Commission
d'accès à l'information
du Québec

Guide d'accompagnement

Réaliser une évaluation des facteurs relatifs à la vie privée

Document mis à jour
le 10 mars 2021

Version de travail

Ce guide est appelé à évoluer. Il sera revu à la lumière de l'adoption du projet de loi no 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*. Il pourrait être remanié en profondeur.

La Commission vous invite tout de même à lui adresser tout commentaire ou suggestion. Veuillez les faire parvenir à l'adresse courriel suivante : veille@cai.gouv.qc.ca

INTRODUCTION

Le droit à la vie privée est un droit fondamental

Il est protégé par la *Charte des droits et libertés de la personne*[1]. Pour toute organisation[2], qu'elle soit entreprise du secteur privé ou organisme public, ce droit se traduit dans l'obligation de respecter l'intimité et la vie personnelle des personnes en minimisant les renseignements personnels qu'elle recueille, utilise, communique et conserve et dans l'obligation d'en assurer la confidentialité.

Le rythme effréné de l'innovation commande la vigilance.

Les normes et la législation peinent à suivre l'émergence continue et accélérée des nouvelles technologies. Leur adoption devient souvent un préalable à la rentabilité et à la survie des organisations. L'information, incluant les renseignements personnels, est une ressource de plus en plus prisée. Les technologies facilitent la collecte, le traitement et le stockage de renseignements personnels et peuvent impacter la vie privée des personnes.

La protection de la vie privée nous concerne tous.

À l'ère numérique, la responsabilité de veiller au respect de la vie privée ne repose plus seulement sur les épaules des institutions ou des citoyens. Elle incombe désormais à toutes les organisations, publiques comme privées.

Celles qui l'ont compris et qui agissent en conséquence diminuent leur chance de causer des préjudices aux personnes et d'avoir à gérer les contrecoups de ces problèmes (par exemple, des recours juridiques, offrir des compensations financières, des atteintes à la réputation de votre organisation, etc.). Elles sont aussi mieux perçues par le public et par les investisseurs[3].

---

[1] RLRQ, c. C-12, art. 5.

[2] Dans ce guide, les parties où le terme « organisation » est utilisé s'appliquent autant aux entreprises du secteur privé qu'aux organismes du secteur public. Le texte sera spécifique lorsque qu'il s'appliquera uniquement à l'un ou l'autre des secteurs.

[3] En 2018, **91 % des Québécois** accordaient de l'importance à la protection de leurs renseignements personnels et auraient fait davantage affaire avec une entreprise possédant une bonne réputation en la matière (sondage Léger Marketing réalisé pour la CAI) : https://www.cai.gouv.qc.ca/documents/CAI_Sondage_perception_2018.pdf)

Le processus dont il est question dans ce guide est donc non seulement un moyen de mener à bien une évaluation des facteurs relatifs à la vie privée, mais aussi l'occasion de démontrer que votre organisation se préoccupe de ces enjeux.

Ce guide a été conçu par la Commission d'accès à l'information du Québec (CAI).

La CAI veille à la promotion et au respect des droits des citoyens en ce qui concerne l'accès aux documents des organismes publics et la protection de leurs renseignements personnels[4].

Elle veille aussi au respect des lois :

- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[5] (Loi sur l'accès);
- La Loi sur la protection des renseignements personnels dans le secteur privé[6] (Loi sur le privé).

L'équipe de la CAI est à votre disposition pour répondre à vos questions générales concernant le présent guide. Elle ne donnera toutefois pas d'avis ou de conseils concernant l'analyse et l'évaluation des facteurs relatifs à la vie privée (EFVP) d'un projet particulier.

[4] Pour plus d'information, consultez le site Internet de la CAI : **www.cai.gouv.qc.ca**.
[5] RLRQ, c. A-2.1.
[6] RLRQ, c. P-39.1.

QUEL EST L'OBJECTIF DE CE GUIDE?

Ce guide a pour objectif de vous accompagner dans l'évaluation des risques liés à la vie privée si vous devez concevoir, développer ou exploiter :

- Un projet[7] ou une initiative impliquant des renseignements personnels[8];
- Un projet risquant d'avoir une incidence sur le respect de la vie privée des personnes.

Exemples de projets concernés pouvant impliquer la collecte, l'utilisation ou la communication des renseignements personnels :

- Développer un nouveau système d'information ou une technique de personnalisation d'un produit ou d'un service;
- Chercher une nouvelle clientèle, explorer de nouveaux marchés;
- Faire appel à un système d'algorithme ou d'intelligence artificielle;
- Installer un système de vidéosurveillance;
- Comparer différentes versions de bases de données ou de fichiers;
- Acquérir ou fusionner des organisations;
- Utiliser des empreintes digitales, la géolocalisation, un système de reconnaissance faciale, des objets connectés, des capteurs pour villes intelligentes, etc.

---

[7] Le terme **projet** réfère à toute activité au sein d'une organisation : mise en place ou modification d'un programme ou d'un service, recours à une technologie particulière, initiative publique, etc.

[8] Les **renseignements personnels** sont ceux qui concernent une personne physique et permettent de l'identifier (art. 54 de la Loi sur l'Accès et art. 2 de la Loi sur le privé). Sauf exception, ils sont confidentiels. Cette définition est la même pour les organisations publiques que pour les organisations privées, quel que soit le support ou le format (écrit, graphique, sonore, visuel, informatisé ou autre).

À QUI S'ADRESSE CE GUIDE?

À toute personne responsable de la conception, du développement ou de l'exploitation de projets au sein d'une organisation.

Principales personnes concernées : les responsables de la protection des renseignements personnels

Autres exemples de personnes impliquées :

- **Dans les petites entreprises du secteur privé**[9] **:** chefs d'entreprise, commerçants, artisans, travailleurs autonomes, responsables associatifs, etc.;
- **Dans les grandes entreprises privées :** responsables des affaires juridiques, responsables organisationnels de la gestion de risque, toute personne chargée de la sécurité des systèmes d'information, de l'éthique, de la gestion documentaire, etc.;
- **Dans les organisations du secteur public**[10] **:** responsables organisationnels de la sécurité de l'information (ROSI), responsables de la gestion documentaire (RGD), responsables de l'éthique (RE), responsables du développement ou de l'acquisition des systèmes d'information (RDASI), responsables de l'architecture de sécurité de l'information (RASI), responsables de la continuité des services (RCS), responsables de la gestion des technologies de l'information (RGTI), responsables de la sécurité physique (RSP), responsables organisationnels de la gestion de risque, responsables de la vérification interne (RVI), etc.

---

[9] Le terme **entreprise** réfère à l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services (art. 1525 du *Code civil du Québec* (CCQ-1991)). Cette définition s'étend notamment à l'entreprise individuelle (travailleur autonome), à la société par actions (compagnie), à la société en nom collectif (S.E.N.C.), à la société en commandite (S.E.C.), à la société en participation, à la personne morale sans but lucratif, au syndicat de copropriété, à l'association (p. ex. : syndicat), au groupement de personnes (p. ex. : consortium) ou à une fiducie exploitant une entreprise à caractère commercial.

[10] L'intitulé du poste peut varier.

QU'EST-CE QU'UNE ÉVALUATION DES FACTEURS DE RELATIFS À LA VIE PRIVÉE (EFVP)?

Un processus préventif

L'EFVP[11] est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques.

Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

Ces facteurs sont

- La conformité de votre projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient;
- L'identification des risques d'atteinte à la vie privée engendrés par votre projet et l'évaluation de leurs impacts;
- La mise en place de stratégies pour éviter ces risques ou les réduire efficacement.

Ce processus vise **d'abord** à protéger les personnes physiques concernées par ces renseignements. Il vise **aussi** la mise en place de mesures adéquates pour respecter vos obligations en matière de protection des renseignements personnels. Ainsi, l'EFVP permet d'éviter des problèmes que causerait une gestion inadéquate (plaintes, incidents de sécurité, poursuites judiciaires, atteinte à l'image, etc.).

Une bonne pratique évolutive

Dès que des renseignements personnels ou la vie privée des personnes sont concernés, réaliser une l'EFVP constitue une bonne pratique. Cependant, l'EFVP n'est efficace que si elle évolue de façon continue : elle doit être revue au besoin, tout au long de la vie du projet.

---

[11] En anglais, l'EFVP est connue sous l'expression *Privacy Impact Assessment* (PIA).

TABLE DES MATIÈRES

À COMPLÉTER

Vous rencontrerez ce symbole au cours de votre lecture.
Chacune de ses apparitions est une invitation à produire une section en vue de votre rapport d'EFVP.
La Commission produira un modèle de rapport pour vous faciliter la tâche de préparation et de production de l'EFVP.

1. PRÉPARER VOTRE ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

La première étape d'une EFVP consiste à vous poser les bonnes questions et à bien comprendre quels aspects de votre projet sont concernés.

1.1. Vous poser les bonnes questions avant de commencer

Êtes-vous obligé de faire une EFVP?

Faire une EFVP n'est pas obligatoire, sauf pour certains organismes publics (voir section 3.2 *Rédiger un rapport est-il obligatoire?*). Mais si votre projet implique la collecte, l'utilisation ou la communication de renseignements personnels, une EFVP est fortement recommandée.

Ne concluez pas trop rapidement qu'une EFVP est superflue sous prétexte que vous ne pensez pas utiliser de renseignements personnels. Des renseignements en apparence anodins peuvent, une fois croisés avec d'autres, révéler de l'information sur les personnes concernées.

En outre, un survol de votre projet pourrait révéler des enjeux insoupçonnés sur la vie privée des personnes visées par celui-ci..

Si vous décidez de ne pas réaliser d'EFVP, soyez en mesure d'expliquer et de justifier pourquoi vous ne le faites pas.

Si des changements sont apportés à un projet, vérifiez d'abord si une EFVP a déjà été faite et révisez-la pour rendre compte de ces changements.

Quand faire l'évaluation?

Vous devez commencer votre EFVP **au tout début de votre projet** plutôt qu'en fin de parcours :

- Pour pouvoir influencer son déroulement en cours de route
- Pour agir et choisir la solution qui protège et respecte le mieux la vie privée

Pour les projets de grande envergure, vous pouvez faire une EFVP préliminaire, plus courte et moins exhaustive, avant une EFVP complète.

Par exemple, certains projets requièrent des études d'opportunité, de préfaisabilité ou de faisabilité. Une EFVP préliminaire dans le cadre de ces études peut éviter d'engager des

frais pour des solutions qui pourraient s'avérer non conformes ou engendrer des enjeux disproportionnés pour les personnes par rapport à vos objectifs d'affaires.

Qu'allez-vous inclure dans votre évaluation?

Vous avez intérêt à délimiter clairement la portée de votre évaluation et à tenir votre analyse à un niveau adapté à votre projet.

Exemple 1 : Vous décidez de ne pas inclure la révision des procédures d'identification des personnes dans votre projet d'assistant virtuel en ligne. Vous jugez que cela n'a pas d'importance, car votre système actuel fonctionne bien avec votre service à la clientèle en personne et au téléphone. **Votre portée est peut-être trop étroite.** Des éléments importants pourraient manquer à votre évaluation, car une identification en ligne n'a peut-être pas les mêmes caractéristiques qu'une identification en personne ou au téléphone.

Exemple 2 : Pour le même projet, vous décidez finalement de revoir les procédures d'identification, l'hébergement des données de vos clients, les formulaires de confidentialité de vos employés du service à la clientèle et l'ensemble de vos infrastructures systèmes. **Votre portée est sans doute trop large.** Des évaluations distinctes pourraient sans doute être produites pour certains sous-processus.

Exemple 3 : Pour le même projet, vous ne faites que la révision de vos politiques et directives de service à la clientèle, sans vous attarder aux détails techniques de la solution logicielle que vous avez acquise ni aux procédures d'identification des personnes. **Votre analyse se situe peut-être à un trop haut niveau.** Vous manquerez sans doute des éléments importants qui existent au niveau de la solution logicielle ou des procédures d'identification.

En définissant clairement votre portée, vous aurez une meilleure idée des ressources à impliquer dans la réalisation de l'EFVP.

Vous devez être en mesure de justifier les limites que vous imposez à votre évaluation.

Exemple 4 : Pour le même projet, des EFVP distinctes ont récemment été produites par votre organisation concernant les procédures et les processus d'identification des personnes qui s'adressent au service à la clientèle. **Vous décidez de ne pas refaire cette partie d'analyse et vous analysez uniquement la partie qui s'ajoute concernant l'identification par l'assistant virtuel.** Vous l'indiquez clairement dans votre rapport afin d'informer les gens des limites que vous posez à votre évaluation.

Qui devriez-vous impliquer?

Principalement

- Les personnes responsables du projet;
- Les personnes au courant des bonnes pratiques en matière de respect de la vie privée, de protection des renseignements personnels et de sécurité de l'information;
- Les personnes responsables des affaires juridiques;
- Les autorités compétentes de votre organisation devant prendre position sur la gestion des risques à la fin de la démarche (voir section 3*)*.

Selon l'envergure du projet ou les impacts sur la vie privée

- Vos collègues de travail dans certains départements : ressources humaines, gestion de risques, gestion documentaire, affaires juridiques, relations avec la clientèle, etc.;
- Vos clients, partenaires corporatifs, sous-traitants, etc.

Devez-vous documenter votre démarche?

Vous avez tout avantage à le faire. Conservez une trace écrite de toute votre démarche.

En cas de problème ou de question en lien avec la vie privée ou avec la protection des renseignements personnels, votre documentation attestera du sérieux de votre réflexion.

1.2. Définir votre projet

Cette première étape de l'EFVP est surtout descriptive. L'objectif est de documenter les informations importantes pour vous permettre d'évaluer les risques et les moyens d'éliminer ou de réduire ces risques (voir sections 2.2, 2.3 et 2.4).

Présentez les grandes lignes de votre projet

- En quoi consiste-t-il?
- Quel était le contexte quand l'idée de ce projet est apparue?
- Quelle est/était la situation au moment de son lancement?
- Quel est l'échéancier de sa mise en œuvre?

Expliquez quels sont les objectifs qui motivent votre projet

Ces objectifs peuvent expliquer pourquoi vous devez mettre en place de nouvelles mesures ou pratiques impliquant la gestion des renseignements personnels.

Cet objectif doit être **légitime** et se rapporter à des **préoccupations réelles et justifiables**.

Exemples d'objectifs visés par un projet :

- Vouloir mieux connaître votre clientèle;
- Offrir un nouveau service public;
- Déployer sur le Web un service existant;
- Accroître la sécurité d'une installation;
- Contrer la fraude;
- Vous mettre en conformité avec la réglementation;
- Conserver votre compétitivité;
- Lancer une nouvelle branche d'affaires ou rechercher une nouvelle clientèle pour appuyer votre croissance;
- Offrir une expérience client plus agréable, plus intuitive et plus efficace en créant la nouvelle version d'une plateforme.

Privilégiez une solution proportionnée à vos objectifs et aux risques d'atteinte à la vie privée

L'évaluation de la proportionnalité doit être faite tout au long de l'évaluation des facteurs à la vie privée et de la mise en place de votre projet.

Votre solution sera proportionnelle si :

- Il existe un lien rationnel entre vos objectifs et la solution proposée, c'est-à-dire qu'il s'agit d'un moyen efficace d'atteindre l'objectif visé. Cette efficacité doit être basée sur des données concrètes et probantes;
- Que l'atteinte à la vie privée est minimale ou qu'il n'y a pas d'autres solutions efficaces moins intrusives;
- Que les avantages concrets surpassent les conséquences ou les préjudices pour les personnes concernées.

1.3. Établir le partage des rôles et des responsabilités

Identifiez les parties impliquées dans le projet

- Qui sont les intervenants au sein de votre organisation
- Quels sont leurs rôles et leurs responsabilité (en incluant les responsables de la protection des renseignements personnels et de la sécurité de l'information);
- Qui sont les intervenants extérieurs (par **exemple**, vos fournisseurs de services, vos partenaires, autres organisations que vous impliquées[12], etc.);
- Qui seront les utilisateurs de votre service et quelle clientèle sera impactée.

À COMPLÉTER

- Description du projet
- Description des rôles et responsabilités

1.4. Connaître vos obligations en matière de protection des renseignements personnels

Les obligations peuvent provenir de sources différentes. Cela dépend de la nature et de l'envergure de votre projet.

Identifier vos obligations et comprendre les enjeux qu'elles impliquent n'est pas une tâche facile. En cas de doute, **n'hésitez pas à consulter un juriste**.

Sur le plan provincial

Au Québec, l'utilisation de renseignements personnels est encadrée principalement par deux lois :

- La *Loi sur la protection des renseignements personnels dans le secteur privé*, qui s'applique aux **organisations du secteur privé** (entreprises et organismes à but non lucratif);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, qui s'applique aux **organisations du secteur**

[12] Pour les organismes publics, pensez à mentionner les autres organisations gouvernementales, sur les plans local, provincial, fédéral et international.

public (ministères et organismes gouvernementaux et municipaux, organismes des réseaux de la santé et de l'éducation).

Voici une liste non exhaustive de lois qui contiennent des particularités en matière de protection des renseignements personnels :

- Code civil (RLRQ, c. CCQ-1991);
- Loi sur les archives (RLRQ, c. A-21.1);
- Loi concernant la cadre juridique des technologies de l'information (RLRQ, c. C-1.1);
- Code des professions (RLRQ, c. C-26);
- Loi sur l'administration fiscale (RLRQ, c. A-6.002);
- Code de la sécurité routière (RLRQ, c. C-24.2);
- Loi sur la protection de la jeunesse (RLRQ, c. P-34.1);
- Loi sur les services de santé et les services sociaux (RLRQ, c. S-4.2);
- Loi sur l'assurance maladie (RLRQ, c. A-29).

