Commission d'accès
à l'information
du Québec

Réaliser une évaluation des facteurs relatifs à la vie privée

Guide d'accompagnement

22 septembre 2023

Version 3.0

22 septembre 2023

Ce guide a été conçu par la Commission d'accès à l'information en 2021. Cette nouvelle version tient compte de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (la Loi 25).

Des versions administratives de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels dans le secteur privé* intégrant les modifications les plus récentes sont accessibles sur le site Web de la Commission : www.cai.gouv.qc.ca. Le texte de ce guide **ne tient pas compte** de changements éventuels apportés par des projets de loi à l'étude, ou non encore en vigueur, à la date de publication de ce guide.

Ce guide est un outil d'accompagnement. Les notions qu'il contient sont informatives et ont pour objectif d'aider à la compréhension. En cas de contradiction entre l'information présentée et les termes mêmes des lois, celles-ci prévaudront.

Les organisations publiques et privées sont responsables de s'assurer de respecter le cadre juridique en vigueur en matière de protection des renseignements personnels.

Le genre masculin désigne aussi bien les femmes que les hommes et n'est utilisé que pour alléger le texte.

Ce guide peut être reproduit en tout ou en partie à la condition d'en mentionner la source et de ne pas l'utiliser à des fins commerciales.

Pour tout **commentaire** à propos de ce guide, contactez-nous à l'adresse veille@cai.gouv.qc.ca. Veuillez noter que nous ne **répondrons pas nécessairement** à ces commentaires, mais que nous en tiendrons compte dans la réflexion sur les prochaines mises à jour du guide.

Pour toute **question générale** sur ce guide, contactez la Commission. Notez qu'elle n'offre pas d'avis ou de conseils juridiques.

Table des matières

À propos de ce guide iii

Introduction 1

Qu'est-ce qu'une évaluation des facteurs relatifs à la vie privée? 1

Pourquoi réaliser une EFVP? 1

Quand réaliser une EFVP? 2

Synthèse de la démarche d'EFVP 3

1. Déterminer si une évaluation est requise 4

1.1. Situations prévues à la Loi sur l'accès et à la Loi sur le privé 5

1.2. Autres situations 6

2. Préparer votre évaluation des facteurs relatifs à la vie privée 8

2.1. Définir votre projet et ses objectifs 8

2.2. Déterminer la portée de l'évaluation 9

2.3. Définir les rôles et les responsabilités 10

2.4. Inventorier et cartographier les renseignements personnels 11

2.4.1. Faire l'inventaire des renseignements personnels 11
2.4.2. Cartographier les renseignements personnels 13

2.5. Évaluer l'ampleur de l'EFVP à réaliser 14

2.5.1. Évaluer le degré de sensibilité des renseignements personnels 15
2.5.2. Évaluer la finalité de l'utilisation ou de la communication des renseignements personnels 15
2.5.3. Évaluer la quantité de renseignements personnels 16
2.5.4. Évaluer la répartition des renseignements personnels 16
2.5.5. Évaluer le support de conservation des renseignements personnels 16

2.6. Dresser la liste de vos obligations 17

3. Analyser et évaluer les facteurs relatifs à la vie privée 19

3.1. Respecter les obligations et les principes de protection des renseignements personnels 19

3.2. Identifier les risques d'atteinte à la vie privée engendrés par votre projet et évaluer leurs conséquences 20
3.2.1. Identifier les risques d'atteinte à la vie privée engendrés par votre projet 20
3.2.2. Évaluer le niveau de chaque risque identifié 23
3.3. Mettre en place des stratégies pour éviter ou réduire les risques 25
3.4. Faire le suivi de votre évaluation 27
4. Rendre compte de l'évaluation 28
4.1. À quoi sert le rapport? 28
4.2. Que devrait contenir le rapport? 28
4.3. Le rapport devrait-il être diffusé? 29
Faire évoluer l'EFVP en continu 30
Annexe 1 – Communication à des fins d'étude, de recherche ou de production de statistiques 31
Annexe 2 – Acquisition, développement ou refonte d'un système d'information ou de prestation électronique de services 35
Annexe 3 – Communication de renseignements personnels à l'extérieur du Québec 37
Annexe 4 – Collecte par un organisme public pour le compte d'un autre .. 40
Annexe 5 – Autres types de communications sans consentement (secteur public) 42
Annexe 6 – Inventaire et cartographie des renseignements personnels : aide à la réflexion 45

À propos de ce guide

Quel est son objectif?

