre les pratiques et vérifier l'atteinte du degré requis d'anonymisation.
- Adapter la politique et les pratiques régulièrement, en tenant compte des variations au niveau des lois, des règlements, des pratiques reconnues et tout autre aspect pertinent.

Mettre à jour les politiques et les pratiques encadrant la conservation, la destruction et l'anonymisation des renseignements personnels

Facteurs de planification

La connaissance des meilleures pratiques en anonymisation et en destruction adéquate des renseignements personnels est une cible qui peut être hors de la portée de l'entreprise. Il serait approprié de faire affaires avec un tier compétent. Que ce soit fait à l'interne ou à l'externe, le facteur temps sera important.

Astuce

- Il est important de bien comprendre ce qu'est l'anonymisation. Pour se qualifier d'anonymisation au sens de la loi, le procédé sélectionné se doit d'être irréversible et ne plus permettre d'identifier directement ou indirectement une personne à son issue.
- Il existe des pratiques d'anonymisation qui existent depuis longtemps. Ces pratiques peuvent reposer sur la cryptographie. La cryptographie utilise souvent des clés, dont la gestion est très sensible.

Ressources disponibles

- Dwork, C. et A. Roth. (2014) The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, Vol. 9, p. 211–407, DOI: 10.1561/0400000042
- ENISA ENISA proposes Best Practices and Techniques for Pseudonymisation, décembre 2019
- NIST IR 8053 De-Identification of Personal Information, octobre 2015
- Dépersonnalisation, anonymisation et désindexation : nouveau jargon, nouvelles obligations! | Ressources | Fasken

Mettre en place un processus de traitement des plaintes relatives à la protection des renseignements personnels

Information chronologique

- **Requis selon 2.2.1.3 le 23 septembre 2023**
- **Prédécesseur :** Mettre à jour les politiques et les pratiques encadrant la collecte, la conservation, l'utilisation, la communication, la destruction et l'anonymisation des renseignements personnels
- **Successeurs :** Publier les politiques et procédures encadrant la gouvernance des renseignements personnels sur le site Web de l'entreprise

Sommaire

Le processus de traitement des plaintes relatives à la protection des renseignements personnels devra se retrouver dans les politiques et pratiques encadrant la gouvernance de l'entreprise en matière de protection des renseignements personnels. Le processus de traitement des plaintes devra être simple et clair et se retrouver sur le site Web de l'entreprise. Les personnes concernées pourront notamment informer l'entreprise d'un traitement inadéquat de leurs renseignements personnels ou des rectifications à y apporter via ce processus.

Activités clés

- Déterminer la stratégie de votre entreprise en matière de traitement des plaintes.
- Identifier qui seront les personnes responsables de répondre aux plaintes des personnes concernées.
- S'assurer que les politiques et pratiques élaborées par l'entreprise prévoient le processus de traitement des plaintes incluant des méthodes d'authentification adéquates pour les personnes qui font des requêtes en personne, au téléphone, par courriel, par le Web, etc.
- Décrire le processus de traitement des plaintes de manière simple et claire pour les personnes concernées.
- Publier le processus sur le site Web de l'entreprise.
- Une fois le processus mis en place, conserver un registre des plaintes et des mesures prises par l'entreprise afin d'y répondre.

Mettre en place un processus de traitement des plaintes relatives à la protection des renseignements personnels

Facteurs de planification

En plus d'élaborer le processus de traitement des plaintes, il faut planifier la manière dont celles-ci seront traitées par votre entreprise. Les personnes qui seront responsables de traiter les plaintes devront donc être formées afin d'être en mesure d'y répondre adéquatement et d'avoir en main les outils nécessaires pour que la situation ayant générée la plainte soit corrigée lorsque nécessaire.

Astuce

- Si votre entreprise a déjà un processus de traitement des plaintes générales ou un service à la clientèle, il est possible d'intégrer le processus de traitement des plaintes relatives à la protection des renseignements personnels à ces derniers. Sinon, il est possible d'utiliser votre outil de suivi des requêtes ou des incidents.
- S'informer sur les différents processus de traitement plaintes en place en matière de protection des renseignements personnels pour des fins d'inspiration.