Exemples de particularités et exceptions précisées dans des lois :

- La collecte et l'utilisation du numéro de permis de conduire et du numéro d'assurance maladie sont régies par des lois, des règlements ou des directives sectorielles[13];
- La gestion du consentement est particulière pour les mineurs et les personnes majeures inaptes;
- L'utilisation et la collecte de renseignements biométriques[14] sont régies de manière spécifique et complémentaire par la *Loi concernant la cadre juridique des technologies de l'information*.

[13] Pour plus d'information sur l'utilisation des pièces d'identité, veuillez vous référez aux fiches Pièces d'identité : citoyens et Pièces d'identité : entreprises.

[14] Pour obtenir plus d'information, voir la section Biométrie du site de la Commission. Voir également note de bas de page 18.

Sur le plan fédéral et à l'international

Le gouvernement fédéral et certaines provinces canadiennes possèdent leurs propres législations et réglementations en matière de protection des renseignements personnels. Si votre entreprise exerce ses activités dans une ou plusieurs autres provinces, assurez-vous de bien connaître les obligations qui découlent de leurs législations.

Rappelez-vous que les communications de renseignements personnels à l'extérieur du Québec et du Canada sont soumises à un encadrement particulier par les lois provinciales et fédérales.

Pour les activités à l'international, sachez que les lois peuvent différer beaucoup d'un pays à l'autre. De plus, des obligations supplémentaires pourraient s'appliquer à certaines catégories de renseignements personnels, notamment pour les renseignements sensibles.

Enfin, certaines législations ont une portée extraterritoriale. Elles s'appliquent si une organisation collecte, utilise, communique ou conserve des renseignements personnels de personnes se trouvant sur le territoire couvert par ces législations, même si cette organisation ne se trouve pas sur ce territoire, Le *Règlement général sur la protection des données* européen est un exemple. Le non-respect de ces législations s'accompagne parfois de lourdes sanctions financières.

Si vos services visent un marché ou des citoyens de l'étranger, informez-vous et considérez les impacts que ces lois pourraient avoir sur votre projet.

Pratiques corporatives

Votre organisation peut encadrer le traitement des renseignements personnels de diverses façons : par des politiques, des processus, des procédures, des méthodes de travail, un plan et un calendrier de conservation, etc.

Bien que de tels documents internes n'aient pas force de loi, il est important d'en tenir compte dans votre évaluation pour ne pas vous écarter des pratiques en vigueur dans votre organisation. Votre travail pourrait même vous permettre d'identifier des lacunes au sein de votre organisation.

Normes

Différentes normes internationales peuvent alimenter votre réflexion sur vos pratiques, par exemple certaines normes ISO ou la documentation produite par l'Union européenne ou l'Organisation de coopération et de développement économiques (OCDE). Consultez-les si vous cherchez à adopter les meilleures pratiques en matière de respect de la vie privée et de protection des renseignements personnels.

1.5. Repérer les renseignements personnels impliqués dans votre projet

Faire l'inventaire des renseignements personnels

Afin de bien évaluer la conformité de votre projet avec la législation applicable et les risques d'atteinte à la vie privée qu'il comporte, vous devez faire l'inventaire des renseignements personnels qu'il implique. Cela vous permettra, par exemple, de vous assurerez de ne recueillir ou d'utiliser que les renseignements personnels nécessaires.

Toutefois, cette liste exhaustive n'est pas nécessaire à toutes les étapes de l'évaluation.

Par exemple, dans le rapport, une liste faisant état de regroupement de renseignements personnels de même nature pourrait suffire.

Ces regroupements contiennent des renseignements personnels qui possèdent des caractéristiques communes et/ou qui sont regroupés afin d'accomplir une fonction ou atteindre un objectif.

Votre liste doit quand même prévoir une courte énumération du contenu de ces regroupements.

Exemples de regroupements de renseignements personnels :

- Renseignements d'identité et coordonnées de vos clients (nom, prénom, nom d'utilisateur, mot de passe);
- Dossiers médicaux, en version électronique et papier (résultats médicaux, résumés des rencontres, données de santé, imagerie médicale);
- Dossiers d'invalidité des employés détenus par les ressources humaines (renseignements d'identité, rapports médicaux, communications avec les assureurs);
- Courriels et enregistrements téléphoniques du centre d'appels (échanges avec les clients, contenu des questions et des réponses, échantillon de la voix);
- Données de journalisation du site Internet et outil d'analyse Web (historiques des pages consultés, adresse IP, navigateur et appareil utilisé, configuration de l'affichage).

Éléments à retenir

- Si vous n'êtes pas certain qu'un regroupement contient des renseignements personnels, conservez-le quand même dans votre liste et considérez-le dans votre EFVP.

- Incluez tous les renseignements que vous créez ou inférez sur les personnes (**exemples :** une cote de crédit, une note d'évaluation, une note dans un dossier). Ce sont des renseignements personnels.
- Pensez aux renseignements collectés automatiquement par les appareils et les systèmes informatiques que vous utilisez.
- Incluez les renseignements pseudonymisés[15], dépersonnalisés ou anonymisés[16] et agrégés[17] dans votre liste. Même si certains de ces renseignements ne sont plus directement reliés à l'identité d'une personne, les nouvelles technologies permettent bien souvent de rétablir ce lien. Il sera pertinent d'évaluer le risque de réidentification de ces renseignements.
- Même si vous ne présentez que regroupements dans le rapport d'évaluation, il est important que votre organisation soit en mesure de connaitre l'étendue de tous les renseignements personnels qu'elle détient.

Évaluer le degré de sensibilité de ces renseignements

Un renseignement est dit « sensible », soit parce qu'il révèle quelque chose d'intime, d'unique ou si sa révélation ou son utilisation peut causer des conséquences négatives pour la personne.

La Loi sur l'accès et la Loi sur le privé reconnaissent cette distinction. Elles prévoient notamment que les mesures de sécurité soient adaptées à la sensibilité des renseignements.

Exemples de renseignements sensibles :

- Renseignements concernant le groupe ethnique ;
- Renseignements concernant les croyances philosophiques ou religieuses;
- Renseignements concernant la santé ou l'orientation sexuelle;
- Renseignements financiers;

---

[15] Des renseignements sont pseudonymisés si les informations qui identifient directement les personnes (**p. ex.** nom, prénom) sont remplacées par des informations qui les identifient de façon indirecte (**p. ex.** no de dossier).
[16] Des renseignements sont dépersonnalisés ou anonymisés s'il est impossible d'identifier une personne à partir du jeu de données. La garantie d'anonymat est obtenue à la suite de l'application d'une ou de plusieurs méthodes. L'anonymisation doit être irréversible.
[17] Des renseignements sont agrégés lorsque plusieurs données de même type sont regroupées (**p. ex.** statistiques), ce qui rend impossible l'identification d'un individu donné.

- Renseignements biométriques[18],
- Identifiants uniques[19].

1.6. Identifier les points où votre organisation entre en interaction avec les renseignements personnels

Les points d'interactions peuvent être

- Les personnes, les ensembles de personnes ou les partenaires et tiers qui accèdent aux renseignements personnels (**exemples :** employés, clientèle, sous-traitants, firmes de consultation, chercheurs externes, équipes d'entretien de bâtiments ou de systèmes informatiques, fournisseurs de télécommunication);
- Les moyens utilisés pour collecter des renseignements personnels (**exemples** : formulaires d'abonnement, boîtes courriel, messageries téléphoniques, plateformes collaboratives, sondages, questionnaires);
- Les moyens utilisés pour communiquer des renseignements personnels (**exemples :** prestations électroniques de service, échanges par courriel, service à la clientèle, sites Web, interfaces d'échange informatisées [API] ou liens électroniques sécurisés);
- Les moyens utilisés pour traiter et conserver des renseignements personnels (**exemples:** systèmes informatiques, services infonuagiques, copies de sauvegarde, outils de télécommunication, salles et classeurs d'entreposage des dossiers papier).

Dégager une vue d'ensemble de la circulation des renseignements personnels tout au long de votre projet

À partir des points d'interaction que vous avez identifiés, illustrez le parcours des renseignements personnels tout au long du processus visé par votre projet.

---

[18] Les renseignements biométriques sont des renseignements portant sur les caractéristiques biologiques ou comportementales d'une personne. Ils sont généralement destinés à déterminer son identité (**p. ex.** empreintes digitales, forme du visage, empreinte de l'iris, empreinte de la voix, démarche, signature, renseignements génétiques).
[19] Un identifiant unique est une information qui permet de distinguer un individu dans un ensemble (**p. ex.** un numéro de client ou d'employé).

Cette vue d'ensemble peut être décrite et/ou schématisée. Le schéma est une façon simple et avantageuse de présenter l'information en un coup d'œil.

Cette description ou ce schéma sera plus complexe pour les grands projets, de sorte qu'un découpage par processus pourrait s'avérer préférable.

Identifier les particularités de chaque phase de votre projet

La **phase de développement** de votre projet peut comporter des risques en matière de vie privée qui sont différents de ceux qui existeront dans la **phase d'exploitation** :

- Phase de **développement** : votre projet prend forme, vous élaborez des solutions pour résoudre les problèmes qui émergent. Des personnes interviennent ponctuellement durant cette phase (par exemple, des consultants). Vous faites des périodes d'essais sur différents produits. Le projet peut être modifié en cours de route.
- Phase d'**exploitation** : votre projet est vivant, vous veillez à ce qu'il produise les résultats escomptés. Des événements peuvent survenir spécifiquement durant cette phase, comme des mises à jour du système. Des employés peuvent quitter votre entreprise. Des personnes peuvent vous faire des demandes d'accès à l'information.

Exemple 1 : Je suis directeur commercial d'une entreprise qui fabrique des vêtements sur mesure. J'aimerais proposer un outil de commande en ligne disponible pour mes clients.

Une firme spécialisée sera embauchée durant **la phase de développement**. Je dois prévoir que ces consultants entreront en contact avec certains renseignements concernant mes vendeurs et mes clients tout au long de la mise en place du système. Cependant, ils n'y auront plus accès un certain temps après la mise en service du système, lors de la **phase d'exploitation**. De plus, je dois considérer que les risques de bogues informatiques seront plus élevés durant cette période. Que dois-je prévoir pour réduire les risques?

Exemple 2 : Je suis directrice des ressources humaines d'une grande organisation gouvernementale. Je vais faire changer le logiciel de gestion des ressources humaines. Le fournisseur du logiciel m'avise que le système est mis à jour fréquemment et m'informe que des refontes plus importantes sont à prévoir dans la prochaine année. Je dois anticiper ces éventuelles refontes qui arriveront en **phase d'exploitation**. Je dois mettre des moyens en place afin que ces opérations de maintenance n'aient pas d'incidence sur les données personnelles des employés.

À COMPLÉTER

- Inventaire des renseignements personnels impliqués
- Vue d'ensemble de la circulation des renseignements

2. ANALYSER ET ÉVALUER LES FACTEURS RELATIFS À LA VIE PRIVÉE

Cette étape est l'essence de la démarche. Il s'agit de considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

Ces facteurs sont :

- La conformité de votre projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient;
- L'identification des risques d'atteinte à la vie privée engendrés par votre projet et l'évaluation de leurs impacts;
- La mise en place de stratégies pour éviter ces risques ou les réduire efficacement.

2.1. Respecter les obligations et les principes de protection des renseignements personnels

Posez-vous les questions suivantes :

- Respectez-vous les obligations et les principes de protection des renseignements personnels pour chacune des catégories de renseignements personnels, à chacun des points d'interaction et tout au long du cycle de vie des renseignements?
- Sinon, quelles sont les modifications que vous devriez apporter à votre projet pour que vos obligations et les principes soient respectés?

Documentez les moyens qui sont mis en place pour respecter vos obligations et ces différents principes.

En cas de doute concernant le respect de vos obligations légales, **n'hésitez pas à consulter un juriste**.

Pour **les entreprises du secteur privé**, les principes applicables sont les suivants :

- **Déterminer les fins de la collecte :** Vous devez avoir un intérêt sérieux et légitime pour constituer un dossier sur une personne.
- **Limiter la collecte de renseignements personnels :** Vous devez collecter uniquement les renseignements nécessaires pour offrir votre bien ou votre

service. Votre collecte doit se faire par des moyens licites. Sauf exception, la collecte doit se faire auprès de la personne concernée.

- **Informer la personne concernée :** Avant de constituer un dossier, vous devez informer la personne concernée des finalités du dossier, de l'utilisation qui sera faite des renseignements personnels, des catégories de personnes qui y auront accès au sein de votre entreprise et de l'endroit où ils seront détenus. Vous devez également informer les personnes concernées des droits d'accès et de rectification qui leur sont accordés par la Loi sur le privé. Vous devez inscrire quel est l'objet du dossier.
- **Mettre en place des mesures de sécurité appropriées :** Vous devez prendre les mesures de sécurité propre à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- **Limiter l'accès aux renseignements personnels :** Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour le recevoir au sein de l'entreprise lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions.
- **Limiter l'utilisation de renseignements personnels :** Vous devez obtenir le consentement de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli, à moins d'une exception prévue par la loi.
- **Obtenir le consentement à communiquer des renseignements personnels :** Vous devez obtenir le consentement de la personne concernée pour communiquer ses renseignements à autrui, à moins d'une exception prévue par la Loi sur le privé;
- **Requérir le consentement des personnes concernées :** À moins d'une exception prévue par la Loi sur le privé, vous devez obtenir le consentement de la personne concernée avant de collecter auprès d'un tiers, d'utiliser ou de communiquer des renseignements personnels. Ce consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. De plus, il ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles vous l'avez demandé.
- **Assurer la qualité des renseignements personnels :** Vous devez veiller à ce que les renseignements personnels que vous détenez soient à jour et exacts au moment où vous les utilisez pour prendre une décision relative à la personne concernée.

- **Permettre l'exercice des droits d'accès et de rectification :** Un renseignement personnel doit pouvoir être accessible et rectifié par la personne concernée.
- **Répondre avec diligence :** Vous devez répondre avec diligence aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées.

Pour les organisations du secteur public, les principes applicables sont les suivants :

- **Assumer vos responsabilités** : Chaque organisme public a la responsabilité d'assurer le caractère confidentiel des renseignements personnels qu'il détient.
- **Déterminer les fins de la collecte de renseignements personnels :** Avant d'entreprendre toute collecte d'information, vous devez définir les raisons pour lesquelles vous comptez recueillir et utiliser un renseignement personnel.
- **Limiter la collecte de renseignements personnels :** Vous ne pouvez recueillir que les seuls renseignements personnels nécessaires à l'exercice des attributions de votre organisme ou à la mise en œuvre d'un programme dont il a la gestion.
- **Informer la personne concernée :** Vous avez l'obligation d'informer adéquatement la personne concernée avant qu'elle vous fournisse les renseignements personnels attendus.
- **Limiter l'accès aux renseignements personnels :** La Loi sur l'accès prévoit qu'un renseignement personnel ne sera accessible qu'aux seules personnes ayant la qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions.
- **Requérir le consentement des personnes concernées** : Un renseignement personnel demeure inaccessible tant que la personne concernée n'a pas consenti à sa divulgation[20].
- **Assurer la qualité des renseignements personnels :** Un renseignement personnel doit être maintenu à jour, être exact et complet afin de servir adéquatement aux fins pour lesquelles il a été recueilli ou est utilisé.

[20] Certaines exceptions précisées par la Loi sur l'accès autorisent la communication de renseignements personnels sans le consentement préalable des personnes concernées.

- **Mettre en place des mesures de sécurité appropriées :** Vous devez prendre les mesures de sécurité propre à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- **Permettre l'exercice des droits d'accès et de rectification :** Un renseignement personnel doit pouvoir être accessible et rectifié par la personne concernée.
- **Limiter la durée de conservation des renseignements personnels :** Vous êtes tenus de détruire irréversiblement tout renseignement personnel lorsque l'objet pour lequel il a été recueilli est accompli.
- **Répondre dans les délais légaux :** Vous devez répondre aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées dans les vingt jours suivant leur réception.

2.2. Repérer et décrire les risques sur la vie privée engendrés par votre projet

Qu'est-ce qu'un risque? Il s'agit d'une situation ou d'un évènement futur qui peut ou non se réaliser et qui causerait une perte ou un préjudice. Le risque est une *menace potentielle*.

Un **risque sur la vie privée** consiste en un événement qui causerait une perte ou un préjudice à une personne au niveau du respect de son intimité ou de sa vie personnelle.

Dans ce cas-ci, la perte ou le préjudice n'a pas besoin d'être tangible : les effets de l'atteinte à la vie privée peuvent être manifestes et externes (**exemple :** en cas de dommage à la réputation), où être vécues de l'intérieur par les personnes concernées (**exemple** : sentiment d'intrusion).

Dans ce contexte, certains aspects d'un projet qui sont conformes du point de vue légal peuvent quand même être perçus comme une atteinte à la vie privée par les personnes concernées.

Faire la gestion des risques dans le cadre de l'EFVP

Cela consiste à recenser les risques auxquels votre organisation est exposée, puis à définir et à mettre en place des mesures préventives appropriées en vue de supprimer ou d'en atténuer les conséquences.

Vous devez donc établir des scénarios de tels événements qui pourraient découler de la mise en œuvre de votre projet et d'estimer les impacts potentiels sur la vie privée des personnes concernées par ces événements.

Posez-vous les questions suivantes :

- Quels sont les situations ou les événements qui peuvent raisonnablement survenir pour chacun des renseignements personnels, à chacun des points d'interaction, tout au long du cycle de vie des renseignements?
- Quels sont les situations ou les événements qui pourraient engendrer une perte ou un préjudice pour les personnes concernées du point de vue du respect de leur vie privée?

Dressez la liste des réponses que vous donnerez à ces questions et décrivez brièvement ces situations.