Ce guide vise à vous **accompagner dans la réalisation d'une évaluation des facteurs relatifs à la vie privée (EFVP)**, que vous la meniez en raison d'une obligation légale ou à titre de bonne pratique.

Exemples de projets[1] concernés :

- Développement d'un nouveau système d'information ou d'une technique de personnalisation d'un produit ou d'un service;
- Acquisition d'un système d'intelligence artificielle ou de caméras de surveillance;
- Utilisation d'empreintes digitales, de géolocalisation, de reconnaissance faciale, d'objets connectés ou de capteurs pour villes intelligentes;
- Communication de renseignements personnels à un chercheur;
- Stockage de renseignements personnels dans un centre infonuagique situé à l'extérieur du Québec.

À qui s'adresse-t-il?

Ce guide s'adresse principalement aux **responsables de la protection des renseignements personnels** dans toutes les organisations[2] et aux **membres d'un comité sur l'accès à l'information et la protection des renseignements personnels** dans le secteur public.

De manière secondaire, il pourra aussi être utile à plusieurs autres personnes au sein :

- **De petites entreprises :** chefs d'entreprise, commerçants, artisans, travailleurs autonomes, responsables associatifs, etc.;

---

[1] Dans ce guide, le terme « **projet** » fait référence à tout projet, technologique ou autre, susceptible d'impliquer la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

[2] Dans ce guide, le terme « **organisation** » désigne les entreprises privées et les organismes publics soumis aux lois sur la protection des renseignements personnels :

- Une **entreprise** est définie comme étant 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 (article 1525 du *Code civil du Québec*). Elle comprend notamment un travailleur autonome, une compagnie, une société en nom collectif ou en commandite, un organisme sans but lucratif, un syndicat de copropriété et un syndicat.
- Le terme **organismes publics** réfère aux **ministères** et **organismes gouvernementaux** et **municipaux** ainsi qu'aux **organismes des réseaux de la santé** et de l'**éducation**.

Le texte sera spécifique lorsqu'il s'appliquera uniquement à l'un ou l'autre des secteurs.

- **De grandes entreprises :** 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.;
- **D'organismes publics[3] :** responsables organisationnels de la sécurité de l'information (ROSI), de la gestion documentaire (RGD), de l'éthique (RE), du développement ou de l'acquisition des systèmes d'information (RDASI), de l'architecture de sécurité de l'information (RASI), de la continuité des services (RCS), de la gestion des technologies de l'information (RGTI), de la sécurité physique (RSP), de la vérification interne (RVI), etc.

Est-il obligatoire de suivre la démarche décrite dans ce guide?

La loi ne précise pas comment réaliser une EFVP. Elle ne prescrit pas non plus le contenu et la forme d'un rapport qui rend compte de cette EFVP.

Ainsi, il n'est pas obligatoire de suivre ou d'appliquer ce guide à la lettre.

Toutefois, vous y trouverez des indications importantes qui vous aideront à structurer votre processus d'EFVP et, s'il y a lieu, vos rapports.

[3] L'intitulé des postes peut varier.

Introduction

Qu'est-ce qu'une évaluation des facteurs relatifs à la vie privée?

L'EFVP[4] est une **démarche visant à protéger les renseignements personnels et à respecter la vie privée des personnes physiques**. Il s'agit d'une forme d'analyse d'impact[5]. Elle est évolutive et doit être revue tout au long du projet.

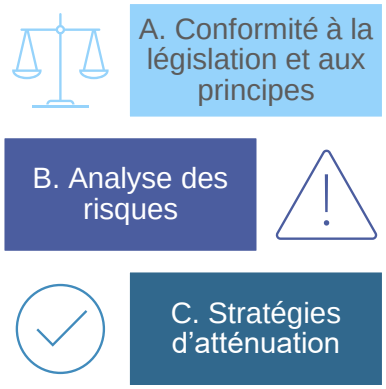
Elle consiste à considérer, avant de commencer un projet et tout au long de sa durée, **tous les facteurs ayant un effet positif ou négatif pour le respect de la vie privée** des personnes concernées.