Ressources disponibles

- Pour dénoncer une pratique ou un comportement suspect | Commission d'accès à l'information du Québec (gouv.qc.ca)
- Déposer une plainte visant une entreprise - Commissariat à la protection de la vie privée du Canada, décembre 2020

Publier les éléments clés des règles de gouvernance encadrant la protection des renseignements personnels sur le site Web de l'entreprise

Information chronologique

- **Requis selon 2.2.2.1 le 23 septembre 2023**
- **Prédécesseur :** Créer ou mettre à jour les politiques et les pratiques encadrant la gouvernance des renseignements personnels
- **Successeurs :** aucun

Sommaire

Les politiques et les pratiques encadrant la gouvernance des renseignements personnels sont des éléments essentiels à une saine gestion de ceux-ci. La publication de ces documents est requise pour le 23 septembre 2023. Cependant, comme ces politiques guident la mise en place de plusieurs autres éléments, leur rédaction (ou révision) est conseillée dès 2022. L'obligation de la publication de l'information sur les politiques et les procédures encadrant la gouvernance des renseignements personnels découle du principe de transparence que doit respecter l'entreprise.

Activités clés

- Élaborer ou mettre à jour les politiques et pratiques pour répondre aux critères de la Loi 25.
- Prévoir une présentation claire, détaillée et dans un langage accessible à tous.tes.
- Publier l'essentiel de ces politiques et pratiques sur le site internet de l'entreprise. Si l'entreprise n'a pas de site internet, elle devra rendre publier l'information au sujet de ses politiques et pratiques par tout autre moyen approprié.
- Tenir à jour l'information publiée.

Publier les éléments clés des règles de gouvernance encadrant la protection des renseignements personnels sur le site Web de l'entreprise

Facteurs de planification

S'assurer d'avoir une politique et des procédures de gouvernance conforment aux exigences règlementaires afin d'en faire ressortir les informations qui sont nécessaires. S'assurer que les informations publiées soient facile d'accès et s'assurer du langage clair en consultant les ressources pertinentes.

Astuce

- La personne responsable de la protection des renseignements personnels de l'entreprise devra s'assurer de la mise à jour des informations publiées. Elle peut obtenir de l'aide de son équipe à cette fin.
- S'assurer de réaliser une divulgation appropriée en consultant vos aviseurs légaux avant la publication des informations sur le site web.

Ressources disponibles

- https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/politiques-pratiques-gouvernance/

Mettre en place un politique et un processus d'évaluation des Facteurs relatifs à la vie privée (EFVP) pour le traitement des renseignements personnels

Information chronologique

- **Requis selon 2.2.2.2 le 23 septembre 2023**
- **Prédécesseur :** Dresser l'inventaire des renseignements personnels de l'entreprise
- **Successeurs :** Mettre en place un processus de traitement des plaintes relatives à la protection des renseignements personnels

Sommaire

La conduite d'une EFVP est une démarche préventive qui consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée. Cette évaluation devrait être menée lors de tout projet d'acquisition, de développement, de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels ou avant la communication de renseignements personnels hors Québec.

Activités clés

- Déterminer les obligations et les principes de protections des renseignements personnels applicables.
- Déterminer la portée de chaque projet impliquant une cueillette, un traitement, une communication ou une conservation de renseignements personnels :
  - Déterminer la nature des renseignements personnels impliqués. En effet, les risques et impacts d'un incident de protection de renseignements personnels sont directement en lien avec la sensibilité des renseignements touchés;
  - Déterminer l'utilisation faite des renseignements personnels (collecte, communication, conservation, destruction, etc.).
- Repérer et décrire les risques sur la vie privée engendrés par le projet et analyser l'impact de ces risques.
- Lorsque possible, déterminer des mesures permettant d'éliminer ou de réduire la probabilité que ces risques surviennent et/ou leur impact.
- S'assurer que les produits et services technologiques offerts au public par l'entreprise qui sont utilisés pour recueillir des renseignements personnels et qui sont dotés de paramètres de confidentialité offrent le plus haut niveau de confidentialité à l'utilisateur.
- Effectuer le suivi de l'EFVP suivant l'évolution du projet.