Exemples de risques sur la vie privée :

- Conservation de renseignements lorsque leur utilité n'est plus démontrée;
- Vol de renseignements personnels;
- Collecte excessive de renseignements;
- Divulgation non autorisée de renseignements personnels;
- Réidentification de renseignements préalablement anonymisés;
- Manque d'information fournie aux individus lors de la collecte;
- Création excessive ou non justifiée d'informations;
- Objectif du projet pas suffisamment important ou non légitime;
- Intrusion dans la vie privée disproportionnée par rapport à l'objectif visé par le projet.

Votre organisation a peut-être déjà en main des avis juridiques ou les résultats d'analyses de sécurité informatique. Si des risques de non-conformité ou des risques en matière de sécurité de l'information ont été abordés dans ces documents, vous pouvez vous en inspirez pour produire votre EFVP.

Décrire et évaluer les impacts potentiels

Chacun des risques peut causer des impacts qu'il convient de décrire, puis d'évaluer.

Les **impacts potentiels** sont variés :

- vol d'identité et fraudes;
- dangers sur la vie et sur la sécurité des personnes (comme les possibilités de harcèlement);
- pertes financières ou d'opportunités;
- dommage à la réputation;
- sollicitation non désirée; et
- Intrusions et autres nuisances dans la vie privée des personnes.

Les considérations en lien avec les dommages à la réputation de votre organisation, les coûts potentiels que l'événement pourrait vous faire encourir, les litiges qui pourraient s'en suivre ou toute autre conséquence négative portée à votre organisation ne doivent pas entrer en ligne de compte dans votre évaluation des impacts sur la vie privée des personnes concernées.

Identifier les causes de ces risques

Précisez quelles seraient les causes de ces situations.

Les **causes potentielles** sont également variées :

- un processus déficient;
- des erreurs dans la manipulation des renseignements;
- un manque de connaissances ou de formation;
- des mécanismes de surveillance insuffisants ou inexistants;
- une distribution inadéquate des responsabilités;
- des comportements malveillants;
- une collecte excessive de renseignements;
- des technologies défaillantes ou désuètes;
- l'utilisation non justifiée ou non nécessaire de renseignements sensibles;
- l'absence de consentement;
- l'existence d'un moyen alternatif moins intrusif et suffisamment efficace pour atteindre l'objectif visé.

Tenez compte de certaines particularités

Projets impliquant de nouvelles technologies

Certaines technologies soulèvent des enjeux particuliers et les technologies émergentes suscitent des questions parfois inédites.

Pour évaluer adéquatement les risques qu'une technologie comporte, il est essentiel de bien la connaître avant de la déployer, surtout si celle-ci n'a jamais été utilisée auparavant.

L'utilisation de données biométriques est un exemple de technologies qui suscitent des questions et des enjeux particuliers[21].

Demandez l'aide de spécialistes si vous ne pouvez pas effectuer une évaluation adéquate par vous-même.

Projets d'envergure

Les grands projets génèrent davantage de risques, car ces risques peuvent toucher davantage de personnes.

Pour les projets comportant plusieurs phases, il peut être avantageux ou nécessaire de produire une EFVP pour chacune d'elle. L'environnement et les risques de chacune des phases seront différents.

Pour les projets s'échelonnant sur de longues périodes, une mise à jour régulière de l'EFVP peut être profitable pour le bon déroulement du projet.

Projets comportant des enjeux éthiques

Certains types de projets exigent qu'une évaluation soit produite par un comité d'éthique. C'est notamment le cas des recherches scientifiques portant sur des humains. Des recommandations en lien avec la protection de la vie privée sont parfois émises par ces comités. Celles-ci devraient normalement être considérées dans vos évaluations.

Des rapports d'évaluation éthique des nouvelles technologies sont fréquemment diffusés par des organismes indépendants ou des chercheurs universitaires. Ces documents abordent bien souvent des questions de vie privée. Ce sont des sources d'information pertinentes pour réfléchir aux enjeux et aux risques générés par les projets technologiques.

---

[21] Pour toute information concernant l'utilisation de systèmes biométriques, veuillez-vous référer au guide produit par la Commission intitulé Biométrie : principes à respecter et obligations légales des organisations. à ce sujet

2.3. Évaluer l'impact des risques identifiés

Se doter d'une méthode pour qualifier les risques

Il n'y a pas de méthode prescrite pour qualifier ou évaluer les risques ni pour présenter les résultats de votre analyse. Néanmoins, une évaluation en fonction de l'impact potentiel d'un événement et de la probabilité qu'il se concrétise peut répondre aux objectifs de l'EFVP.

L'évaluation des risques est un processus subjectif, il est souvent utile de constituer un comité pour tenir cette activité.

Si des pratiques en matière de gestion de risques sont en vigueur dans votre organisation, privilégiez-les.

Évaluer l'impact de chacun des risques identifiés

L'appréciation de l'impact peut se faire à l'aide d'un système de cotes.

Exemple d'un système de cotes pour apprécier **l'impact d'un risque** :

- Très faible et/ou inexistant (1) : le risque n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne;
- Faible (2) : le risque engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes;
- Grand (3) : le risque engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes;
- Très grand (4) : le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes;
- Inacceptable (non coté) : le risque engendre des conséquences trop importantes et/ou implique une non-conformité aux lois.

L'évaluation de l'impact peut être influencée par certaines variables

- La quantité de renseignements impliqués;
- La nature et la sensibilité des renseignements impliqués;
- La gravité et la nature des préjudices qui pourraient être causés aux personnes (**exemples :** impacts sévères sur la vie personnelle ou professionnelle, sur les

finances, procédures juridiques pour résoudre la situation, mettre en danger la vie de la personne);

- Le nombre de personnes touchées potentiellement ou le profil de ces personnes (**exemples :** enfants, personnes en situation de handicap, immigrants).

Estimer la probabilité que les risques se réalisent

Votre estimation peut aussi se faire à l'aide d'un système de cotes.

Exemple d'un système de cote pour évaluer **les probabilités** :

- Très faible et/ou inexistant (1) : Le risque n'a aucune chance de se concrétiser;
- Faible (2) : le risque a peu de chance de se concrétiser ou un événement similaire ne s'est jamais produit;
- Grand (3) : le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelque reprises;
- Très grand (4) : le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises

Considérant que le risque zéro n'existe pas, cette estimation peut être très difficile à faire. Soyez réaliste : évitez d'être trop confiant ou trop conservateur.

Considérer les stratégies et moyens de contrôle existants

Votre organisation peut déjà avoir mis en place des outils, des politiques, des directives, des procédures ou d'autres moyens pour atténuer ou éliminer le risque sans que des mesures supplémentaires n'aient été adoptées.

Listez-les et réévaluez les risques à la lumière de ces informations.

Déterminer le seuil acceptable de tolérance pour chaque risque

Mettez-vous dans la peau des personnes concernées et demandez-vous comment elles pourraient s'attendre à ce que leurs renseignements personnels soient utilisés et protégés.

Fixez-vous des seuils à atteindre selon ce qui pourrait paraître acceptable pour ces personnes.

Vous devez établir ces seuils en tenant compte du contexte de votre projet. Par exemple, une personne qui fournit des renseignements médicaux a des attentes différentes envers un centre hospitalier qu'envers des publicitaires.

2.4. Éliminer ou réduire les risques d'atteintes à la vie privée

Étudier les stratégies envisageables pour éliminer ou réduire les risques

Les stratégies peuvent chercher à réduire, soit l'impact du risque, soit les chances que ce dernier se concrétise, soit les deux en même temps.

Ainsi, réduire la quantité de renseignements personnels que vous collectez réduit l'impact d'un vol de données. L'ajout de mesures de sécurité réduit plutôt les probabilités qu'il se réalise.

Exemples de stratégies :

- Prévoir une révision périodique des différentes collectes de renseignements personnels;
- Mettre en place un système de gestion documentaire qui permet l'application automatisée du calendrier de conservation;
- Revoir les processus d'attribution et de gestion des accès informatiques;
- Engager des firmes de sécurité informatique pour revoir périodiquement les paramètres de sécurité de la prestation électronique de service;
- Revoir les clauses des contrats en matière de confidentialité;
- Établir un calendrier de formation et d'activités de sensibilisation pour vos employés;
- Faire une campagne d'information concernant votre nouvelle utilisation des renseignements personnels;
- Journaliser les accès et exploiter les journaux pour détecter les anomalies;
- Dépersonnaliser ou anonymiser les renseignements si leur utilisation sous une forme nominative n'est pas requise pour tous.

Choisir les stratégies à adopter

Déterminez quelles stratégies et quels moyens vous mettrez en place pour éliminer ou réduire un risque.

Ce choix ne peut se faire sans tenir compte de la réalité de votre projet et de votre organisation ainsi que des ressources à votre disposition. Songez à des solutions réalisables pour votre organisation.

Réévaluer le niveau de chacun des risques

À la lumière des stratégies et moyens retenus, réévaluez le niveau d'impact du risque et la probabilité qu'il se concrétise.

Vérifiez si vous avez atteint le seuil de tolérance que vous vous étiez fixé. Si le seuil n'est pas atteint, réévaluez votre choix de stratégies ou de moyens.

Si après avoir revu votre choix, vous ne parvenez toujours pas à éliminer un risque important ou que le seuil de tolérance que vous vous étiez fixé n'est pas atteint*, pensez à revoir en profondeur cet aspect de votre projet ou à le retirer.*

Tout risque qui persiste à la fin, une fois que vous avez pris les mesures visant à diminuer ou éliminer les risques identifiés au départ, devient un **risque résiduel**.

Il est possible que des risques d'atteinte à la vie privée subsistent même après avoir éliminé ou minimisé la plupart d'entre eux. Votre organisation doit néanmoins être en mesure d'assumer la responsabilité des risques résiduels qu'elle fait encourir aux personnes concernées.

Un conseil

Même si un risque est complètement éliminé ou qu'une stratégie n'est pas retenue, vous gagnez à garder des traces de votre démarche. Votre organisation pourra ainsi s'y référer dans le futur. Elle pourra connaître les raisons qui vous ont poussé à faire vos choix ou évitera de refaire la démarche complète inutilement.

Revoir la proportionnalité de votre solution

Après avoir terminé l'exercice de gestion des risques, refaites l'exercice d'évaluer la proportionnalité de votre projet par rapport aux risques qu'il fait toujours encourir aux personnes concernées (voir section 1.2).

À la lumière de l'ensemble de votre évaluation de facteurs relatifs à la vie privée, est-ce que la solution que vous proposez pour atteindre vos objectifs paraît toujours proportionnelle compte tenu de ces risques?

En cas de plaintes par une personne concernée ou de vérification par un organisme de contrôle, serez-vous prêt à démontrer qu'il s'agit d'une solution proportionnelle?

2.5. Faire le suivi de l'évaluation des facteurs relatifs à la vie privée

Établir votre plan d'action

La préparation d'un plan d'action permet d'assurer la mise en œuvre des stratégies et des moyens retenus.

L'insertion des différentes actions dans vos activités régulières concrétise l'EFVP et permet d'en retirer les bénéfices.

Identifier les responsables de la gestion des risques résiduels

Il est préférable d'identifier des personnes responsables de surveiller l'évolution des risques résiduels. Ces personnes seront aussi responsables de la gestion de l'événement s'il devait se concrétiser.

Informer vos autorités

Il est important que les hautes autorités de votre organisation soient tenues informées des résultats de l'EFVP. Elles doivent accepter les conclusions de votre analyse et cautionner les risques qui subsistent malgré les moyens déployés pour les atténuer.

À COMPLÉTER

- Description des moyens mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels
- Évaluation des risques
- Plan d'action

3. RÉDIGER UN RAPPORT D'ÉVALUATION

Le rapport est la dernière étape de votre processus de réflexion. Il devrait être simple et accessible : tout lecteur qui n'aurait pas été directement impliqué dans votre projet devrait pouvoir comprendre quel est le projet, comment ce projet est susceptible d'affecter la vie privée et comment vous avez considéré et mesuré les risques identifiés.

3.1. À quoi sert le rapport?

Un rapport d'EFVP sert **à consolider** les résultats de votre évaluation. Il permet d'attester de vos démarches et de votre réflexion dans le cas d'une vérification, d'une inspection ou d'une enquête par une autorité réglementaire.

Un **résumé** de votre rapport peut également être diffusé auprès de vos clients, de vos partenaires, de toute autre entité concernée, ou même au sein de votre organisation. Vous pouvez rendre ce résumé public en le publiant sur votre site Web. Le diffuser permet de :

- Faire preuve de transparence auprès des personnes qui font affaire avec votre organisation;
- Démontrer que vous avez pris en considération le respect de la vie privée dans l'élaboration et la mise en œuvre de votre projet.

3.2. Rédiger un rapport est-il obligatoire?

Non, sauf pour les organismes publics, dans certains cas précis prévus par la Loi sur l'accès. Faire une EFVP est alors obligatoire et requiert la rédaction et la diffusion d'un rapport.

Exemples de projets où une EFVP est exigée :

- Projets gouvernementaux visés par la Loi favorisant la transformation numérique de l'administration publique;
- Projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels en vertu du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (R.L.R.Q chapitre A-2.1, r.2).

Même si vous ne prévoyez pas faire de rapport, documenter votre EFVP au fur et à mesure vous permet de conserver une trace écrite de votre démarche. Si vous décidez finalement de rédiger un rapport, l'essentiel du travail aura été fait.

Garder une trace écrite est donc une bonne pratique, répandue dans plusieurs provinces canadiennes[22] et dans plusieurs pays[23].

3.3. Que devrait contenir le rapport?

L'essentiel de votre projet et le cadre dans lequel il s'inscrit

- La description de votre projet;
- Ce qui l'a motivé et les objectifs poursuivis;
- Toutes les parties prenantes au projet, en incluant la description de leur rôle et de leurs responsabilités : celles impliquées dans sa mise en œuvre et celles impliquées par la suite, c'est-à-dire les ressources de votre organisation, vos différents partenaires et votre clientèle;
- Les personnes ou secteurs de votre organisation qui seront responsables de gérer les risques résiduels[24];
- L'inventaire et la vue d'ensemble de la circulation des renseignements personnels impliqués;
- La description des moyens mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels
- La liste des risques identifiés;
- Vos stratégies, mécanismes et mesures de sécurité déployés pour éliminer ou réduire ces risques;
- Les personnes responsables de mettre en œuvre ces stratégies, mécanismes et mesures de sécurité;
- Un échéancier avec les mesures mises en place pour réévaluer périodiquement (**exemple** : un audit).

[22] En Alberta, par exemple, un rapport d'EFVP est obligatoire pour tout projet en matière de santé. (https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx).
[23] En Europe, une analyse d'impact relative à la protection des données (AIPD) est obligatoire quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Une mention de l'approbation de votre rapport par les hautes instances de votre organisation

Autrement dit, les détails de l'approbation du rapport, incluant les noms, les postes et les signatures des personnes l'ayant approuvé.

Des informations complémentaires sous forme d'annexes

- Une liste de vos politiques pertinentes en matière de gestion des renseignements personnels et de protection de la vie privée;
- Résumé des avis de sécurité produits en collaboration avec des fournisseurs ou partenaires (**exemple** : test d'intrusion);
- Certifications obtenues dans le cadre de votre projet (quand un organisme d'évaluation certifie que votre produit ou service est conforme à certaines exigences).

À COMPLÉTER

- Rapport d'EFVP

Commission
d'accès à l'information
du Québec

Guide d'accompagnement

Réaliser une évaluation des facteurs relatifs à la vie privée

Document mis à jour
le 10 mars 2021

Les informations incluses dans ce guide reflètent les lois avant leur modification par la Loi 25. Il sera révisé ultérieurement. Pour connaître les modifications apportées au régime de protection des renseignements personnels, qui entreront en vigueur en septembre 2022 et les années suivantes, nous vous invitons à consultez la section Espace évolutif - Modernisation des lois du site Web de la Commission.

Version de travail

Ce guide est appelé à évoluer. Il sera révisé à la lumière de l'adoption de la Loi 25, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels.* Il pourrait être remanié en profondeur.

La Commission vous invite tout de même à lui adresser tout commentaire ou suggestion. Veuillez les faire parvenir à l'adresse courriel suivante : veille@cai.gouv.qc.ca

INTRODUCTION

Le droit à la vie privée est un droit fondamental

Il est protégé par la *Charte des droits et libertés de la personne*[1]. Pour toute organisation[2], qu'elle soit entreprise du secteur privé ou organisme public, ce droit se traduit dans l'obligation de respecter l'intimité et la vie personnelle des personnes en minimisant les renseignements personnels qu'elle recueille, utilise, communique et conserve et dans l'obligation d'en assurer la confidentialité.

Le rythme effréné de l'innovation commande la vigilance.

Les normes et la législation peinent à suivre l'émergence continue et accélérée des nouvelles technologies. Leur adoption devient souvent un préalable à la rentabilité et à la survie des organisations. L'information, incluant les renseignements personnels, est une ressource de plus en plus prisée. Les technologies facilitent la collecte, le traitement et le stockage de renseignements personnels et peuvent impacter la vie privée des personnes.

La protection de la vie privée nous concerne tous.

À l'ère numérique, la responsabilité de veiller au respect de la vie privée ne repose plus seulement sur les épaules des institutions ou des citoyens. Elle incombe désormais à toutes les organisations, publiques comme privées.

Celles qui l'ont compris et qui agissent en conséquence diminuent leur chance de causer des préjudices aux personnes et d'avoir à gérer les contrecoups de ces problèmes (par exemple, des recours juridiques, offrir des compensations financières, des atteintes à la réputation de votre organisation, etc.). Elles sont aussi mieux perçues par le public et par les investisseurs[3].

---

[1] RLRQ, c. C-12, art. 5.

[2] Dans ce guide, les parties où le terme « organisation » est utilisé s'appliquent autant aux entreprises du secteur privé qu'aux organismes du secteur public. Le texte sera spécifique lorsque qu'il s'appliquera uniquement à l'un ou l'autre des secteurs.