Ces facteurs sont les suivants :

A. La **conformité** du projet à la **législation applicable** en matière de protection des renseignements personnels et le **respect des principes** l'appuyant;

B. L'identification des **risques** d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs conséquences;

C. La mise en place de **stratégies** pour éviter ces risques ou les réduire efficacement et leur maintien dans le temps.



Pourquoi réaliser une EFVP?

En dehors de son caractère obligatoire dans certaines situations prévues par la loi, l'EFVP a pour objectifs de :

- **Protéger les personnes** concernées par un projet, et ce, de la collecte de leurs renseignements personnels à leur destruction[6];
- **Mettre en place des mesures appropriées** pour respecter vos obligations en matière de protection des renseignements personnels;

[4] En anglais, l'EFVP est généralement appelée *privacy impact assessment* (PIA) ou *data protection impact assessment* (DPIA).
[5] Comme d'autres démarches semblables, elle permet de réfléchir à l'incidence d'un projet sur un domaine particulier de la vie humaine. On peut par exemple la rapprocher, dans son esprit, de l'évaluation d'impact environnemental, de l'évaluation d'incidence algorithmique ou de l'étude d'impact sur les droits humains. Toutes impliquent des étapes similaires.
[6] Les lois prévoient désormais la possibilité d'anonymiser les renseignements personnels au lieu de les détruire, dans certains cas.

- **Éviter les conséquences** que causerait une gestion inadéquate de ces renseignements (incidents de confidentialité, poursuites, atteintes à l'image, etc.).

Quand réaliser une EFVP?

Vous devez commencer votre EFVP **dès le début de votre projet** :

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

En effet, attendre avant de commencer vous mettrait à risque de devoir apporter des modifications importantes tardivement, avec les coûts et les délais associés. Cependant, il n'est jamais trop tard pour amorcer votre EFVP si vous réalisez qu'elle s'impose.

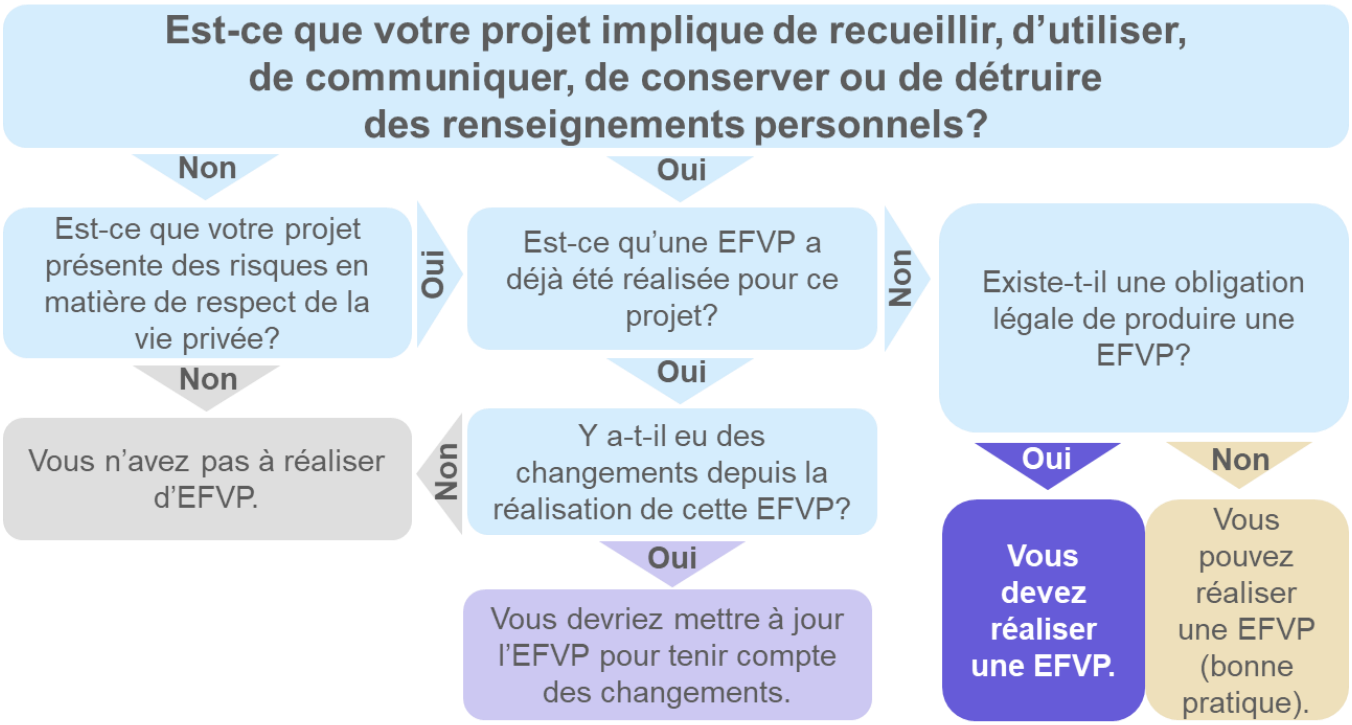
L'EFVP doit évoluer tout au long du projet, selon les changements que vous y apportez. Si une EFVP a déjà été réalisée dans le passé pour le même projet, vous pouvez donc en faire la mise à jour.