Mettre en place un politique et un processus d'évaluation des Facteurs relatifs à la vie privée (EFVP) pour le traitement des renseignements personnels

Facteurs de planification

- L'EFVP devrait être conduite au début du projet.
- L'EFVP 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.
- Définir les rôles de chacun afin de faciliter la conduite de l'EFVP dont la cueillette des informations.
- Documenter la démarche par écrit afin d'en conserver des traces.
- Mettre en place un processus permettant de réviser adéquatement l'EFVP afin qu'elle puisse suivre l'évolution du projet et être cohérente.

Astuce

- Il peut être facilitant de préparer un modèle d'EFVP clair et uniforme comportant les bonnes questions à compléter par écrit. De cette façon, il sera facile d'assurer une uniformisation et une cohérence en plus de faciliter une éventuelle démonstration de conformité le cas échéant. Également, il peut être pertinent de documenter les raisons pour lesquelles une EFVP n'a pas été conduite pour un projet donné.
- Aucun système ne devrait être mis en production si les risques de non-conformité à Loi 25 sont importants. Il faut prévoir discuter de ces risques dans la prise de décision visant la mise en production.

Ressources disponibles

- **Guide D'accompagnement (CAI):** https://www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf
- **Évaluations de facteurs relatifs à la vie privée (Commissariat à la protection de la vie privée du Canada):** https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/

Mettre en place un processus de cueillette du consentement pour recueillir, détenir, utiliser ou communiquer des renseignements personnels

Information chronologique

- **Requis selon 2.2.2.3 le 23 septembre 2023**
- **Prédécesseur :** Mettre à jour les politiques et les pratiques encadrant la collecte, la conservation, l'utilisation, la communication, la destruction et l'anonymisation des renseignements personnels
- **Successeurs :** Mettre en place des processus de destruction, d'anonymisation et de désindexation

Sommaire

Bien que le consentement soit déjà exigé pour recueillir, détenir, utiliser ou communiquer des renseignements personnels, il faudra maintenant s'assurer que ce consentement soit demandé et obtenu pour chacune des fins visées par le traitement des renseignements personnels de façon distincte des autres informations communiquées à la personne concernée. Ce consentement sera valide uniquement afin de réaliser les fins communiquées par l'entreprise au moment de la collecte.

Activités clés

- Réviser le processus actuel de l'entreprise en matière de cueillette et de conservation du consentement et identifier si des améliorations doivent y être apportées.
- S'assurer que les personnes concernées soient informées des raisons de l'entreprise motivant la collecte de renseignements personnels, de l'utilisation qui sera faite des renseignements, si la collecte est faite pour un tiers, de son droit de retirer son consentement et de ses droits d'accès et de rectification de ses renseignements personnels.
- S'assurer d'être en mesure de communiquer à la personne qui en fait la demande quels sont les renseignements personnels que l'entreprise détient à son sujet, les catégories de personnes qui ont accès à ses renseignements, la durée de leur conservation ainsi que les coordonnées de la personne responsable de la protection des renseignements personnels de l'entreprise.
- S'assurer que les personnes concernées disposent de toute l'information nécessaire en termes simples et clairs afin de donner un consentement manifeste, libre et éclairé.
- Si l'entreprise traite des renseignements personnels sensibles, le consentement de la personne concernée devra être obtenu de manière expresse. Il faudra donc prévoir un processus impliquant un geste positif dans la communication du consentement, comme le fait de cocher une case.
- Se demander si l'entreprise collecte des renseignements personnels de mineurs de moins de 14 ans. Si tel est le cas, prévoir un processus permettant d'obtenir le consentement du titulaire de l'autorité parentale de ce dernier.
- Conserver des preuves des consentements obtenus des personnes concernées.

Mettre en place un processus de cueillette du consentement pour recueillir, détenir, utiliser ou communiquer des renseignements personnels

Facteurs de planification

- Une révision du processus actuel de votre entreprise en matière d'obtention du consentement des personnes concernées par la collecte de renseignements personnels est la première étape à réaliser pour mener à terme votre mise à niveau aux nouvelles exigences législatives. Ainsi, vous serez en mesure d'identifier les éléments manquants et pourrez déterminer plus facilement les prochaines étapes à réaliser.