[3] En 2018, **91 % des Québécois** accordaient de l'importance à la protection de leurs renseignements personnels et auraient fait davantage affaire avec une entreprise possédant une bonne réputation en la matière (sondage Léger Marketing réalisé pour la CAI) : https://www.cai.gouv.qc.ca/documents/CAI_Sondage_perception_2018.pdf)

Le processus dont il est question dans ce guide est donc non seulement un moyen de mener à bien une évaluation des facteurs relatifs à la vie privée, mais aussi l'occasion de démontrer que votre organisation se préoccupe de ces enjeux.

Ce guide a été conçu par la Commission d'accès à l'information du Québec (CAI).

La CAI veille à la promotion et au respect des droits des citoyens en ce qui concerne l'accès aux documents des organismes publics et la protection de leurs renseignements personnels[4].

Elle veille aussi au respect des lois :

- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[5] (Loi sur l'accès);
- La Loi sur la protection des renseignements personnels dans le secteur privé[6] (Loi sur le privé).

L'équipe de la CAI est à votre disposition pour répondre à vos questions générales concernant le présent guide. Elle ne donnera toutefois pas d'avis ou de conseils concernant l'analyse et l'évaluation des facteurs relatifs à la vie privée (EFVP) d'un projet particulier.

[4] Pour plus d'information, consultez le site Internet de la CAI : **www.cai.gouv.qc.ca**.
[5] RLRQ, c. A-2.1.
[6] RLRQ, c. P-39.1.

QUEL EST L'OBJECTIF DE CE GUIDE?

Ce guide a pour objectif de vous accompagner dans l'évaluation des risques liés à la vie privée si vous devez concevoir, développer ou exploiter :

- Un projet[7] ou une initiative impliquant des renseignements personnels[8];
- Un projet risquant d'avoir une incidence sur le respect de la vie privée des personnes.

Exemples de projets concernés pouvant impliquer la collecte, l'utilisation ou la communication des renseignements personnels :

- Développer un nouveau système d'information ou une technique de personnalisation d'un produit ou d'un service;
- Chercher une nouvelle clientèle, explorer de nouveaux marchés;
- Faire appel à un système d'algorithme ou d'intelligence artificielle;
- Installer un système de vidéosurveillance;
- Comparer différentes versions de bases de données ou de fichiers;
- Acquérir ou fusionner des organisations;
- Utiliser des empreintes digitales, la géolocalisation, un système de reconnaissance faciale, des objets connectés, des capteurs pour villes intelligentes, etc.

---

[7] Le terme **projet** réfère à toute activité au sein d'une organisation : mise en place ou modification d'un programme ou d'un service, recours à une technologie particulière, initiative publique, etc.

[8] Les **renseignements personnels** sont ceux qui concernent une personne physique et permettent de l'identifier (art. 54 de la Loi sur l'Accès et art. 2 de la Loi sur le privé). Sauf exception, ils sont confidentiels. Cette définition est la même pour les organisations publiques que pour les organisations privées, quel que soit le support ou le format (écrit, graphique, sonore, visuel, informatisé ou autre).

À QUI S'ADRESSE CE GUIDE?

À toute personne responsable de la conception, du développement ou de l'exploitation de projets au sein d'une organisation.

Principales personnes concernées : les responsables de la protection des renseignements personnels

Autres exemples de personnes impliquées :

- **Dans les petites entreprises du secteur privé**[9] **:** chefs d'entreprise, commerçants, artisans, travailleurs autonomes, responsables associatifs, etc.;
- **Dans les grandes entreprises privées :** responsables des affaires juridiques, responsables organisationnels de la gestion de risque, toute personne chargée de la sécurité des systèmes d'information, de l'éthique, de la gestion documentaire, etc.;
- **Dans les organisations du secteur public**[10] **:** responsables organisationnels de la sécurité de l'information (ROSI), responsables de la gestion documentaire (RGD), responsables de l'éthique (RE), responsables du développement ou de l'acquisition des systèmes d'information (RDASI), responsables de l'architecture de sécurité de l'information (RASI), responsables de la continuité des services (RCS), responsables de la gestion des technologies de l'information (RGTI), responsables de la sécurité physique (RSP), responsables organisationnels de la gestion de risque, responsables de la vérification interne (RVI), etc.

---

[9] Le terme **entreprise** réfère à l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services (art. 1525 du *Code civil du Québec* (CCQ-1991)). Cette définition s'étend notamment à l'entreprise individuelle (travailleur autonome), à la société par actions (compagnie), à la société en nom collectif (S.E.N.C.), à la société en commandite (S.E.C.), à la société en participation, à la personne morale sans but lucratif, au syndicat de copropriété, à l'association (p. ex. : syndicat), au groupement de personnes (p. ex. : consortium) ou à une fiducie exploitant une entreprise à caractère commercial.

[10] L'intitulé du poste peut varier.

QU'EST-CE QU'UNE ÉVALUATION DES FACTEURS DE RELATIFS À LA VIE PRIVÉE (EFVP)?

Un processus préventif

L'EFVP[11] est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques.

Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

Ces facteurs sont

- La conformité de votre projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient;
- L'identification des risques d'atteinte à la vie privée engendrés par votre projet et l'évaluation de leurs impacts;
- La mise en place de stratégies pour éviter ces risques ou les réduire efficacement.

Ce processus vise **d'abord** à protéger les personnes physiques concernées par ces renseignements. Il vise **aussi** la mise en place de mesures adéquates pour respecter vos obligations en matière de protection des renseignements personnels. Ainsi, l'EFVP permet d'éviter des problèmes que causerait une gestion inadéquate (plaintes, incidents de sécurité, poursuites judiciaires, atteinte à l'image, etc.).

Une bonne pratique évolutive

Dès que des renseignements personnels ou la vie privée des personnes sont concernés, réaliser une l'EFVP constitue une bonne pratique. Cependant, l'EFVP n'est efficace que si elle évolue de façon continue : elle doit être revue au besoin, tout au long de la vie du projet.

---

[11] En anglais, l'EFVP est connue sous l'expression *Privacy Impact Assessment* (PIA).

TABLE DES MATIÈRES

À COMPLÉTER

Vous rencontrerez ce symbole au cours de votre lecture.

Chacune de ses apparitions est une invitation à produire une section en vue de votre rapport d'EFVP.

1. PRÉPARER VOTRE ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

La première étape d'une EFVP consiste à vous poser les bonnes questions et à bien comprendre quels aspects de votre projet sont concernés.

1.1. Vous poser les bonnes questions avant de commencer

Êtes-vous obligé de faire une EFVP?

Faire une EFVP n'est pas obligatoire, sauf pour certains organismes publics (voir section 3.2 *Rédiger un rapport est-il obligatoire?*). Mais si votre projet implique la collecte, l'utilisation ou la communication de renseignements personnels, une EFVP est fortement recommandée.

Ne concluez pas trop rapidement qu'une EFVP est superflue sous prétexte que vous ne pensez pas utiliser de renseignements personnels. Des renseignements en apparence anodins peuvent, une fois croisés avec d'autres, révéler de l'information sur les personnes concernées.

En outre, un survol de votre projet pourrait révéler des enjeux insoupçonnés sur la vie privée des personnes visées par celui-ci..

Si vous décidez de ne pas réaliser d'EFVP, soyez en mesure d'expliquer et de justifier pourquoi vous ne le faites pas.

Si des changements sont apportés à un projet, vérifiez d'abord si une EFVP a déjà été faite et révisez-la pour rendre compte de ces changements.

Quand faire l'évaluation?

Vous devez commencer votre EFVP **au tout début de votre projet** plutôt qu'en fin de parcours :

- Pour pouvoir influencer son déroulement en cours de route
- Pour agir et choisir la solution qui protège et respecte le mieux la vie privée

Pour les projets de grande envergure, vous pouvez faire une EFVP préliminaire, plus courte et moins exhaustive, avant une EFVP complète.

Par exemple, certains projets requièrent des études d'opportunité, de préfaisabilité ou de faisabilité. Une EFVP préliminaire dans le cadre de ces études peut éviter d'engager des

frais pour des solutions qui pourraient s'avérer non conformes ou engendrer des enjeux disproportionnés pour les personnes par rapport à vos objectifs d'affaires.

Qu'allez-vous inclure dans votre évaluation?

Vous avez intérêt à délimiter clairement la portée de votre évaluation et à tenir votre analyse à un niveau adapté à votre projet.

Exemple 1 : Vous décidez de ne pas inclure la révision des procédures d'identification des personnes dans votre projet d'assistant virtuel en ligne. Vous jugez que cela n'a pas d'importance, car votre système actuel fonctionne bien avec votre service à la clientèle en personne et au téléphone. **Votre portée est peut-être trop étroite.** Des éléments importants pourraient manquer à votre évaluation, car une identification en ligne n'a peut-être pas les mêmes caractéristiques qu'une identification en personne ou au téléphone.

Exemple 2 : Pour le même projet, vous décidez finalement de revoir les procédures d'identification, l'hébergement des données de vos clients, les formulaires de confidentialité de vos employés du service à la clientèle et l'ensemble de vos infrastructures systèmes. **Votre portée est sans doute trop large.** Des évaluations distinctes pourraient sans doute être produites pour certains sous-processus.

Exemple 3 : Pour le même projet, vous ne faites que la révision de vos politiques et directives de service à la clientèle, sans vous attarder aux détails techniques de la solution logicielle que vous avez acquise ni aux procédures d'identification des personnes. **Votre analyse se situe peut-être à un trop haut niveau.** Vous manquerez sans doute des éléments importants qui existent au niveau de la solution logicielle ou des procédures d'identification.

En définissant clairement votre portée, vous aurez une meilleure idée des ressources à impliquer dans la réalisation de l'EFVP.

Vous devez être en mesure de justifier les limites que vous imposez à votre évaluation.

Exemple 4 : Pour le même projet, des EFVP distinctes ont récemment été produites par votre organisation concernant les procédures et les processus d'identification des personnes qui s'adressent au service à la clientèle. **Vous décidez de ne pas refaire cette partie d'analyse et vous analysez uniquement la partie qui s'ajoute concernant l'identification par l'assistant virtuel.** Vous l'indiquez clairement dans votre rapport afin d'informer les gens des limites que vous posez à votre évaluation.

Qui devriez-vous impliquer?

Principalement

- Les personnes responsables du projet;
- Les personnes au courant des bonnes pratiques en matière de respect de la vie privée, de protection des renseignements personnels et de sécurité de l'information;
- Les personnes responsables des affaires juridiques;
- Les autorités compétentes de votre organisation devant prendre position sur la gestion des risques à la fin de la démarche (voir section 3*)*.

Selon l'envergure du projet ou les impacts sur la vie privée

- Vos collègues de travail dans certains départements : ressources humaines, gestion de risques, gestion documentaire, affaires juridiques, relations avec la clientèle, etc.;
- Vos clients, partenaires corporatifs, sous-traitants, etc.

Devez-vous documenter votre démarche?

Vous avez tout avantage à le faire. Conservez une trace écrite de toute votre démarche.

En cas de problème ou de question en lien avec la vie privée ou avec la protection des renseignements personnels, votre documentation attestera du sérieux de votre réflexion.

1.2. Définir votre projet

Cette première étape de l'EFVP est surtout descriptive. L'objectif est de documenter les informations importantes pour vous permettre d'évaluer les risques et les moyens d'éliminer ou de réduire ces risques (voir sections 2.2, 2.3 et 2.4).

Présentez les grandes lignes de votre projet

- En quoi consiste-t-il?
- Quel était le contexte quand l'idée de ce projet est apparue?
- Quelle est/était la situation au moment de son lancement?
- Quel est l'échéancier de sa mise en œuvre?

Expliquez quels sont les objectifs qui motivent votre projet

Ces objectifs peuvent expliquer pourquoi vous devez mettre en place de nouvelles mesures ou pratiques impliquant la gestion des renseignements personnels.

Cet objectif doit être **légitime** et se rapporter à des **préoccupations réelles et justifiables**.

Exemples d'objectifs visés par un projet :

- Vouloir mieux connaître votre clientèle;
- Offrir un nouveau service public;
- Déployer sur le Web un service existant;
- Accroître la sécurité d'une installation;
- Contrer la fraude;
- Vous mettre en conformité avec la réglementation;
- Conserver votre compétitivité;
- Lancer une nouvelle branche d'affaires ou rechercher une nouvelle clientèle pour appuyer votre croissance;
- Offrir une expérience client plus agréable, plus intuitive et plus efficace en créant la nouvelle version d'une plateforme.

Privilégiez une solution proportionnée à vos objectifs et aux risques d'atteinte à la vie privée

L'évaluation de la proportionnalité doit être faite tout au long de l'évaluation des facteurs à la vie privée et de la mise en place de votre projet.

Votre solution sera proportionnelle si :

- Il existe un lien rationnel entre vos objectifs et la solution proposée, c'est-à-dire qu'il s'agit d'un moyen efficace d'atteindre l'objectif visé. Cette efficacité doit être basée sur des données concrètes et probantes;
- Que l'atteinte à la vie privée est minimale ou qu'il n'y a pas d'autres solutions efficaces moins intrusives;
- Que les avantages concrets surpassent les conséquences ou les préjudices pour les personnes concernées.

1.3. Établir le partage des rôles et des responsabilités

Identifiez les parties impliquées dans le projet

- Qui sont les intervenants au sein de votre organisation
- Quels sont leurs rôles et leurs responsabilité (en incluant les responsables de la protection des renseignements personnels et de la sécurité de l'information);
- Qui sont les intervenants extérieurs (par **exemple**, vos fournisseurs de services, vos partenaires, autres organisations que vous impliquées[12], etc.);
- Qui seront les utilisateurs de votre service et quelle clientèle sera impactée.

À COMPLÉTER

- Description du projet
- Description des rôles et responsabilités

1.4. Connaître vos obligations en matière de protection des renseignements personnels

Les obligations peuvent provenir de sources différentes. Cela dépend de la nature et de l'envergure de votre projet.

Identifier vos obligations et comprendre les enjeux qu'elles impliquent n'est pas une tâche facile. En cas de doute, **n'hésitez pas à consulter un juriste**.

Sur le plan provincial

Au Québec, l'utilisation de renseignements personnels est encadrée principalement par deux lois :

- La *Loi sur la protection des renseignements personnels dans le secteur privé*, qui s'applique aux **organisations du secteur privé** (entreprises et organismes à but non lucratif);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, qui s'applique aux **organisations du secteur**

[12] Pour les organismes publics, pensez à mentionner les autres organisations gouvernementales, sur les plans local, provincial, fédéral et international.

public (ministères et organismes gouvernementaux et municipaux, organismes des réseaux de la santé et de l'éducation).

Voici une liste non exhaustive de lois qui contiennent des particularités en matière de protection des renseignements personnels :

- Code civil (RLRQ, c. CCQ-1991);
- Loi sur les archives (RLRQ, c. A-21.1);
- Loi concernant la cadre juridique des technologies de l'information (RLRQ, c. C-1.1);
- Code des professions (RLRQ, c. C-26);
- Loi sur l'administration fiscale (RLRQ, c. A-6.002);
- Code de la sécurité routière (RLRQ, c. C-24.2);
- Loi sur la protection de la jeunesse (RLRQ, c. P-34.1);
- Loi sur les services de santé et les services sociaux (RLRQ, c. S-4.2);
- Loi sur l'assurance maladie (RLRQ, c. A-29).

Exemples de particularités et exceptions précisées dans des lois :

- La collecte et l'utilisation du numéro de permis de conduire et du numéro d'assurance maladie sont régies par des lois, des règlements ou des directives sectorielles[13];
- La gestion du consentement est particulière pour les mineurs et les personnes majeures inaptes;
- L'utilisation et la collecte de renseignements biométriques[14] sont régies de manière spécifique et complémentaire par la *Loi concernant la cadre juridique des technologies de l'information*.

[13] Pour plus d'information sur l'utilisation des pièces d'identité, veuillez vous référez aux fiches Pièces d'identité : citoyens et Pièces d'identité : entreprises.

[14] Pour obtenir plus d'information, voir la section Biométrie du site de la Commission. Voir également note de bas de page 18.

Sur le plan fédéral et à l'international

Le gouvernement fédéral et certaines provinces canadiennes possèdent leurs propres législations et réglementations en matière de protection des renseignements personnels. Si votre entreprise exerce ses activités dans une ou plusieurs autres provinces, assurez-vous de bien connaître les obligations qui découlent de leurs législations.

Rappelez-vous que les communications de renseignements personnels à l'extérieur du Québec et du Canada sont soumises à un encadrement particulier par les lois provinciales et fédérales.

Pour les activités à l'international, sachez que les lois peuvent différer beaucoup d'un pays à l'autre. De plus, des obligations supplémentaires pourraient s'appliquer à certaines catégories de renseignements personnels, notamment pour les renseignements sensibles.

Enfin, certaines législations ont une portée extraterritoriale. Elles s'appliquent si une organisation collecte, utilise, communique ou conserve des renseignements personnels de personnes se trouvant sur le territoire couvert par ces législations, même si cette organisation ne se trouve pas sur ce territoire, Le *Règlement général sur la protection des données* européen est un exemple. Le non-respect de ces législations s'accompagne parfois de lourdes sanctions financières.

Si vos services visent un marché ou des citoyens de l'étranger, informez-vous et considérez les impacts que ces lois pourraient avoir sur votre projet.

Pratiques corporatives

Votre organisation peut encadrer le traitement des renseignements personnels de diverses façons : par des politiques, des processus, des procédures, des méthodes de travail, un plan et un calendrier de conservation, etc.

Bien que de tels documents internes n'aient pas force de loi, il est important d'en tenir compte dans votre évaluation pour ne pas vous écarter des pratiques en vigueur dans votre organisation. Votre travail pourrait même vous permettre d'identifier des lacunes au sein de votre organisation.