Synthèse de la démarche d’EFVP

La suite de ce guide est structurée selon les étapes de la démarche proposée par la Commission, présentées dans la synthèse suivante :

1. Déterminer si une évaluation est requise

Avant de vous lancer dans une démarche d'EFVP, **vérifiez si celle-ci est requise**. L'arbre décisionnel suivant présente les questions que vous devez vous poser :



Comme l'illustre cet arbre décisionnel, la question maîtresse est la suivante : votre projet implique-t-il la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels?

- **Si la réponse est non, sans équivoque,** et que votre projet ne présente aucun risque en matière de respect de la vie privée, vous n'avez pas à réaliser d'EFVP.

  Attention! Des renseignements peuvent, une fois qu'ils sont croisés avec d'autres, révéler de l'information sur les personnes concernées. N'écartez pas l'EFVP trop rapidement.

- **Si la réponse est oui**, une EFVP peut être requise. Poursuivez votre analyse :

  - Si vous avez **déjà réalisé une EFVP** pour une version antérieure de ce projet et que des changements sont survenus, vous devez la mettre à jour ou la recommencer pour tenir compte de ces changements.

- Si vous n'avez **pas réalisé d'EFVP** auparavant pour ce projet, sachez que différentes situations déclenchent l'obligation légale de mener une EFVP. Elles sont prévues dans les lois suivantes :
  - > *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès);
  - > *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé);
  - > *Loi favorisant la transformation numérique de l'administration publique* (LFTNAP);
  - > *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI);
  - > *Loi sur l'administration fiscale* (LAF).

Les tableaux suivants présentent toutes les situations dans lesquelles l'EFVP est **obligatoire**, et ce, dans le cadre juridique existant **à la date de publication de ce guide** (22 septembre 2023)**.** Notez que :

- Votre analyse doit tenir compte du cadre légal particulier à votre situation. Consultez les détails et particularités dans les annexes mentionnées dans le premier tableau;
- Les étapes suivantes de la démarche proposée s'appliquent à toute situation;
- Si vous n'êtes pas dans une des situations mentionnées dans les tableaux, vous pouvez tout de même réaliser une EFVP à titre de bonne pratique.

1.1. Situations prévues à la Loi sur l'accès et à la Loi sur le privé

Situation	Articles	Secteur public	Secteur privé
1. Communication de renseignements personnels à un tiers, sans le consentement des personnes concernées, pour une utilisation à des fins d'étude, de recherche ou de production de statistiques → Détails et particularités : annexe 1	67.2.1 - Loi sur l'accès 21 - Loi sur le privé	Oui	Oui
2. Projet d'acquisition, de développement ou de refonte d'un système d'information ou de prestation électronique de services impliquant des renseignements personnels → Détails et particularités : annexe 2	63.5 - Loi sur l'accès 3.3 - Loi sur le privé	Oui	Oui
3. Communication de renseignements personnels à l'extérieur du Québec → Détails et particularités : annexe 3	70.1 - Loi sur l'accès 17 - Loi sur le privé	Oui	Oui
4. Collecte de renseignements personnels par un organisme public pour le compte d'un autre organisme → Détails et particularités : annexe 4	64 - Loi sur l'accès	Oui	Non