Astuce

- Consulter les ressources disponibles sur le sujet afin de bien comprendre les nouvelles exigences législatives.
- Favoriser le consentement explicite et positif, c'est-à-dire que la personne doit, par exemple, cocher une case pour donner son consentement.
- Une fois la mise à niveau réalisée, ne pas hésiter à consulter vos aviseurs légaux qui pourront vous confirmer si votre processus d'obtention du consentement respecte bien toutes vos obligations.

Ressources disponibles

- Consentement | Commission d'accès à l'information du Québec (gouv.qc.ca)
- Renseignements sensibles | Commission d'accès à l'information du Québec (gouv.qc.ca)
- Lignes directrices pour l'obtention d'un consentement valable - Commissariat à la protection de la vie privée du Canada, 13 août 2021
- Vidéo : Renforcez la protection de la vie privée : Obtenez un consentement valable - Commissariat à la protection de la vie privée du Canada
- PL 64 – C comme Consentement - Une simplification complexe? | Ressources | Fasken, 29 juin 2020

Mettre en place un processus de désindexation

Information chronologique

- **Requis selon 2.2.2.4 le 22 septembre 2023**
- **Désindexation requis selon 2.2.2.6 le 22 septembre 2023**
- **Prédécesseur :** Mettre à jour les politiques et les pratiques encadrant la conservation, la destruction et l'anonymisation des renseignements personnels
- **Successeurs :** aucun

Sommaire

Le droit à la désindexation permet à une personne tierce d'une entreprise d'exiger d'être désindexée de l'ensemble de ses systèmes dans certaines circonstances. Cela veut dire qu'il ne sera plus possible de faire le lien entre la personne et ses données, mais ne signifie pas que les renseignements seront supprimés. Cette demande doit être honorée si elle ne cause pas de préjudice à la société et qu'elle ne soit pas assujettie à une exigence légale, réglementaire ou normative à laquelle l'entreprise doit se conformer.

Activités clés

- Mettre en place un processus afin de recevoir la requête de la personne.
- Vérifier l'absence d'exigences légales, réglementaires ou normatives empêchant l'entreprise d'agréer à la demande.
- Développer des processus de destruction, d'anonymisation et de désindexation
- S'il est impossible d'appliquer le droit à la désindexation, informer la personne requérante de la raison empêchant l'entreprise de procéder.
- Si c'est possible, utiliser les techniques d'anonymisation ou de destruction des renseignements personnels.

Mettre en place un processus de désindexation

Facteurs de planification

Selon le secteur d'activité de l'entreprise, le nombre de requêtes peut être élevé. Il est préférable de mettre en place ou d'adapter un système de billetterie qui permet de suivre la progression des requêtes dans le processus.

Astuce

- S'assurer de tenir les personnes requérantes informées tout au long du processus, en indiquant le délai prévisionnel de traitement.
- Les renseignements personnels peuvent être omniprésents dans les systèmes d'information de l'entreprise. Il faut s'assurer d'avoir adapté ces systèmes d'information pour qu'ils soient résilients à une information des tiers anonymisée ou détruite. Ceci inclut les sauvegardes, dont le cycle de vie peut être assez long.
- Séparer les utilisations des renseignements personnels sous une exigence légale, réglementaire ou normative, des utilisations qui ne le sont pas. Si un renseignement personnel est dans la première catégorie, il faudra le conserver malgré tout, ce qui n'est pas le cas pour la deuxième catégorie.
- Tous les fournisseurs de l'entreprise doivent se conformer à ce droit à la désindexation. Il sera fondamental de s'assurer que la chaîne de services TI respecte les pratiques de l'entreprise.