Normes

Différentes normes internationales peuvent alimenter votre réflexion sur vos pratiques, par exemple certaines normes ISO ou la documentation produite par l'Union européenne ou l'Organisation de coopération et de développement économiques (OCDE). Consultez-les si vous cherchez à adopter les meilleures pratiques en matière de respect de la vie privée et de protection des renseignements personnels.

1.5. Repérer les renseignements personnels impliqués dans votre projet

Faire l'inventaire des renseignements personnels

Afin de bien évaluer la conformité de votre projet avec la législation applicable et les risques d'atteinte à la vie privée qu'il comporte, vous devez faire l'inventaire des renseignements personnels qu'il implique. Cela vous permettra, par exemple, de vous assurerez de ne recueillir ou d'utiliser que les renseignements personnels nécessaires.

Toutefois, cette liste exhaustive n'est pas nécessaire à toutes les étapes de l'évaluation.

Par exemple, dans le rapport, une liste faisant état de regroupement de renseignements personnels de même nature pourrait suffire.

Ces regroupements contiennent des renseignements personnels qui possèdent des caractéristiques communes et/ou qui sont regroupés afin d'accomplir une fonction ou atteindre un objectif.

Votre liste doit quand même prévoir une courte énumération du contenu de ces regroupements.

Exemples de regroupements de renseignements personnels :

- Renseignements d'identité et coordonnées de vos clients (nom, prénom, nom d'utilisateur, mot de passe);
- Dossiers médicaux, en version électronique et papier (résultats médicaux, résumés des rencontres, données de santé, imagerie médicale);
- Dossiers d'invalidité des employés détenus par les ressources humaines (renseignements d'identité, rapports médicaux, communications avec les assureurs);
- Courriels et enregistrements téléphoniques du centre d'appels (échanges avec les clients, contenu des questions et des réponses, échantillon de la voix);
- Données de journalisation du site Internet et outil d'analyse Web (historiques des pages consultés, adresse IP, navigateur et appareil utilisé, configuration de l'affichage).

Éléments à retenir

- Si vous n'êtes pas certain qu'un regroupement contient des renseignements personnels, conservez-le quand même dans votre liste et considérez-le dans votre EFVP.

- Incluez tous les renseignements que vous créez ou inférez sur les personnes (**exemples :** une cote de crédit, une note d'évaluation, une note dans un dossier). Ce sont des renseignements personnels.
- Pensez aux renseignements collectés automatiquement par les appareils et les systèmes informatiques que vous utilisez.
- Incluez les renseignements pseudonymisés[15], dépersonnalisés ou anonymisés[16] et agrégés[17] dans votre liste. Même si certains de ces renseignements ne sont plus directement reliés à l'identité d'une personne, les nouvelles technologies permettent bien souvent de rétablir ce lien. Il sera pertinent d'évaluer le risque de réidentification de ces renseignements.
- Même si vous ne présentez que regroupements dans le rapport d'évaluation, il est important que votre organisation soit en mesure de connaitre l'étendue de tous les renseignements personnels qu'elle détient.

Évaluer le degré de sensibilité de ces renseignements

Un renseignement est dit « sensible », soit parce qu'il révèle quelque chose d'intime, d'unique ou si sa révélation ou son utilisation peut causer des conséquences négatives pour la personne.

La Loi sur l'accès et la Loi sur le privé reconnaissent cette distinction. Elles prévoient notamment que les mesures de sécurité soient adaptées à la sensibilité des renseignements.

Exemples de renseignements sensibles :

- Renseignements concernant le groupe ethnique ;
- Renseignements concernant les croyances philosophiques ou religieuses;
- Renseignements concernant la santé ou l'orientation sexuelle;
- Renseignements financiers;

---

[15] Des renseignements sont pseudonymisés si les informations qui identifient directement les personnes (**p. ex.** nom, prénom) sont remplacées par des informations qui les identifient de façon indirecte (**p. ex.** no de dossier).
[16] Des renseignements sont dépersonnalisés ou anonymisés s'il est impossible d'identifier une personne à partir du jeu de données. La garantie d'anonymat est obtenue à la suite de l'application d'une ou de plusieurs méthodes. L'anonymisation doit être irréversible.
[17] Des renseignements sont agrégés lorsque plusieurs données de même type sont regroupées (**p. ex.** statistiques), ce qui rend impossible l'identification d'un individu donné.

- Renseignements biométriques[18],
- Identifiants uniques[19].

1.6. Identifier les points où votre organisation entre en interaction avec les renseignements personnels

Les points d'interactions peuvent être

- Les personnes, les ensembles de personnes ou les partenaires et tiers qui accèdent aux renseignements personnels (**exemples :** employés, clientèle, sous-traitants, firmes de consultation, chercheurs externes, équipes d'entretien de bâtiments ou de systèmes informatiques, fournisseurs de télécommunication);
- Les moyens utilisés pour collecter des renseignements personnels (**exemples** : formulaires d'abonnement, boîtes courriel, messageries téléphoniques, plateformes collaboratives, sondages, questionnaires);
- Les moyens utilisés pour communiquer des renseignements personnels (**exemples :** prestations électroniques de service, échanges par courriel, service à la clientèle, sites Web, interfaces d'échange informatisées [API] ou liens électroniques sécurisés);
- Les moyens utilisés pour traiter et conserver des renseignements personnels (**exemples:** systèmes informatiques, services infonuagiques, copies de sauvegarde, outils de télécommunication, salles et classeurs d'entreposage des dossiers papier).

Dégager une vue d'ensemble de la circulation des renseignements personnels tout au long de votre projet

À partir des points d'interaction que vous avez identifiés, illustrez le parcours des renseignements personnels tout au long du processus visé par votre projet.

---

[18] Les renseignements biométriques sont des renseignements portant sur les caractéristiques biologiques ou comportementales d'une personne. Ils sont généralement destinés à déterminer son identité (**p. ex.** empreintes digitales, forme du visage, empreinte de l'iris, empreinte de la voix, démarche, signature, renseignements génétiques).
[19] Un identifiant unique est une information qui permet de distinguer un individu dans un ensemble (**p. ex.** un numéro de client ou d'employé).

Cette vue d'ensemble peut être décrite et/ou schématisée. Le schéma est une façon simple et avantageuse de présenter l'information en un coup d'œil.

Cette description ou ce schéma sera plus complexe pour les grands projets, de sorte qu'un découpage par processus pourrait s'avérer préférable.

Identifier les particularités de chaque phase de votre projet

La **phase de développement** de votre projet peut comporter des risques en matière de vie privée qui sont différents de ceux qui existeront dans la **phase d'exploitation** :

- Phase de **développement** : votre projet prend forme, vous élaborez des solutions pour résoudre les problèmes qui émergent. Des personnes interviennent ponctuellement durant cette phase (par exemple, des consultants). Vous faites des périodes d'essais sur différents produits. Le projet peut être modifié en cours de route.
- Phase d'**exploitation** : votre projet est vivant, vous veillez à ce qu'il produise les résultats escomptés. Des événements peuvent survenir spécifiquement durant cette phase, comme des mises à jour du système. Des employés peuvent quitter votre entreprise. Des personnes peuvent vous faire des demandes d'accès à l'information.

Exemple 1 : Je suis directeur commercial d'une entreprise qui fabrique des vêtements sur mesure. J'aimerais proposer un outil de commande en ligne disponible pour mes clients.

Une firme spécialisée sera embauchée durant **la phase de développement**. Je dois prévoir que ces consultants entreront en contact avec certains renseignements concernant mes vendeurs et mes clients tout au long de la mise en place du système. Cependant, ils n'y auront plus accès un certain temps après la mise en service du système, lors de la **phase d'exploitation**. De plus, je dois considérer que les risques de bogues informatiques seront plus élevés durant cette période. Que dois-je prévoir pour réduire les risques?

Exemple 2 : Je suis directrice des ressources humaines d'une grande organisation gouvernementale. Je vais faire changer le logiciel de gestion des ressources humaines. Le fournisseur du logiciel m'avise que le système est mis à jour fréquemment et m'informe que des refontes plus importantes sont à prévoir dans la prochaine année. Je dois anticiper ces éventuelles refontes qui arriveront en **phase d'exploitation**. Je dois mettre des moyens en place afin que ces opérations de maintenance n'aient pas d'incidence sur les données personnelles des employés.

À COMPLÉTER

- Inventaire des renseignements personnels impliqués
- Vue d'ensemble de la circulation des renseignements

2. ANALYSER ET ÉVALUER LES FACTEURS RELATIFS À LA VIE PRIVÉE

Cette étape est l'essence de la démarche. Il s'agit de considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

Ces facteurs sont :

- La conformité de votre projet à la législation applicable à la protection des renseignements personnels et le respect des principes qui l'appuient;
- L'identification des risques d'atteinte à la vie privée engendrés par votre projet et l'évaluation de leurs impacts;
- La mise en place de stratégies pour éviter ces risques ou les réduire efficacement.

2.1. Respecter les obligations et les principes de protection des renseignements personnels

Posez-vous les questions suivantes :

- Respectez-vous les obligations et les principes de protection des renseignements personnels pour chacune des catégories de renseignements personnels, à chacun des points d'interaction et tout au long du cycle de vie des renseignements?
- Sinon, quelles sont les modifications que vous devriez apporter à votre projet pour que vos obligations et les principes soient respectés?

Documentez les moyens qui sont mis en place pour respecter vos obligations et ces différents principes.

En cas de doute concernant le respect de vos obligations légales, **n'hésitez pas à consulter un juriste**.

Pour **les entreprises du secteur privé**, les principes applicables sont les suivants :

- **Déterminer les fins de la collecte :** Vous devez avoir un intérêt sérieux et légitime pour constituer un dossier sur une personne.
- **Limiter la collecte de renseignements personnels :** Vous devez collecter uniquement les renseignements nécessaires pour offrir votre bien ou votre

service. Votre collecte doit se faire par des moyens licites. Sauf exception, la collecte doit se faire auprès de la personne concernée.

- **Informer la personne concernée :** Avant de constituer un dossier, vous devez informer la personne concernée des finalités du dossier, de l'utilisation qui sera faite des renseignements personnels, des catégories de personnes qui y auront accès au sein de votre entreprise et de l'endroit où ils seront détenus. Vous devez également informer les personnes concernées des droits d'accès et de rectification qui leur sont accordés par la Loi sur le privé. Vous devez inscrire quel est l'objet du dossier.
- **Mettre en place des mesures de sécurité appropriées :** Vous devez prendre les mesures de sécurité propre à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- **Limiter l'accès aux renseignements personnels :** Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour le recevoir au sein de l'entreprise lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions.
- **Limiter l'utilisation de renseignements personnels :** Vous devez obtenir le consentement de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli, à moins d'une exception prévue par la loi.
- **Obtenir le consentement à communiquer des renseignements personnels :** Vous devez obtenir le consentement de la personne concernée pour communiquer ses renseignements à autrui, à moins d'une exception prévue par la Loi sur le privé;
- **Requérir le consentement des personnes concernées :** À moins d'une exception prévue par la Loi sur le privé, vous devez obtenir le consentement de la personne concernée avant de collecter auprès d'un tiers, d'utiliser ou de communiquer des renseignements personnels. Ce consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. De plus, il ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles vous l'avez demandé.
- **Assurer la qualité des renseignements personnels :** Vous devez veiller à ce que les renseignements personnels que vous détenez soient à jour et exacts au moment où vous les utilisez pour prendre une décision relative à la personne concernée.

- **Permettre l'exercice des droits d'accès et de rectification :** Un renseignement personnel doit pouvoir être accessible et rectifié par la personne concernée.
- **Répondre avec diligence :** Vous devez répondre avec diligence aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées.

Pour les organisations du secteur public, les principes applicables sont les suivants :

- **Assumer vos responsabilités** : Chaque organisme public a la responsabilité d'assurer le caractère confidentiel des renseignements personnels qu'il détient.
- **Déterminer les fins de la collecte de renseignements personnels :** Avant d'entreprendre toute collecte d'information, vous devez définir les raisons pour lesquelles vous comptez recueillir et utiliser un renseignement personnel.
- **Limiter la collecte de renseignements personnels :** Vous ne pouvez recueillir que les seuls renseignements personnels nécessaires à l'exercice des attributions de votre organisme ou à la mise en œuvre d'un programme dont il a la gestion.
- **Informer la personne concernée :** Vous avez l'obligation d'informer adéquatement la personne concernée avant qu'elle vous fournisse les renseignements personnels attendus.
- **Limiter l'accès aux renseignements personnels :** La Loi sur l'accès prévoit qu'un renseignement personnel ne sera accessible qu'aux seules personnes ayant la qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de leurs fonctions.
- **Requérir le consentement des personnes concernées** : Un renseignement personnel demeure inaccessible tant que la personne concernée n'a pas consenti à sa divulgation[20].
- **Assurer la qualité des renseignements personnels :** Un renseignement personnel doit être maintenu à jour, être exact et complet afin de servir adéquatement aux fins pour lesquelles il a été recueilli ou est utilisé.

[20] Certaines exceptions précisées par la Loi sur l'accès autorisent la communication de renseignements personnels sans le consentement préalable des personnes concernées.

- **Mettre en place des mesures de sécurité appropriées :** Vous devez prendre les mesures de sécurité propre à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.
- **Permettre l'exercice des droits d'accès et de rectification :** Un renseignement personnel doit pouvoir être accessible et rectifié par la personne concernée.
- **Limiter la durée de conservation des renseignements personnels :** Vous êtes tenus de détruire irréversiblement tout renseignement personnel lorsque l'objet pour lequel il a été recueilli est accompli.
- **Répondre dans les délais légaux :** Vous devez répondre aux demandes d'accès aux renseignements personnels et de rectification soumises par les personnes concernées dans les vingt jours suivant leur réception.

2.2. Repérer et décrire les risques sur la vie privée engendrés par votre projet

Qu'est-ce qu'un risque? Il s'agit d'une situation ou d'un évènement futur qui peut ou non se réaliser et qui causerait une perte ou un préjudice. Le risque est une *menace potentielle*.

Un **risque sur la vie privée** consiste en un événement qui causerait une perte ou un préjudice à une personne au niveau du respect de son intimité ou de sa vie personnelle.

Dans ce cas-ci, la perte ou le préjudice n'a pas besoin d'être tangible : les effets de l'atteinte à la vie privée peuvent être manifestes et externes (**exemple :** en cas de dommage à la réputation), où être vécues de l'intérieur par les personnes concernées (**exemple** : sentiment d'intrusion).

Dans ce contexte, certains aspects d'un projet qui sont conformes du point de vue légal peuvent quand même être perçus comme une atteinte à la vie privée par les personnes concernées.

Faire la gestion des risques dans le cadre de l'EFVP

Cela consiste à recenser les risques auxquels votre organisation est exposée, puis à définir et à mettre en place des mesures préventives appropriées en vue de supprimer ou d'en atténuer les conséquences.

Vous devez donc établir des scénarios de tels événements qui pourraient découler de la mise en œuvre de votre projet et d'estimer les impacts potentiels sur la vie privée des personnes concernées par ces événements.

Posez-vous les questions suivantes :

- Quels sont les situations ou les événements qui peuvent raisonnablement survenir pour chacun des renseignements personnels, à chacun des points d'interaction, tout au long du cycle de vie des renseignements?
- Quels sont les situations ou les événements qui pourraient engendrer une perte ou un préjudice pour les personnes concernées du point de vue du respect de leur vie privée?

Dressez la liste des réponses que vous donnerez à ces questions et décrivez brièvement ces situations.

Exemples de risques sur la vie privée :

- Conservation de renseignements lorsque leur utilité n'est plus démontrée;
- Vol de renseignements personnels;
- Collecte excessive de renseignements;
- Divulgation non autorisée de renseignements personnels;
- Réidentification de renseignements préalablement anonymisés;
- Manque d'information fournie aux individus lors de la collecte;
- Création excessive ou non justifiée d'informations;
- Objectif du projet pas suffisamment important ou non légitime;
- Intrusion dans la vie privée disproportionnée par rapport à l'objectif visé par le projet.

Votre organisation a peut-être déjà en main des avis juridiques ou les résultats d'analyses de sécurité informatique. Si des risques de non-conformité ou des risques en matière de sécurité de l'information ont été abordés dans ces documents, vous pouvez vous en inspirez pour produire votre EFVP.

Décrire et évaluer les impacts potentiels

Chacun des risques peut causer des impacts qu'il convient de décrire, puis d'évaluer.

Les **impacts potentiels** sont variés :

- vol d'identité et fraudes;
- dangers sur la vie et sur la sécurité des personnes (comme les possibilités de harcèlement);
- pertes financières ou d'opportunités;
- dommage à la réputation;
- sollicitation non désirée; et
- Intrusions et autres nuisances dans la vie privée des personnes.

Les considérations en lien avec les dommages à la réputation de votre organisation, les coûts potentiels que l'événement pourrait vous faire encourir, les litiges qui pourraient s'en suivre ou toute autre conséquence négative portée à votre organisation ne doivent pas entrer en ligne de compte dans votre évaluation des impacts sur la vie privée des personnes concernées.

Identifier les causes de ces risques

Précisez quelles seraient les causes de ces situations.

Les **causes potentielles** sont également variées :

- un processus déficient;
- des erreurs dans la manipulation des renseignements;
- un manque de connaissances ou de formation;
- des mécanismes de surveillance insuffisants ou inexistants;
- une distribution inadéquate des responsabilités;
- des comportements malveillants;
- une collecte excessive de renseignements;
- des technologies défaillantes ou désuètes;
- l'utilisation non justifiée ou non nécessaire de renseignements sensibles;
- l'absence de consentement;
- l'existence d'un moyen alternatif moins intrusif et suffisamment efficace pour atteindre l'objectif visé.

Tenez compte de certaines particularités

Projets impliquant de nouvelles technologies

Certaines technologies soulèvent des enjeux particuliers et les technologies émergentes suscitent des questions parfois inédites.