Situation	Articles	Secteur public	Secteur privé
5. Autre communication de renseignements personnels, sans le consentement de la personne concernée : a) À un autre organisme public, au Québec ou ailleurs : ○ Pour l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion ○ Lorsque la communication est manifestement au bénéfice de la personne concernée; b) À toute personne ou à tout organisme : ○ Lorsque des circonstances exceptionnelles le justifient Pour la prestation d'un service à rendre à la personne concernée par un organisme public, notamment à des fins d'identification → Détails et particularités : annexe 5	68 - Loi sur l'accès	Oui	Non

Il n'est pas obligatoire de mener rétroactivement une EFVP prévue par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (la Loi 25). Autrement dit, si votre projet était déjà **finalisé** à la date d'entrée en vigueur[7] (p. ex. entente de communication conclue, système d'information implanté, etc.), vous n'êtes pas tenu de réaliser d'EFVP sur celui-ci.

Malgré cela, vous devez réaliser une EFVP :

- **Si vous modifiez ce projet (p. ex. amendement à l'entente[8], refonte du système, etc.);**
- **Si votre projet implique des communications de renseignements personnels à l'extérieur du Québec faites après le 22 septembre 2023.**

De manière plus générale, dès qu'un projet implique des renseignements personnels, **la réalisation d'une EFVP constitue aussi une bonne pratique**. Il peut donc être bénéfique d'analyser l'existant à la lumière des nouvelles obligations légales.

1.2. Autres situations

Ce guide se concentre seulement sur les situations prévues par la Loi sur l'accès et la Loi sur le privé. La démarche générale qu'il présente reste néanmoins applicable dans les cas suivants :

[7] Soit le 22 septembre 2022 pour la situation n° 1 et le 22 septembre 2023 pour les situations nos 2 à 5 dans le tableau.
[8] Notez que des dispositions transitoires s'appliquent pour les situations nos 4 et 5. Voir l'annexe 4 et l'annexe 5.

Situation	Articles	Secteur public	Secteur privé
6. Projet en ressources informationnelles d'intérêt gouvernemental	9 - LFTNAP	Oui	Non
7. Collecte, utilisation ou communication pour les fonctions d'un organisme public désigné comme source officielle de données numériques gouvernementales	12.16 - LGGRI	Oui	Non
8. Communication par Revenu Québec à un organisme public désigné comme source officielle de données numériques gouvernementales	69.1.1 - LAF	Oui	Non

2. Préparer votre évaluation des facteurs relatifs à la vie privée

Une fois qu'il est déterminé qu'une EFVP est requise, vous devez la préparer. Vous devrez vous poser les bonnes questions pour bien cibler les aspects de votre projet qui doivent être considérés, répertorier les renseignements personnels concernés, évaluer l'ampleur de l'analyse à faire et connaître les obligations à respecter.

2.1. Définir votre projet et ses objectifs

D'abord, définissez votre projet et les objectifs qui le motivent.

Présentez les grandes lignes de votre projet

Cette étape 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 3.2 et 3.3).

Par exemple :

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

Expliquez 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.

Un objectif doit être **légitime** et se rapporter à des **préoccupations réelles et sérieuses**.

Exemples d'objectifs d'un projet :

- Offrir un nouveau service public;
- Déployer, sur le Web, un service existant;
- Accroître la sécurité d'une installation;
- Contrer la fraude;
- Améliorer la détection d'un problème de santé rare;
- Vous conformer avec la réglementation;

- Conserver votre compétitivité;
- Offrir une expérience client plus agréable en créant la nouvelle version d'une plateforme.

Privilégiez un projet proportionné à vos objectifs et aux risques d'atteinte à la vie privée

Vous devez évaluer la **proportionnalité** tout au long du processus d'EFVP et de la mise en œuvre de ce projet.

La proportionnalité sera constatée si :

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

2.2. Déterminer la portée de l'évaluation

Par *portée*, on entend ce sur quoi portera l'EFVP, son objet.