Ressources disponibles

- ENISA The right to be forgotten – between expectations and practice, 2011
- Erdos, D. (2021) The 'right to be forgotten' beyond the EU : an analysis of wider G20 regulatory action and potential next steps, Journal of Media Law, vol. 13.
- Dépersonnalisation, anonymisation et désindexation : nouveau jargon, nouvelles obligations! | Ressources | Fasken

Action à compléter pour
Septembre 2024

12. Implanter des mesures facilitant le droit à la portabilité des données

Implanter des mesures facilitant le droit à la portabilité des données

Information chronologique

- **Requis le 23 septembre 2024**
- **Prédécesseur :** Mettre en place un processus de désindexation
- **Successeurs :** aucun

Sommaire

Le droit à la portabilité des données permet à la personne concernée d'obtenir une copie des renseignements personnels qu'une entreprise détient à son sujet et permet également à cette personne de demander le transfert de ces renseignements d'une organisation à une autre.

Ce droit concerne uniquement les renseignements personnels que l'entreprise a recueilli auprès de la personne concernée. Il ne vise pas les renseignements créés, dérivés, calculés ou inférés à partir de ces renseignements.

Activités clés

- Réviser et, le cas échéant, mettre à jour le processus permettant aux personnes concernées d'avoir accès aux renseignements personnels que l'entreprise détient à son sujet.
- Mettre en place un processus permettant à la personne concernée de demander une copie des renseignements personnels que l'entreprise détient à son sujet.
- Si les renseignements personnels sont informatisés, s'assurer d'être en mesure de les communiquer dans un format technologique structuré et couramment utilisé.
- S'informer sur les personnes ainsi que les organismes qui sont autorisés par la loi à recueillir des renseignements personnels à la suite d'une demande de transfert de la personne concernée.
- S'assurer que les personnes responsables de répondre à de telles demandes des personnes concernées disposent de la formation nécessaire pour communiquer les renseignements personnels de manière sécuritaire et dans un délai raisonnable.

Implanter des mesures facilitant le droit à la portabilité des données

Facteurs de planification

La première étape à réaliser est de réviser le processus déjà en place au sein de votre entreprise en matière d'accès aux renseignements personnels. Par la suite, il est suggéré de procéder à l'identification des éléments manquants afin de répondre aux nouvelles exigences législatives, ce qui vous permettra d'établir un plan d'action efficace pour la mise à jour de votre processus d'accès et de communication des renseignements personnels.

Astuce

- S'informer sur les processus existants en matière de portabilité des données (ex. en vertu du RGPD).
- Impliquer la personne responsable de la protection des renseignements personnels de votre entreprise dans la mise en place de vos nouveaux processus facilitant le droit à la portabilité des données.
- Dans le cas de communication de renseignements personnels automatisés, voici quelques suggestions afin de s'assurer d'être en mesure de les communiquer dans un format technologique structuré et couramment utilisé :
  - Déterminer le format intelligible sous lequel exporter les données (ex. CSV, JSON, XML, etc.);
  - Mettre en place un outil permettant d'extraire les renseignements personnels d'une personne des systèmes de l'entreprise;
  - Définir une procédure d'extraction sécuritaire;
  - Effectuer des tests afin de s'assurer de la complétude des données extraites.
- N'hésitez pas à consulter vos aviseurs légaux pour vous assurer que le processus mis en place respecte toutes les nouvelles exigences législatives applicables et pour obtenir des avis légaux.

Ressources disponibles

- Le droit à la portabilité, une réelle portabilité ou une simple modernisation du droit d'accès? | Ressources | Fasken
- Professionnels : comment répondre à une demande de droit à la portabilité ? | CNIL
- Le droit à la portabilité : obtenir et réutiliser une copie de vos données | CNIL

Cybereco tient à remercier ses membres pour leur précieuse contribution à l'élaboration de ce guide sur la loi 25

Bien que nous espérons que ce guide soit une introduction utile pour mieux comprendre et découvrir le paysage complexe de la loi 25, il ne peut en aucun cas se substituer à des conseils professionnels compétents. Consultez un professionnel avant de prendre des décisions impactant vos finances, vos opérations ou votre protection.

Deloitte.