Pour évaluer adéquatement les risques qu'une technologie comporte, il est essentiel de bien la connaître avant de la déployer, surtout si celle-ci n'a jamais été utilisée auparavant.

L'utilisation de données biométriques est un exemple de technologies qui suscitent des questions et des enjeux particuliers[21].

Demandez l'aide de spécialistes si vous ne pouvez pas effectuer une évaluation adéquate par vous-même.

Projets d'envergure

Les grands projets génèrent davantage de risques, car ces risques peuvent toucher davantage de personnes.

Pour les projets comportant plusieurs phases, il peut être avantageux ou nécessaire de produire une EFVP pour chacune d'elle. L'environnement et les risques de chacune des phases seront différents.

Pour les projets s'échelonnant sur de longues périodes, une mise à jour régulière de l'EFVP peut être profitable pour le bon déroulement du projet.

Projets comportant des enjeux éthiques

Certains types de projets exigent qu'une évaluation soit produite par un comité d'éthique. C'est notamment le cas des recherches scientifiques portant sur des humains. Des recommandations en lien avec la protection de la vie privée sont parfois émises par ces comités. Celles-ci devraient normalement être considérées dans vos évaluations.

Des rapports d'évaluation éthique des nouvelles technologies sont fréquemment diffusés par des organismes indépendants ou des chercheurs universitaires. Ces documents abordent bien souvent des questions de vie privée. Ce sont des sources d'information pertinentes pour réfléchir aux enjeux et aux risques générés par les projets technologiques.

---

[21] Pour toute information concernant l'utilisation de systèmes biométriques, veuillez-vous référer au guide produit par la Commission intitulé Biométrie : principes à respecter et obligations légales des organisations. à ce sujet

2.3. Évaluer l'impact des risques identifiés

Se doter d'une méthode pour qualifier les risques

Il n'y a pas de méthode prescrite pour qualifier ou évaluer les risques ni pour présenter les résultats de votre analyse. Néanmoins, une évaluation en fonction de l'impact potentiel d'un événement et de la probabilité qu'il se concrétise peut répondre aux objectifs de l'EFVP.

L'évaluation des risques est un processus subjectif, il est souvent utile de constituer un comité pour tenir cette activité.

Si des pratiques en matière de gestion de risques sont en vigueur dans votre organisation, privilégiez-les.

Évaluer l'impact de chacun des risques identifiés

L'appréciation de l'impact peut se faire à l'aide d'un système de cotes.

Exemple d'un système de cotes pour apprécier **l'impact d'un risque** :

- Très faible et/ou inexistant (1) : le risque n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne;
- Faible (2) : le risque engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes;
- Grand (3) : le risque engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes;
- Très grand (4) : le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes;
- Inacceptable (non coté) : le risque engendre des conséquences trop importantes et/ou implique une non-conformité aux lois.

L'évaluation de l'impact peut être influencée par certaines variables

- La quantité de renseignements impliqués;
- La nature et la sensibilité des renseignements impliqués;
- La gravité et la nature des préjudices qui pourraient être causés aux personnes (**exemples :** impacts sévères sur la vie personnelle ou professionnelle, sur les

finances, procédures juridiques pour résoudre la situation, mettre en danger la vie de la personne);

- Le nombre de personnes touchées potentiellement ou le profil de ces personnes (**exemples :** enfants, personnes en situation de handicap, immigrants).

Estimer la probabilité que les risques se réalisent

Votre estimation peut aussi se faire à l'aide d'un système de cotes.

Exemple d'un système de cote pour évaluer **les probabilités** :

- Très faible et/ou inexistant (1) : Le risque n'a aucune chance de se concrétiser;
- Faible (2) : le risque a peu de chance de se concrétiser ou un événement similaire ne s'est jamais produit;
- Grand (3) : le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelque reprises;
- Très grand (4) : le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises

Considérant que le risque zéro n'existe pas, cette estimation peut être très difficile à faire. Soyez réaliste : évitez d'être trop confiant ou trop conservateur.

Considérer les stratégies et moyens de contrôle existants

Votre organisation peut déjà avoir mis en place des outils, des politiques, des directives, des procédures ou d'autres moyens pour atténuer ou éliminer le risque sans que des mesures supplémentaires n'aient été adoptées.

Listez-les et réévaluez les risques à la lumière de ces informations.

Déterminer le seuil acceptable de tolérance pour chaque risque

Mettez-vous dans la peau des personnes concernées et demandez-vous comment elles pourraient s'attendre à ce que leurs renseignements personnels soient utilisés et protégés.

Fixez-vous des seuils à atteindre selon ce qui pourrait paraître acceptable pour ces personnes.

Vous devez établir ces seuils en tenant compte du contexte de votre projet. Par exemple, une personne qui fournit des renseignements médicaux a des attentes différentes envers un centre hospitalier qu'envers des publicitaires.

2.4. Éliminer ou réduire les risques d'atteintes à la vie privée

Étudier les stratégies envisageables pour éliminer ou réduire les risques

Les stratégies peuvent chercher à réduire, soit l'impact du risque, soit les chances que ce dernier se concrétise, soit les deux en même temps.

Ainsi, réduire la quantité de renseignements personnels que vous collectez réduit l'impact d'un vol de données. L'ajout de mesures de sécurité réduit plutôt les probabilités qu'il se réalise.

Exemples de stratégies :

- Prévoir une révision périodique des différentes collectes de renseignements personnels;
- Mettre en place un système de gestion documentaire qui permet l'application automatisée du calendrier de conservation;
- Revoir les processus d'attribution et de gestion des accès informatiques;
- Engager des firmes de sécurité informatique pour revoir périodiquement les paramètres de sécurité de la prestation électronique de service;
- Revoir les clauses des contrats en matière de confidentialité;
- Établir un calendrier de formation et d'activités de sensibilisation pour vos employés;
- Faire une campagne d'information concernant votre nouvelle utilisation des renseignements personnels;
- Journaliser les accès et exploiter les journaux pour détecter les anomalies;
- Dépersonnaliser ou anonymiser les renseignements si leur utilisation sous une forme nominative n'est pas requise pour tous.

Choisir les stratégies à adopter

Déterminez quelles stratégies et quels moyens vous mettrez en place pour éliminer ou réduire un risque.

Ce choix ne peut se faire sans tenir compte de la réalité de votre projet et de votre organisation ainsi que des ressources à votre disposition. Songez à des solutions réalisables pour votre organisation.

Réévaluer le niveau de chacun des risques

À la lumière des stratégies et moyens retenus, réévaluez le niveau d'impact du risque et la probabilité qu'il se concrétise.

Vérifiez si vous avez atteint le seuil de tolérance que vous vous étiez fixé. Si le seuil n'est pas atteint, réévaluez votre choix de stratégies ou de moyens.

Si après avoir revu votre choix, vous ne parvenez toujours pas à éliminer un risque important ou que le seuil de tolérance que vous vous étiez fixé n'est pas atteint*, pensez à revoir en profondeur cet aspect de votre projet ou à le retirer.*

Tout risque qui persiste à la fin, une fois que vous avez pris les mesures visant à diminuer ou éliminer les risques identifiés au départ, devient un **risque résiduel**.

Il est possible que des risques d'atteinte à la vie privée subsistent même après avoir éliminé ou minimisé la plupart d'entre eux. Votre organisation doit néanmoins être en mesure d'assumer la responsabilité des risques résiduels qu'elle fait encourir aux personnes concernées.

Un conseil

Même si un risque est complètement éliminé ou qu'une stratégie n'est pas retenue, vous gagnez à garder des traces de votre démarche. Votre organisation pourra ainsi s'y référer dans le futur. Elle pourra connaître les raisons qui vous ont poussé à faire vos choix ou évitera de refaire la démarche complète inutilement.

Revoir la proportionnalité de votre solution

Après avoir terminé l'exercice de gestion des risques, refaites l'exercice d'évaluer la proportionnalité de votre projet par rapport aux risques qu'il fait toujours encourir aux personnes concernées (voir section 1.2).

À la lumière de l'ensemble de votre évaluation de facteurs relatifs à la vie privée, est-ce que la solution que vous proposez pour atteindre vos objectifs paraît toujours proportionnelle compte tenu de ces risques?

En cas de plaintes par une personne concernée ou de vérification par un organisme de contrôle, serez-vous prêt à démontrer qu'il s'agit d'une solution proportionnelle?

2.5. Faire le suivi de l'évaluation des facteurs relatifs à la vie privée

Établir votre plan d'action

La préparation d'un plan d'action permet d'assurer la mise en œuvre des stratégies et des moyens retenus.

L'insertion des différentes actions dans vos activités régulières concrétise l'EFVP et permet d'en retirer les bénéfices.

Identifier les responsables de la gestion des risques résiduels

Il est préférable d'identifier des personnes responsables de surveiller l'évolution des risques résiduels. Ces personnes seront aussi responsables de la gestion de l'événement s'il devait se concrétiser.

Informer vos autorités

Il est important que les hautes autorités de votre organisation soient tenues informées des résultats de l'EFVP. Elles doivent accepter les conclusions de votre analyse et cautionner les risques qui subsistent malgré les moyens déployés pour les atténuer.

À COMPLÉTER

- Description des moyens mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels
- Évaluation des risques
- Plan d'action

3. RÉDIGER UN RAPPORT D'ÉVALUATION

Le rapport est la dernière étape de votre processus de réflexion. Il devrait être simple et accessible : tout lecteur qui n'aurait pas été directement impliqué dans votre projet devrait pouvoir comprendre quel est le projet, comment ce projet est susceptible d'affecter la vie privée et comment vous avez considéré et mesuré les risques identifiés.

3.1. À quoi sert le rapport?

Un rapport d'EFVP sert **à consolider** les résultats de votre évaluation. Il permet d'attester de vos démarches et de votre réflexion dans le cas d'une vérification, d'une inspection ou d'une enquête par une autorité réglementaire.

Un **résumé** de votre rapport peut également être diffusé auprès de vos clients, de vos partenaires, de toute autre entité concernée, ou même au sein de votre organisation. Vous pouvez rendre ce résumé public en le publiant sur votre site Web. Le diffuser permet de :

- Faire preuve de transparence auprès des personnes qui font affaire avec votre organisation;
- Démontrer que vous avez pris en considération le respect de la vie privée dans l'élaboration et la mise en œuvre de votre projet.

3.2. Rédiger un rapport est-il obligatoire?

Non, sauf pour les organismes publics, dans certains cas précis prévus par la Loi sur l'accès. Faire une EFVP est alors obligatoire et requiert la rédaction et la diffusion d'un rapport.

Exemples de projets où une EFVP est exigée :

- Projets gouvernementaux visés par la Loi favorisant la transformation numérique de l'administration publique;
- Projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels en vertu du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (R.L.R.Q chapitre A-2.1, r.2).

Même si vous ne prévoyez pas faire de rapport, documenter votre EFVP au fur et à mesure vous permet de conserver une trace écrite de votre démarche. Si vous décidez finalement de rédiger un rapport, l'essentiel du travail aura été fait.

Garder une trace écrite est donc une bonne pratique, répandue dans plusieurs provinces canadiennes[22] et dans plusieurs pays[23].

3.3. Que devrait contenir le rapport?

L'essentiel de votre projet et le cadre dans lequel il s'inscrit

- La description de votre projet;
- Ce qui l'a motivé et les objectifs poursuivis;
- Toutes les parties prenantes au projet, en incluant la description de leur rôle et de leurs responsabilités : celles impliquées dans sa mise en œuvre et celles impliquées par la suite, c'est-à-dire les ressources de votre organisation, vos différents partenaires et votre clientèle;
- Les personnes ou secteurs de votre organisation qui seront responsables de gérer les risques résiduels[24];
- L'inventaire et la vue d'ensemble de la circulation des renseignements personnels impliqués;
- La description des moyens mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels
- La liste des risques identifiés;
- Vos stratégies, mécanismes et mesures de sécurité déployés pour éliminer ou réduire ces risques;
- Les personnes responsables de mettre en œuvre ces stratégies, mécanismes et mesures de sécurité;
- Un échéancier avec les mesures mises en place pour réévaluer périodiquement (**exemple** : un audit).

[22] En Alberta, par exemple, un rapport d'EFVP est obligatoire pour tout projet en matière de santé. (https://www.oipc.ab.ca/action-items/privacy-impact-assessments.aspx).
[23] En Europe, une analyse d'impact relative à la protection des données (AIPD) est obligatoire quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Une mention de l'approbation de votre rapport par les hautes instances de votre organisation

Autrement dit, les détails de l'approbation du rapport, incluant les noms, les postes et les signatures des personnes l'ayant approuvé.

Des informations complémentaires sous forme d'annexes

- Une liste de vos politiques pertinentes en matière de gestion des renseignements personnels et de protection de la vie privée;
- Résumé des avis de sécurité produits en collaboration avec des fournisseurs ou partenaires (**exemple** : test d'intrusion);
- Certifications obtenues dans le cadre de votre projet (quand un organisme d'évaluation certifie que votre produit ou service est conforme à certaines exigences).

À COMPLÉTER

- Rapport d'EFVP

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE :
SAVOIR DÉTECTER ET ATTÉNUER LES RISQUES D'ATTEINTE AUX RENSEIGNEMENTS PERSONNELS

#FicheInfo

L'évaluation des facteurs relatifs à la vie privée, ci-après appelée « EFVP », est un processus permettant de déterminer si certains projets impliquant l'utilisation de renseignements personnels posent des risques en matière de protection de la vie privée[1].

Les EFVP permettent de détecter ces risques et de proposer des solutions visant à les éliminer ou les minimiser. L'EFVP devrait être réalisée[2] dès lors que sont envisagés la mise en place d'un projet, le développement d'un système d'information ou le recours à de nouvelles technologies qui pourraient comporter des risques du fait de la collecte, de l'utilisation et, plus globalement, de la gestion de renseignements personnels.

Pour tirer tous les bénéfices de l'EFVP, celle-ci doit être réalisée **en amont** du projet et **impliquer toutes les parties** prenantes au sein de l'entreprise ou de l'organisme public. L'EFVP aide à élaborer un projet en conformité avec les lois de protection des renseignements personnels, tout en minimisant les risques d'atteinte à la vie privée des personnes concernées.

Constitue un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier

(article 54 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et article 2 de la *Loi sur la protection des renseignements personnels dans le secteur privé)*

QU'EST-CE QU'UNE EFVP ?

C'est un outil d'analyse pratique pour :

- déterminer si un projet est susceptible d'avoir des répercussions sur les renseignements personnels des personnes concernées par le projet;
- vérifier si le projet est conforme aux lois de protection des renseignements personnels;
- procéder à des ajustements afin de minimiser les risques et maximiser la protection des renseignements personnels;
- servir de document de référence si le projet évolue ou lors d'une vérification ou d'une inspection de la part des autorités de contrôle;
- agir de manière transparente dans la gestion des renseignements personnels[3].

Une EFVP permet d'identifier de façon préventive les problèmes les plus importants en matière de protection des renseignements personnels et de trouver des solutions réfléchies et opérationnelles ainsi que des possibilités d'amélioration dès la conception d'un projet.

[1] L'EFVP, connue en anglais sous l'expression *privacy impact assessment* ou *PIA*, est un outil reconnu et utilisé à l'échelle mondiale, tout comme le principe de prise en compte de la protection des renseignements personnels dès la conception d'un projet et à toutes ses étapes ultérieures (*privacy by design*).

[2] La rédaction d'une EFVP est exigée dans certains cas, par exemple dans le cas décrit à l'alinéa 2, paragraphe 2 de l'article 7 du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels.

[3] Plusieurs organisations diffusent, en ligne, les EFVP ou un résumé de celles-ci. Certaines législations prévoient l'envoi d'une copie de certaines EFVP à l'organisme qui surveille l'application de la loi.

Commission d'accès à l'information du Québec

POURQUOI EST-IL IMPORTANT DE PRENDRE EN CONSIDÉRATION LES ENJEUX DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS SES PRATIQUES OPÉRATIONNELLES?

Les personnes, que ce soit les citoyens, les clients, les consommateurs, etc., sont soucieuses de la façon dont leurs renseignements personnels sont gérés et acceptent de les confier à des entreprises ou des organismes publics qui ont le souci de la protection des renseignements personnels et qui font la preuve de leurs efforts en la matière, notamment grâce à une EFVP.

Ainsi, à l'objectif de conformité avec les lois de protection des renseignements personnels et de minimisation des conséquences sur la vie privée des personnes concernées s'ajoutent d'autres avantages essentiels :

- des économies de temps et d'argent;
- une hausse de la confiance des personnes dont les renseignements personnels sont collectés et/ou utilisés;
- un avantage concurrentiel dans un environnement d'affaires.

QUELS TYPES DE RISQUES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS UNE EFVP PEUT-ELLE DÉTECTER?

Une EFVP peut identifier des problématiques telles qu'une collecte non nécessaire de renseignements personnels, une sécurisation inappropriée de ceux-ci, une communication à des tiers non autorisée par la loi, une information insuffisante fournie aux personnes concernées, une utilisation secondaire des renseignements non autorisée, etc.

QUELS TYPES DE PROJETS DEVRAIENT FAIRE L'OBJET D'UNE EFVP?

La réalisation d'une EFVP est pertinente dès qu'une entreprise ou qu'un organisme public envisage de mettre en place ou de modifier un projet et ce, peu importe son envergure, impliquant des renseignements personnels. En voici quelques exemples :

- confier l'hébergement des données clients sur le serveur externe d'un fournisseur;
- analyser des données massives de clients à des fins de marketing;
- changer une politique publique ou une législation qui implique la collecte et l'utilisation de renseignements personnels;
- mettre en place une technologie susceptible d'affecter la vie privée des citoyens (vidéosurveillance, drones qui captent des images dans des lieux publics, radars photo, mouchards sur un site Internet, etc.);
- développer une application mobile qui fait la collecte des noms, adresses et données de localisation des personnes;
- installer une banque de mesures biométriques;
- comparer des fichiers de renseignements personnels;
- etc.