Qu'allez-vous inclure dans votre EFVP?

Vous avez intérêt à délimiter clairement la portée de votre EFVP 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 système. **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 du 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 sans doute à un trop haut niveau.** Vous manquerez des éléments importants qui existent au niveau de la solution logicielle ou des procédures d'identification.

Exemple 4 : Pour le même projet, des EFVP distinctes ont récemment été réalisées 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.

Vous devriez être en mesure de justifier la portée de votre évaluation.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE ET LA PRÉCÉDENTE VOUS PERMETTENT D'Y INCLURE :

- La description du projet et de sa portée.

2.3. Définir les rôles et les responsabilités

C'est l'organisation détentrice des renseignements personnels qui a la responsabilité de réaliser l'EFVP. Celle-ci ne revient pas aux éventuels sous-traitants, fournisseurs ou partenaires (ex. chercheurs qui demandent accès aux renseignements), même si ceux-ci peuvent vous aider dans la réflexion et l'analyse de certains aspects.

La loi identifie des catégories ou groupes de personnes devant obligatoirement être consultées dans le cadre d'une EFVP :

- L'organisme public doit consulter, dès le début du projet, son **comité sur l'accès à l'information et la protection des renseignements personnels** dont fait partie le responsable de l'accès et de la protection des renseignements personnels;
- De son côté, l'entreprise doit consulter son **responsable de la protection des renseignements personnels**.

Certaines autres catégories de personnes peuvent être consultées en fonction de la portée du projet (voir section 2.2) et de l'évaluation d'ampleur que vous avez réalisée (voir section 2.5). Il peut s'agir, par exemple, des personnes responsables :

- Du projet;
- Des affaires juridiques;
- De la gestion documentaire;
- Des ressources humaines;
- Des relations avec la clientèle.

Il peut s'agir également :

- Des autorités compétentes de votre organisation devant prendre position sur la gestion des risques à la fin de la démarche (voir section 3.4);
- De représentants des personnes concernées;
- De vos clients ou partenaires corporatifs;
- De vos sous-traitants;
- De chercheurs, etc.

Précisez les **rôles et les responsabilités** de chacun des acteurs impliqués dans l'évaluation et le **moment où ils devront intervenir** dans la démarche d'EFVP.

Par exemple, certaines personnes devront être consultées dès le début du projet. D'autres personnes pourraient être consultées à un moment précis du projet en raison de leur expertise particulière, comme lorsqu'un enjeu en matière de protection des renseignements personnels est identifié. D'autres encore pourraient être mandatées pour suivre l'évolution du projet et ses conséquences sur la vie privée des personnes concernées.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET D'Y INCLURE :

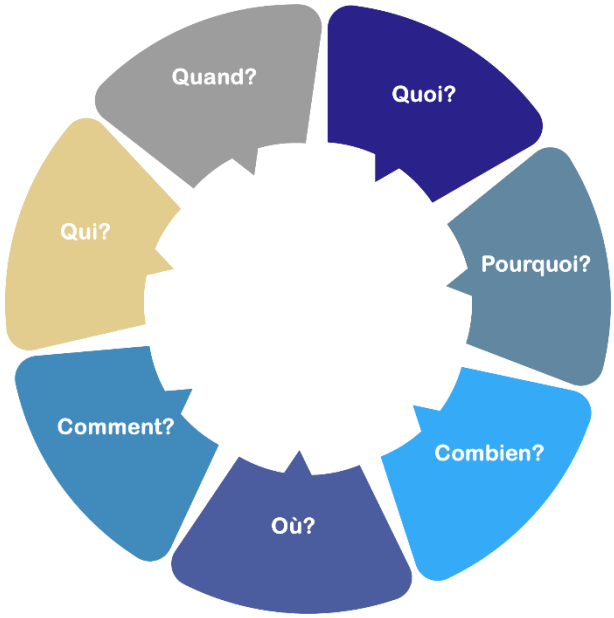
- La description des rôles et des responsabilités.

2.4. Inventorier et cartographier les renseignements personnels

Les renseignements personnels sont au cœur de votre évaluation. Faites l'inventaire des renseignements personnels et dressez une cartographie[9] (description, schéma, etc.) qui indiquera clairement le parcours de ces renseignements tout au long du projet.