Desjardins®

FASKEN

mondata

QOHASH

UNIVERSITÉ DE SHERBROOKE

Annexe

Autres ressources disponibles

https://terranovasecurity.com/fr-fr/protection-donnees-personnelles/

https://business.adobe.com/ca_fr/products/advertising/general-data-protection-regulation.html

https://cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/Cyber%20Security%20Small%20Business%20Toolkit_FR.pdf

https://www.lemagit.fr/conseil/GDPR-une-trousse-a-outils-qui-commence-par-une-cartographie

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Conformité et gouvernance

D'ici le 22 septembre 2022	D'ici le 22 septembre 2023	D'ici le 22 septembre 2024
• L'entreprise a-t-elle identifié les critères, telles les connaissances, les compétences et les aptitudes désirées, pour la désignation interne, l'embauche latérale ou l'externalisation du rôle de responsable de la PRP? • La description des rôles et responsabilités du responsable a-t-elle été établie? • De qui relèvera cette personne au sein de l'organisation? • Des changements dans la gouvernance actuelle sont-ils requis pour intégrer et encadrer ce rôle? • La personne responsable de la PRP a-t-elle été désignée? • Cette personne a-t-elle reçu de la formation sur son rôle? • Un programme de formation continue a-t-il été mis en place pour combler tout écart de connaissance et mettre à jour les connaissances du/de la responsable? • Est-ce qu'une évaluation des ressources humaines et matérielles nécessaires à l'exécution des activités de conformité de l'entreprise à la loi a été effectuée?	• L'entreprise connaît-elle ses traitements des renseignements personnels, les écarts avec les nouvelles exigences ont-ils été identifiés et un plan d'action de correction de la situation est-il suivi ? • L'entreprise dispose-t-elle d'un inventaire à jour [1] des traitements qui utilisent des renseignements personnels? • Les politiques de l'entreprise ont-elles été mises à jour pour les rendre conformes aux exigences de la nouvelle loi (incluant : protection, rétention, destruction, transfert et anonymisation?) • Les politiques mises à jour sont-elles approuvées par le responsable de la PRP (secteur privé) ou le comité sur l'accès à l'information et la protection des renseignements personnels (secteur public)? • Un processus de traitement des demandes d'information , demandes d'accès, de rectification et de traitement des plaintes est-il en place? • Disposez-vous de méthodes d'authentification adéquates pour les personnes qui font des requêtes en personne, au téléphone, par courriel, par le Web, etc. ?	• L'entreprise dispose-t-elle d'une politique traitant de l'accès, de la rectification et de la portabilité des données? • L'entreprise dispose-t-elle des moyens technologiques nécessaires pour répondre aux exigences de la loi en matière de portabilité?

1. Cette exigence est prévue pour 2023, mais CyberEcho conseille de réaliser cette étape dès 2022 sachant que celle-ci est préalable à plusieurs autres actions.
2. La Loi 25 introduit le droit de la personne concernée d'obtenir certaines informations «sur demande», notamment à la suite de l'obtention de son consentement à la cueillette de renseignements personnels ou lors d'une décision automatisée.

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Obligations d'information		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
• Les coordonnées du responsable de la PRP sont-elles publiées sur le site web ou par tout autre moyen pour rejoindre l'entreprise (p.ex. site Facebook)?	• Les informations concernant les politiques et pratiques de l'entreprise au niveau de la protection des renseignements personnels sont-elles publiées sur le site internet? • L'entreprise a-t-elle répertorié et documenté les situations où elle utilise des renseignements personnels afin de rendre une décision fondée exclusivement sur un traitement automatisé? Est-ce que l'entreprise est en mesure de déterminer les raisons, principaux facteurs et paramètres menant à ce type de décision?	

Formation		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
• Un programme de formation sur la protection des renseignements personnels des employés et dirigeants a-t-il été élaboré? Est-ce que l'organisation a prévu une mise à jour périodique de son programme? • Comment seront communiquées les politiques et procédures mises à jour au sein de l'entreprise?		

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Incidents de confidentialité		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
• Le plan de réponse aux incidents de confidentialité a-t-il été conçu? Est-il à jour pour répondre aux exigences de la nouvelle loi? • L'organisation s'est-elle dotée d'un modèle de registre des incidents? • L'organisation a-t-elle mis en place et socialisé à ses employés un processus de signalement des incidents? • L'organisation a-t-elle évalué les besoins en termes de ressources et de formation pour la mise en place et le maintien du registre des incidents?		