COMMENT RÉALISER UNE EFVP?

La bonne évaluation est celle qui est adaptée à votre entreprise ou à votre organisme public. Son ampleur peut être proportionnelle à la nature du projet envisagé. Il est important de retenir qu'il n'est pas nécessaire d'être un spécialiste de la protection des renseignements personnels pour procéder à une EFVP et que celle-ci peut être intégrée, au besoin, aux processus de gestion de projet d'une organisation.

L'EFVP consiste à bâtir et remplir une grille d'analyse ayant pour objet :

- de présenter le projet (objectif, procédures internes concernées, etc.);
- d'identifier les renseignements personnels visés par le projet, ainsi que leur circulation au sein du système d'information (cycle de vie du renseignement);
- de décrire quelles sont les répercussions du projet à l'égard des renseignements personnels visés;
- de faire un lien entre le projet et les principes légaux de protection des renseignements personnels (objet du fichier, nécessité, collecte, information, utilisation, consentement, communication, destruction, sécurité, accès, etc.);
- d'identifier les risques et les conséquences en matière de protection des renseignements personnels;
- de déterminer les solutions envisageables et les mettre en place.

janvier 2018

Faire une EFVP, c'est prévoir les répercussions que peuvent avoir de nouveaux projets et de nouvelles technologies sur la protection des renseignements personnels.

C'est adopter une approche globale, systématique, préventive et proactive du respect de la vie privée visant à atténuer les risques dès la conception d'un projet.

C'est favoriser le développement d'une véritable culture de la protection des renseignements personnels au sein de l'entreprise ou de l'organisme public et faire preuve de transparence dans la gestion de ceux-ci.

Bref, faire une EFVP, c'est agir de façon diligente et responsable au regard des enjeux relatifs à la protection des renseignements personnels, dans le respect des lois et des personnes concernées.

POUR JOINDRE LA COMMISSION :

Québec
Bureau 2.36
525, René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

Montréal
Bureau 18.200
500, boul. René-Lévesque Ouest
Montréal (Québec) H2Z 1W7
Téléphone : 514 873-4196
Télécopieur : 514 844-6170
Télécopieur affaires juridiques :
514 864-3225

Téléphone sans frais pour les deux bureaux
1 888 528-7741

Courrier électronique
cai.communications@cai.gouv.qc.ca

Site Internet
www.cai.gouv.qc.ca

Commission d'accès à l'information du Québec

Statistique Canada Statistics Canada

Microsoft 365 - Sommaire de l'évaluation des facteurs relatifs à la vie privée

Introduction

Microsoft 365 est une version infonuagique des outils de productivité de Microsoft Office qui est utilisée à l'échelle de l'organisation et qui permet de créer des documents, des présentations et des feuilles de calcul électroniques pour gérer des courriels, planifier du travail et effectuer d'autres tâches administratives courantes. Cette suite intégrée d'outils appuie les activités quotidiennes des employés de Statistique Canada, y compris la collaboration au sein de l'organisme.

Objectif

On a mené une évaluation des facteurs relatifs à la vie privée (EFVP) pour Microsoft 365 (M365) afin de déterminer si, entre autres, ce produit soulève des problèmes ou des questions sur le plan de la protection de la vie privée, de la confidentialité et de la sécurité, et, le cas échéant, de formuler des recommandations en vue de les résoudre ou de les atténuer.

Description

Microsoft 365 remplacera la suite Microsoft Office (p. ex. Word, Excel, PowerPoint) et le système de courriel actuel. Il offre également d'autres applications et produits (p. ex. le Planificateur, PowerApps) pour aider le

personnel à travailler efficacement.

Détermination et catégorisation des secteurs de risque

L'évaluation des facteurs relatifs à la vie privée détermine le niveau de risque potentiel (le niveau 1 correspond au niveau de risque le plus faible, et le niveau 4, au plus élevé) associé aux secteurs de risque suivants :

a) Type de programme ou d'activité

Administration des programmes, des activités et des services.

Échelle de risque : 2

b) Type de renseignements personnels recueillis et contexte

Les renseignements personnels peuvent comprendre le numéro d'assurance sociale d'une personne, des renseignements médicaux et financiers ou d'autres renseignements personnels de nature délicate, des renseignements personnels dont le contexte est de nature délicate, des renseignements personnels sur des mineurs ou des personnes légalement incapables ou des renseignements mettant en cause un représentant agissant au nom de la personne concernée.

Échelle de risque : 3

c) Participation des partenaires et du secteur privé au programme ou à l'activité

Organisations du secteur privé, organisations internationales ou gouvernements étrangers.

Échelle de risque : 4

d) Durée du programme ou de l'activité

Programme ou activité à long terme (continu).

Échelle de risque : 3

e) Personnes concernées par le programme

Les renseignements personnels utilisés dans le cadre du programme à des fins administratives internes touchent tous les employés.

Échelle de risque : 2

f) Transmission de renseignements personnels

Les renseignements personnels sont transmis à l'aide de technologies sans fil.

Échelle de risque : 4

g) Technologie et protection des renseignements personnels

M365 comprend des applications de productivité de bureau et des outils logiciels mis à jour et nouveaux qui appuieront la création, l'utilisation et le stockage de renseignements personnels par les employés dans le cadre de leur travail quotidien.

h) Risque qu'en cas d'atteinte à la vie privée, il y ait une incidence sur la personne ou l'employé

Il y a un risque qu'une atteinte à la vie privée ait une incidence sur une personne. Selon le type d'information divulguée, l'incidence pourrait comprendre un préjudice financier, un préjudice à la réputation, un embarras personnel ou un inconvénient.

Le risque global d'atteinte à la vie privée est faible en raison des contrôles et des procédures en place dans le système.

i) Risque potentiel pour l'établissement institutionnel en cas d'atteinte à la vie privée

Il y a un risque qu'une atteinte à la vie privée ait une incidence sur Statistique Canada. Selon le type d'information divulguée, les répercussions pourraient comprendre un préjudice à la réputation, une perte de confiance des employés à l'égard de la sécurité de cet outil et des inconvénients. Le risque global d'atteinte à la vie privée est faible en raison des contrôles et des procédures en place dans le système.

Conclusion

La présente évaluation de Microsoft 365 n'a pas permis de déterminer de risques relatifs à la vie privée qui ne peuvent pas être gérés à l'aide des mesures de protection existantes.

Date de modification :
2021-10-20

Office 365 – Résumé de l'évaluation des facteurs relatifs à la vie privée

Description du projet

Le passage à des services infonuagiques est un projet mis de l'avant par la Commission de la capitale nationale (CCN), le gouvernement du Canada n'offrant pas de tels services. Les services infonuagiques procurent des avantages impossibles à obtenir avec les moyens actuels dont dispose la CCN. Afin de répondre aux attentes de la population canadienne tout en offrant des services d'information fiables à son personnel, la CCN doit avoir recours à des solutions technologiques plus efficaces, novatrices et sûres.

L'évaluation des facteurs relatifs à la vie privée (EFVP) visait à évaluer les besoins en matière de protection des renseignements personnels, y compris les renseignements opérationnels de nature délicate, lors de l'utilisation de services infonuagiques. Le présent rapport aidera le personnel des technologies de l'information, de la gestion de l'information ainsi que de l'accès à l'information et de la protection de la vie privée, de même que les directeurs et directeurs généraux, à mieux connaître les risques et à recommander des mesures de protection afin que la transition vers l'infonuagique se déroule bien.

Ce projet porte principalement sur le passage des produits Microsoft Office (Outlook, PowerPoint, Word et Excel) et du réseau personnel (P) de la CCN d'un stockage sur place à un stockage infonuagique. Les solutions auxquelles la CCN entend avoir recours tireront parti d'Office 365 et de OneDrive Entreprise, deux produits offerts par Microsoft. La solution sera inspirée du modèle de logiciel à la demande ou logiciel-service (modèle SaaS). La CCN sera considérée « locataire/abonnée », et Microsoft Canada, « fournisseur de service ». L'information de la CCN sera stockée et traitée à des centres de données situés au Canada, ce qui devrait répondre aux exigences de souveraineté des données.

Le but du projet est de moderniser les processus liés à l'information organisationnelle et aux technologies de l'information (TI) de la CCN. Le projet comporte de nombreux avantages, dont :

- tirer parti des caractéristiques de sécurité inhérentes à l'infonuagique;
- permettre la mobilité de l'effectif et assurer une meilleure disponibilité des services;
- accroître la réactivité;
- réduire les coûts de fonctionnement;
- améliorer les capacités de reprise après sinistre de la CCN;
- permettre un accès rapide à des technologies novatrices.

Notre projet de passage à l'infonuagique implique l'utilisation de nouveaux logiciels servant à l'exécution des programmes et des activités de la CCN. Cela indique qu'il pourrait y avoir des problèmes et des risques liés à la protection des renseignements personnels. Afin de veiller à ce que la CCN respecte la *Loi sur la protection des renseignements personnels*, et afin de définir, de traiter et de résoudre les implications à cet égard, il a été convenu de procéder à une EFVP avant le lancement d'un projet pilote.

Portée de l'EFPV

La présente EFPV porte sur Microsoft Office 365 (fournisseur d'infonuagique), une suite de logiciels à la demande axée sur la collaboration et la productivité. La portée s'étendra aux flux de données personnelles entre les abonnés clients de la CCN (selon le modèle de service partagé) et Microsoft Cloud, en plus des données personnelles stockées dans des centres de données gérés par Microsoft.

La suite offerte par Microsoft comprend les éléments suivants :

- Exchange Online
- OneDrive Entreprise
- Office Online (Word, Excel, PowerPoint)
- Sauvegarde dans le nuage
  Remarque : Si la CCN décide de sauvegarder ses données chez un autre fournisseur, il faudra mener une autre EFPV.
- Skype Entreprise Online
  Remarque : Si nous mettons en service Skype Entreprise, la fonction qui permet l'enregistrement sera désactivée. Si la CCN souhaite rétablir la fonction d'enregistrement, nous examinerons l'incidence possible sur la protection des renseignements personnels et il faudra mener une autre EFPV.
- SharePoint Online (non visé par l'évaluation)

But de l'évaluation

Le but d'une EFVP est de déterminer la façon dont un programme ou un service, comme Microsoft Office 365, pourrait porter atteinte à la vie privée d'une personne. Elle peut aussi contribuer à atténuer les effets négatifs possibles sur la vie privée découlant de l'utilisation d'un programme ou d'un service. En outre, l'EFPV est un moyen pour la CCN d'énoncer son engagement à protéger la vie privée des personnes. Les EFPV favorisent la transparence et la responsabilité et contribuent à maintenir la confiance du public sur la façon dont la CCN gère les renseignements personnels. Sur le plan législatif, la présente EFPV permet de cerner des questions de non-conformité à la *Loi sur la protection des renseignements personnels* et de déterminer comment la CCN peut éviter ou réduire au minimum la perte, le mauvais usage ou l'usage abusif de renseignements personnels, ou le préjudice connexe.

Détermination et classement du risque

Niveau de risque : 1 = faible et 4 = très élevé

A. **Type de programme ou d'activité :** administration des programmes, des activités et des services.
   Niveau de risque : 2

B. **Type de renseignements personnels recueillis et contexte :** renseignements personnels de nature délicate, dont les profils détaillés, allégations ou soupçons, ou le contexte des renseignements personnels de nature particulièrement délicate.
   Niveau de risque : 4

C. **Participation de partenaires et du secteur privé au programme ou à l'activité :** avec des gouvernements étrangers, des organisations internationales et/ou des organisations du secteur privé.
Niveau de risque : 4

D. **Durée du programme ou de l'activité :** programme à long terme.
Niveau de risque : 3

E. **Personnes visées par le programme :** L'utilisation de renseignements personnels dans le cadre du programme à des fins administratives externes touche tous les individus.
Niveau de risque : 4

F. **Technologie et vie privée**
Est-ce que le programme ou l'activité, nouveau ou ayant subi des modifications importantes, comprend la mise en œuvre d'un nouveau système électronique, logiciel ou programme d'application, dont un collecticiel (ou logiciel de groupe), qui sera mis sur pieds afin de créer, collecter ou traiter les renseignements personnels dans le but de soutenir le programme ou l'activité? Oui.

L'activité ou le programme, nouveau ou ayant subi des modifications importantes, requiert-il des modifications aux systèmes hérités des TI? Oui.

Questions spécifiques aux technologies et à la protection de la vie privée
- Indiquer si le programme ou l'activité, nouveau ou ayant subi des modifications importantes, comprend la mise en œuvre d'une ou de plusieurs des technologies suivantes :

- **Méthodes d'identification améliorées**
- **Recours à la surveillance**
- **Recours à des techniques d'analyse automatisée des renseignements personnels, de comparaison des renseignements personnels et de découverte de connaissances**

Non.

G. **Transmission des renseignements personnels :** Les renseignements personnels sont transmis à l'aide de technologies sans fil.
Niveau de risque : 4

H. **Les risques possibles à l'individu ou à l'employé lors d'atteinte à la vie privée :**

- Les employés pourraient avoir accès à leurs renseignements personnels, les utiliser ou les divulguer à des fins personnelles.
- La demande pourrait ne pas venir d'un client (par exemple, quelqu'un d'autre pourrait utiliser leur adresse courriel).
- Les renseignements personnels d'un client pourraient être compromis lors du transfert vers le fournisseur de service.
- Les renseignements personnels d'un client pourraient être compromis lors de leur récupération par le fournisseur de service.

- Les risques inhérents à l'envoi par courriel de renseignements personnels à un client.
- Les risques inhérents au stockage de renseignements personnels sur des serveurs de fournisseurs d'infonuagique.
- L'information stockée sur des serveurs du fournisseur de services infonuagiques pourrait par mégarde franchir des frontières (infraction à la souveraineté des données).
- Il pourrait y avoir divulgation ou fuite accidentelle de renseignements personnels d'un abonné/locataire à un autre, ce qui peut survenir dans une configuration infonuagique à locataires multiples.

Résumé de l'évaluation des facteurs relatifs à la vie privée (EFVP) de l'EFPC : Microsoft Office 365

Description du projet

Le but de ce projet est de migrer et de moderniser les outils de travail et de collaboration de l'École de la fonction publique du Canada (EFPC) d'Office 2016 à Office 365.

Pourquoi l'EFVP était nécessaire

L'École recueille, utilise et divulgue des renseignements personnels pour maintenir une base de données d'utilisateurs et pour donner à ces utilisateurs l'accès aux outils dont ils ont besoin pour remplir leurs rôles. Office 2016 était géré localement sur les serveurs de l'EFPC et de Services partagés Canada (SSC), mais comme Office 365 sera hébergé sur des serveurs appartenant au fournisseur de services en nuage Microsoft Azure, les répercussions sur la vie privée doivent être réévaluées.

Objectifs de l'EFVP

L'EFVP vise à s'assurer que l'EFPC demeure conforme à la Loi sur la protection des renseignements personnels, et d'aider à identifier et à atténuer tout risque de réputation associé aux tâches administratives

requises pour donner accès aux outils Microsoft Office 365 aux employés de l'EFPC. Il vise également à sensibiliser l'École aux risques potentiels découlant de l'utilisation des renseignements personnels nécessaires à la maintenance des services Microsoft Office 365.

Conclusions de L'EFVP et résumé des risques

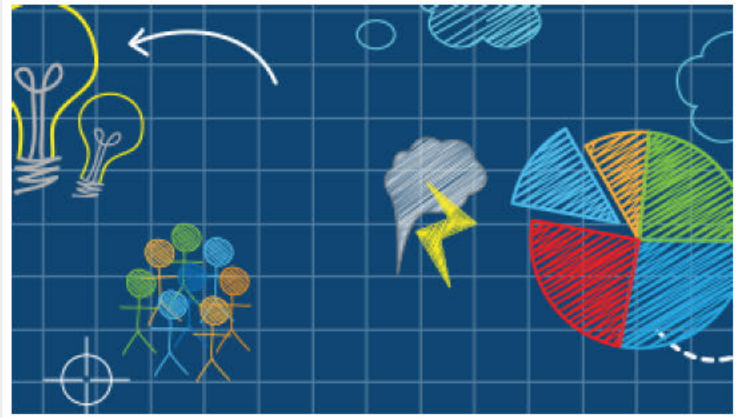
Les risques pour la vie privée découlant de l'administration de Microsoft Office 365 par l'École sont considérés comme modérés à faibles, car ils impliquent des collectes limitées de données non sensibles. Ces données sont collectées et utilisées à des fins administratives et comprennent des noms, des adresses courriels et des adresses IP. Les données sont obtenues indirectement par le biais de programmes de dotation ou d'apprentissage et sont partagées avec le SSC puisqu'il est également responsable de la gestion des comptes d'utilisateurs. Il n'y a pas de nouveaux renseignements personnels collectés par rapport à Office 2016, mais en plus d'être stockés localement, les données sont désormais également stockées sur des serveurs Microsoft Azure. Cette nouvelle stratégie pourrait augmenter le profil de risque de l'EFPC en matière de protection de la vie privée.

Recommandations

Bien que les risques actuels sur la vie privée des personnes soient gérés adéquatement par l'École au moyen de mesures juridiques, politiques et techniques axées sur la protection des renseignements personnels, il est de la plus haute importance de s'assurer que nous continuons à le faire. Toute modification de Microsoft Office 365 susceptible d'avoir un impact sur la vie privée des personnes doit être examinée attentivement et évaluée en fonction de l'EFVP.

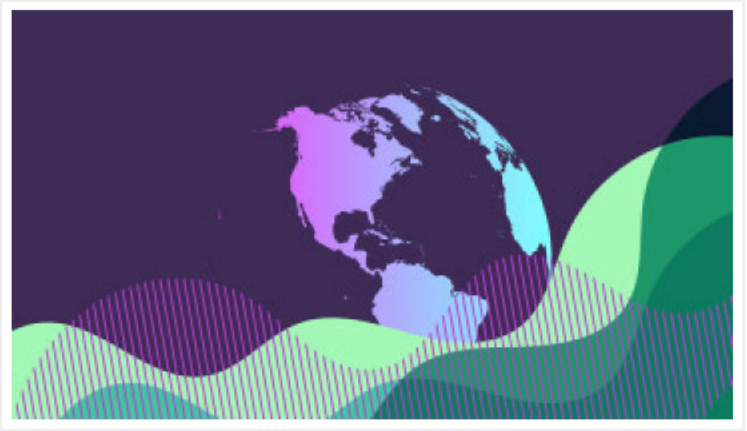
Contactez-nous | Abonnez-vous au bulletin GCApprentissage

En vedette



Événement : Série sur les méthodes de service et de conception : Équipes interfonctionnelles au gouvernement
(28 septembre 2023)

Événement : Journée nationale de la vérité et de la réconciliation 2023 : Lutter contre le négationnisme des pensionnats et concrétiser la réconciliation
(29 septembre 2023)



Événement : Série sur le changement climatique et les migrations humaines : Déplacements dus au changement climatique et migrations dans le monde
(3 octobre 2023)

Date de modification :
2021-12-08

Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner of Canada

Résumé de l'évaluation des facteurs relatifs à la vie privée du projet infonuagique Microsoft Office 365

Les sections qui suivent et les informations présentées ci-dessous constituent le contenu minimal d'une évaluation des facteurs relatifs à la vie privée de base (EFVP) pour le projet du Commissariat à la protection de la vie privée (Commi ariat) Ce projet vi e à mettre en œuvre la uite Micro oft Office 365, un logiciel ervice dan le nuage contenant plusieurs applications (services infonuagiques M365).

L'objectif de ce projet de mise en œuvre d'un service infonuagique est la modernisation de la technologie qu'utilise présentement le Commissariat. Il pourra ainsi optimiser ses opérations grâce à des fonctionnalités qui surpassent les capacité de outil qu'il utili e à l'heure actuelle La mi e en œuvre permettra au Commi ariat de gérer l'information plus efficacement afin de soutenir la prestation de ses programmes et services. Ce projet correspond aussi aux directives, au guide et à la stratégie d'adoption de l'information en nuage du gouvernement du Canada (GC).

Dirigeants de l'institution – évaluation des facteurs relatifs à la vie privée et projet infonuagique

- **In titution du gouvernement du Canada** Commi ariat à la protection de la vie privée du Canada
- **Représentante gouvernementale responsable de l'évaluation des facteurs relatifs à la vie privée de base** : Sue Lajoie, chef de la protection des renseignements personnels
- **Chef de l'institution gouvernementale / Déléguée pour l'article 10 de la *Loi sur la protection des renseignements personnels*** : Sue Lajoie, chef de la protection des renseignements personnels
- **Cadre upérieur re pon able du projet de mi e en œuvre de l'infonuagique M365** Séba tien Deli le Côté, dirigeant principal de l'information

Nom et description de l'institution gouvernementale

Le Commissariat est un agent du Parlement qui a pour mandat de superviser la protection et la promotion du droit à la vie privée Ain i, il veille, entre autre , à ce que le in titution gouvernementale re pectent la *Loi sur la protection des renseignements personnels* lors de la manipulation de ces types de renseignements. De plus, le Commissariat veille au respect de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la loi fédérale sur la protection des renseignements personnels dans le secteur privé.

Pour remplir son mandat, le Commissariat entreprend plusieurs activités, p. ex. (par exemple) des enquêtes sur des plaintes relatives à la protection de la vie privée, de la recherche, des vérifications, des poursuites en justice, des rapports à l'intention du public et de la sensibilisation du public par des initiatives. En tant qu'institution gouvernementale, le Commissariat est aussi sujet aux dispositions de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*.

Autorisation légale

En vertu de la *Loi sur la protection des renseignements personnels* et de la LPRPDE (Loi sur la protection des renseignements personnels et les documents électroniques), le Commissariat est autorisé à recevoir des plaintes et à conduire des enquêtes à leur sujet, à procéder à des vérifications et à entreprendre d'autres activités pour protéger et promouvoir le droit des personnes à la vie privée. Conformément à ces lois, le Commissariat a l'autorisation légale de recueillir, d'utiliser et de communiquer des renseignements, dont les renseignements personnels, afin de remplir son mandat.

Le Commissariat a le pouvoir de gérer son infrastructure de technologie de l'information et les renseignements qu'il détient en vertu de l'article 161 de la *Loi sur la gestion des finances publiques* ainsi que des directives et des politiques applicables du SCT (Secrétariat du Conseil du Trésor).

Services partagés Canada est autorisé, en vertu des articles 6 et 8 de la *Loi sur Services partagés Canada* et du décret c.p. (conseil privé) 2015-1071 du 16 juillet 2015, à fournir au Commissariat des services relatifs à la technologie de l'information (« TI ») des utilisateurs finaux, des services relatifs aux courriels, des services relatifs aux centres de données, et des services relatifs aux réseaux.

Conformément aux exigences du Conseil du Trésor régissant l'utilisation de services infonuagiques par des institutions gouvernementales, le Commissariat utilise les services de cyberdéfense du Centre canadien pour la cybersécurité (CCC), une division du Centre de la sécurité des télécommunications (CST). La *Loi sur le Centre de la sécurité des télécommunications* autorise le CST (Centre de la sécurité des télécommunications) à fournir « des services afin d'aider à protéger […] l'information électronique et les infrastructures de l'information des institutions fédérales » [1]. De plus, le CST (Centre de la sécurité des télécommunications) est autorisé à mener « des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales » [2].

Fichiers de renseignements personnels

La *Loi sur la protection des renseignements personnels* exige que les institutions gouvernementales recensent et décrivent leurs fichiers et catégories de renseignements personnels, en plus de rendre compte de ceux-ci. De cette façon, les institutions indiquent au public et à leurs employés quels renseignements personnels le Commissariat recueille, utilise et retire à l'appui de ses fonctions et de ses activités. M365 stockera certains renseignements détenus par le Commissariat, tels que des renseignements sur les programmes et sur les employés contenant eux-mêmes des renseignements personnels obtenus à l'appui des fonctions et des activités du Commissariat. L'instauration de M365 apportera des modifications en ce qui concerne :

i. qui stockera les renseignements personnels détenus pas le Commissariat (il s'agit de Microsoft);
ii. où les renseignements personnels seront stockés (il s'agit d'un emplacement de stockage externe dans le nuage géré par Microsoft);
iii. les raisons du traitement des renseignements personnels, puisque Microsoft reconnaît qu'il les utilise pour ses propres besoins.

À ce jour, les fichiers de renseignements personnels du Commissariat sont les suivants :

Fichiers de renseignements personnels ordinaires

Programme/activité	Numéro FRP (fichiers de renseignements personnels)	Titre
Services d'acquisitions	POU (Numéro d'identification d'un FRP ordinaire) 912	Marchés de services professionnels
Services de communications	POU (Numéro d'identification d'un FRP ordinaire) 915	Communications internes
	POU (Numéro d'identification d'un FRP ordinaire) 914	Communications publiques
Services de gestion financière	POU (Numéro d'identification d'un FRP ordinaire) 931	Comptes créditeurs
	POU (Numéro d'identification d'un FRP ordinaire) 932	Comptes débiteurs
	POU (Numéro d'identification d'un FRP ordinaire) 940	Cartes d'achat

Programme/activité	Numéro FRP (fichiers de renseignements personnels)	Titre
Services de gestion des ressources humaines	POE (Numéro d'identification d'un FRP ordinaire sur les employés) 920	Programme de reconnaissance
	POE 902	Dotation
	POE 903	Présences et congés
	POE 904	Rémunération et avantages sociaux
	POE 918	Équité en emploi et diversité
	POU (Numéro d'identification d'un FRP ordinaire) 908	Accueil
	POU (Numéro d'identification d'un FRP ordinaire) 935	Planification des ressources humaines
	POU (Numéro d'identification d'un FRP ordinaire) 933	Plaintes déposées en vertu de la *Loi canadienne sur les droits de la personne*
	POE 911	Mesures disciplinaires
	POE 910	Griefs
	POE 919	Harcèlement
	POE 907	Santé et de sécurité au travail
	POU (Numéro d'identification d'un FRP ordinaire) 906	Divulgation d'information sur les actes fautifs commis en milieu de travail
	POE 915	Codes de valeurs et d'éthique du secteur public et Code(s) de conduite organisationnel(s)
	POE 916	Aide aux employés

Programme/activité	**Numéro FRP (fichiers de renseignements personnels)**	**Titre**
	POE 908	Accidents d'automobile, de bateau, d'embarcation et d'avion
	POE 906	Langues officielles
	POE 912	Programme de gestion du rendement des employés
	POU (Numéro d'identification d'un FRP ordinaire) 911	Demandes d'emploi
	POE 901	Dossier personnel d'un employé
	POU (Numéro d'identification d'un FRP ordinaire) 934	Gestion des talents des cadres supérieurs
	POU (Numéro d'identification d'un FRP ordinaire) 917	Filtrage de sécurité du personnel
	POU (Numéro d'identification d'un FRP ordinaire) 910	Réinstallation
	POE 905	Formation et perfectionnement
Services de gestion de l'information	POU (Numéro d'identification d'un FRP ordinaire) 901	Demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*
	POU (Numéro d'identification d'un FRP ordinaire) 936	Services de bibliothèque
Services de technologie de l'information	POU (Numéro d'identification d'un FRP ordinaire) 905	Journaux de contrôle des réseaux électroniques

Programme/activité	**Numéro FRP (fichiers de renseignements personnels)**	**Titre**
Services de gestion et de surveillance	POU (Numéro d'identification d'un FRP ordinaire) 938	Activités de sensibilisation
	POU (Numéro d'identification d'un FRP ordinaire) 902	Correspondance à la direction
	POU (Numéro d'identification d'un FRP ordinaire) 942	Évaluation
	POU (Numéro d'identification d'un FRP ordinaire) 941	Vérification interne
Services du matériel	POE 908	Accidents d'automobile, de bateau, d'embarcation et d'avion

Programme/activité	Numéro FRP (fichiers de renseignements personnels)	Titre
Services de voyage et autres services administratifs	POE 914	Stationnement
	POU (Numéro d'identification d'un FRP ordinaire) 918	Nominations par le gouverneur en conseil
	POU (Numéro d'identification d'un FRP ordinaire) 919	Membres de conseils d'administration, de comités et de conseils
	POU (Numéro d'identification d'un FRP ordinaire) 903	Planification de la continuité des activités
	POU (Numéro d'identification d'un FRP ordinaire) 923	Divulgation aux organismes d'enquête
	POU (Numéro d'identification d'un FRP ordinaire) 908	Accueil
	POU (Numéro d'identification d'un FRP ordinaire) 909	Voyages
	POE 917	Cartes d'identification et laissez-passer
	POU (Numéro d'identification d'un FRP ordinaire) 906	Divulgation d'information sur les actes fautifs commis en milieu de travail
	POU (Numéro d'identification d'un FRP ordinaire) 917	Filtrage de sécurité du personnel

Programme/activité	Numéro FRP (fichiers de renseignements personnels)	Titre
	POU (Numéro d'identification d'un FRP ordinaire) 939	Incidents de sécurité et atteintes à la vie privée
	POU (Numéro d'identification d'un FRP ordinaire) 907	Surveillance vidéo, registres de contrôle d'accès des visiteurs et laissez-passer

Fichiers de renseignements personnels ordinaires

Programme/activité	Numéro FRP (fichiers de renseignements personnels)	Titre
Activités relatives à la conformité	CPVP (Commissariat à la protection de la vie privée du Canada) PPU (Numéro d'identification d'un FRP particulier) 005	Plaintes et enquêtes concernant la vie privée
	CPVP (Commissariat à la protection de la vie privée du Canada) PPU 001	Demandes de renseignements concernant la vie privée
	CPVP (Commissariat à la protection de la vie privée du Canada) PPU 008	Commissaire spécial à la protection de la vie privée – plaintes et enquêtes
	CPVP (Commissariat à la protection de la vie privée du Canada) PPU 004	Avis au CPVP (Commissariat à la protection de la vie privée du Canada) – Communications de renseignements dans l'intérêt public
	CPVP (Commissariat à la protection de la vie privée du Canada) PPU 006	Avis au Commissariat en vertu de la LPRPDE (Loi sur la protection des renseignements personnels et les documents électroniques) lorsque l'accès aux renseignements personnels est refusé
Recherche et élaboration des politiques	CPVP (Commissariat à la protection de la vie privée du Canada) PPU 003	Demandes de publications

Détermination et classification des secteurs de risque

a) Type de programme ou d'activité	Échelle de risque	Applicable
Programme ou activité qui ne nécessite pas la prise d'une décision concernant une personne identifiable	1	**Oui**
Administration des programmes, des activités et des services	2	**Oui**
Enquête sur la conformité ou enquête réglementaire, et application de la loi	3	Non
Enquête criminelle et application de la loi/sécurité nationale	4	Non

b) Type de renseignements personnels recueillis et contexte	Échelle de risque	Applicable
Seuls les renseignements personnels fournis par la personne – au moment de la collecte – relatifs à un programme autorisé et recueillis directement auprès de la personne ou avec son consentement pour la diffusion pourvu que les renseignements ne soient pas de nature sensible dans le contexte.	1	**Oui**
Les renseignements personnels fournis par la personne avec le consentement à utiliser les renseignements personnels détenus par une autre source pourvu que les renseignements ne soient pas de nature sensible après la collecte.	2	**Oui**
Le numéro d'assurance sociale, les renseignements personnels médicaux, financiers ou autres de nature sensible ou dont l'utilisation peut s'avérer sensible dans certains contextes; renseignements personnels relatifs à des mineurs ou à des personnes légalement incapables, ou mettant en cause un représentant qui agit au nom de la personne.	3	**Oui**
Renseignements personnels de nature sensible, dont les profils détaillés, les allégations ou les soupçons, et les échantillons de substances corporelles, ou contexte particulièrement sensible lié aux renseignements personnels.	4	**Oui**

c) Participation des partenaires et du secteur privé au programme ou à l'activité	Échelle de risque	Applicable
Au sein de l'institution (dans le cadre d'un seul programme ou de plusieurs programmes au sein de la même institution)	1	**Oui**
Autres institutions gouvernementales	2	**Oui**
Autre administration publique fédérale, provinciale, territoriale ou municipale ou combinaison de celles-ci	3	Non
Organisations du secteur privé, organisations internationales ou gouvernements étrangers	4	**Oui**

d) Durée du programme ou de l'activité	Échelle de risque	Applicable
Programme ponctuel ou activité ponctuelle	1	Non
Programme ou activité de courte durée	2	Non
Programme ou activité de longue durée	3	**Oui**

e) Personnes visées par le programme	Échelle de risque	Applicable
L'utilisation, dans le cadre de ce programme, de renseignements personnels à des fins administratives internes touche certains employés.	1	Non
L'utilisation, dans le cadre de ce programme, de renseignements personnels à des fins administratives internes touche tous les employés.	2	**Oui**
L'utilisation, dans le cadre de ce programme, de renseignements personnels à des fins administratives externes touche certaines personnes.	3	**Oui**
L'utilisation, dans le cadre de ce programme, de renseignements personnels à des fins administratives externes touche toutes les personnes	4	Non

f) Technologie et vie privée (Une réponse affirmative à l'une ou l'autre des questions uivante ignale un ri que d'atteinte à la vie privée ur lequel il faudra e pencher et qui devra, au besoin, être atténué.)		
Question	**Oui**	**Non**
E t ce que le programme ou l'activité, de création récente ou ayant ubi de modifications importantes, prévoit l'installation d'un nouveau système électronique, logiciel ou programme d'application (y compris les collecticiels ou logiciels de groupe) pour faciliter la création, la collecte ou le traitement des ren eignement per onnel ?	**X**	
E t ce que le programme ou l'activité, de création récente ou ayant ubi de modification importante , néce ite que de modification oient apportée aux systèmes de TI (technologie de l'information) existants?	**X**	
Est-ce que le programme ou l'activité, de création récente ou ayant subi des modifications importantes, nécessite la mise en œuvre de nouvelles technologies ou d'au moins une des activités suivantes?		
Méthode d'identification améliorée	**X**	
Surveillance	**X**	
Techniques d'analyse automatisée des renseignements personnels, de comparaison des renseignements personnels et d'acquisition de connaissances.	**X**	

g) Transmission des renseignements personnels	Échelle de risque	Applicable
Les renseignements personnels sont utilisés à l'intérieur d'un système fermé (c.-à-d. pas de connexion à Internet, à l'intranet ou à un autre système, et diffusion contrôlée des documents papier).	1	Non
Les renseignements personnels sont utilisés dans un système qui est connecté à au moins un autre système.	2	**Oui**
Les renseignements personnels sont transférés sur un dispositif portatif (c.à-d. clé USB, disquette, ordinateur portatif) ou sur un autre support, ou sont imprimés.	3	**Oui**
Les renseignements personnels sont transmis à l'aide de technologies sans fil.	4	**Oui**

h) Impact d'une atteinte à la vie privée pour l'individu ou l'employé)		
Question	**Oui**	**Non**
Risque possible, en cas d'atteinte à la vie privée, de répercussions pour l'individu ou l'employé	**X**	

i) Impact d'une atteinte à la vie privée sur l'institution – Commentaire		
Question	**Oui**	**Non**
Risque possible, en cas d'atteinte à la vie privée, de répercussions pour l'institution.	**X**	

Notes de bas de page

1 *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13 (Loi sur le CST (Centre de la sécurité des télécommunications)), art. 17

2 *Loi sur le CST (Centre de la sécurité des télécommunications)*, par. 18(a)

▶ Signaler un problème ou une erreur sur cette page

Date de modification :
2022-06-22