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Évaluation des facteurs relatifs à la vie privée		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
	• Les projets requérant de procéder à une EFVP ont-ils été identifiés? • Les situations de transfert de renseignements personnels hors Québec ont-elles été identifiées? • Une politique visant la réalisation des EFVP a-t-elle été adoptée? • Quel processus sera suivi afin de porter un projet à l'attention du responsable PRP afin d'enclencher une EFVP? • La méthodologie pour procéder aux EFVP est-elle établie? • Qui accompagnera le responsable PRP dans la réalisation des EFVP?	

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Conception de produits et services		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
	• Les produits et services technologiques offerts par l'entreprise au public, lorsqu'ils sont utilisés pour recueillir des renseignements personnels et qu'ils sont dotés de paramètres de confidentialité, offrent-ils le plus haut niveau de confidentialité à l'utilisateur? • Un inventaire des systèmes d'information ou de prestation électronique de services impliquant l'identification, la localisation ou le profilage d'une personne a-t-il été fait? • Une analyse de la conformité du processus d'activation des fonctions permettant d'identifier, de localiser ou de profiler à la loi a-t-elle été faite? • Les systèmes d'information utilisés par les employés de l'entreprise sont-ils conformes aux exigences de la nouvelle loi?	

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Consentement		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**

	• Les formulaires, processus et autres outils de cueillette de consentements utilisés ont-ils été révisés pour tenir compte des exigences de la nouvelle loi?
	  • Intérêt sérieux et légitime
	  • Déterminer les fins spécifiques avant la collecte
	  • Ne recueillir que ce qui est nécessaire aux fins déterminées avant la collecte
	  • Divulguer, lors de la collecte, les informations listées aux articles 8 et 8.1, le cas échéant
	  • Emploi de termes simples et clairs lors de l'obtention du consentement
	  • Le consentement doit être manifeste, libre et éclairé. Pour les renseignements sensibles, il doit être exprès.
	  • Respect des exigences de l'article 14 pour tout consentement obtenu par écrit
	• Si une collecte auprès de tiers est requise, l'entreprise a-t-elle identifié et documenté que les critères de la loi sont satisfaits?
	• L'entreprise a-t-elle identifié si des renseignements personnels de mineurs de moins de 14 ans étaient recueillis et dans l'affirmative, mis en place les procédés permettant de recueillir ces renseignements de façon valide (par exemple, obtenir le consentement du titulaire de l'autorité parentale ou du tuteur)	

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Utilisation de renseignements personnels		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
	• L'entreprise a-t-elle identifié les situations où elle doit mettre en place un consentement additionnel pour l'utilisation des renseignements personnels à d'autres fins que celles initialement divulguées, et élaboré un processus pour le faire en conformité avec la loi?	

Durée de conservation et destruction des renseignements personnels		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
	• L'entreprise a-t-elle adopté une politique de rétention et de destruction conforme aux exigences de la loi? • L'entreprise a-t-elle adopté et mis à jour son calendrier de rétention de renseignements personnels? • L'entreprise a-t-elle mis en place des techniques d'anonymisation qui respectent les exigences de la loi? • L'entreprise a-t-elle documenté les fins pour lesquelles elle procède à l'anonymisation des renseignements personnels qu'elle détient au lieu de procéder à leur destruction?	

Outil de diagnostic au niveau des nouvelles exigences découlant du projet de loi 25

Mesures de sécurité		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
• Les mesures pour renforcer la cybersécurité des petites et moyennes entreprises (ITSAP.10.035) • D'autres cadres de référence comme ISO 27001 & 2 (sécurité), ISO 29100 (Privacy), NIST – CSF, NIST – Privacy framework peuvent être utilisés pour identifier les mesures de sécurité à mettre en place.		

Désindexation		
D'ici le 22 septembre 2022	**D'ici le 22 septembre 2023**	**D'ici le 22 septembre 2024**
	• L'entreprise a-t-elle prévu un processus conforme à la loi permettant de traiter les demandes liées à la suppression, la désindexation, la réindexation ou la cessation de la diffusion des renseignements personnels des personnes concernées? • L'entreprise s'est-elle munie des ressources et des moyens technologiques nécessaires afin de donner suite aux requêtes des personnes concernées à ce sujet?	

cyber eco