Vous obtiendrez des informations qui vous permettront de déterminer l'ampleur de votre EFVP. Ces informations faciliteront aussi votre analyse de la conformité du projet avec la législation applicable et des risques d'atteinte à la vie privée qu'il comporte.

L'annexe 6 propose une liste de questions à vous poser à cette étape de la démarche.



2.4.1. Faire l'inventaire des renseignements personnels

L'inventaire des renseignements personnels vous permet d'en connaître la **nature** (p. ex. renseignements d'identité, médicaux, financiers), la **sensibilité**, la **quantité** et la **finalité**. Ces concepts sont présentés à la section 2.5.

La réalisation de l'inventaire est aussi incontournable pour vous assurer que vous ne recueillerez, utiliserez ou communiquerez que les renseignements personnels nécessaires à la réalisation du projet.

[9] En anglais, on utilise souvent le terme *data mapping*.

Une liste exhaustive de renseignements personnels n'est toutefois pas requise à toutes les étapes de l'EFVP. Par exemple, dans le rapport d'EFVP, une liste de regroupements de renseignements personnels apparentés pourrait suffire.

Ces regroupements contiennent des renseignements personnels possédant des caractéristiques communes et/ou qui permettent, ensemble, d'accomplir une fonction ou d'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, etc.);
- Dossiers médicaux, en version électronique et papier (résultats médicaux, résumés des rencontres, données de santé, imagerie médicale, etc.);
- Dossiers d'invalidité des employés détenus par les ressources humaines (renseignements d'identité, rapports médicaux, communications avec les assureurs, etc.);
- Courriels et enregistrements téléphoniques du centre d'appels (échanges avec les clients, contenu des questions et des réponses, échantillon de la voix, etc.);
- Données de journalisation du site Internet et outils d'analyse Web (historiques des pages consultées, adresse IP, navigateur et appareil utilisé, configuration de l'affichage, etc.).

Éléments à retenir

- Si vous n'êtes pas certain qu'un regroupement contient des renseignements personnels, conservez-le quand même et considérez-le dans votre EFVP.
- Incluez tous les renseignements que vous créez ou inférez sur les personnes (cote de crédit, note d'évaluation, note dans un dossier, etc.) : ce sont des renseignements personnels.
- Pensez aux renseignements collectés automatiquement par les appareils et les systèmes informatiques que vous utilisez (identifiant d'un appareil, journalisation d'une connexion, etc.).
- Incluez les renseignements dépersonnalisés, anonymisés et agrégés[10] 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 est nécessaire d'évaluer le risque de réidentification de ces renseignements.
- Même si vous ne présentez que des regroupements dans le rapport d'EFVP, il est important que votre organisation soit en mesure de connaître l'étendue de tous les renseignements personnels qu'elle détient.
- L'inventaire des renseignements personnels est évolutif. Tenez-le à jour pour rendre compte des changements susceptibles d'être survenus au sein de votre organisation (p. ex. nouvelle collecte de renseignements personnels pour un projet). Vous pourrez ainsi planifier adéquatement vos actions et respecter toutes vos obligations.

[10] 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.

2.4.2. Cartographier les renseignements personnels

La cartographie des renseignements personnels impliqués vise à illustrer leur parcours tout au long du projet, notamment leur **répartition** (entre des organisations, des personnes, des systèmes) et leur **support** de conservation à chaque étape. Ces concepts sont présentés à la section 2.4.

Dans un premier temps, à la lumière des réponses que vous aurez fournies aux questions liées à l'inventaire (voir section 2.4.1 et annexe 6), identifiez les **points où votre organisation entre en interaction** avec les renseignements personnels.

Les points d'interactions peuvent être :

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

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.

Cette cartographie peut prendre diverses formes, comme un tableau, un schéma ou un texte descriptif. Elle sera plus complexe pour les projets de plus grande envergure, de sorte qu'un découpage par processus pourrait s'avérer préférable, dans ces cas.

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.

Tenez compte de cette dimension en dressant votre cartographie.

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 pendant 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.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET D'Y INCLURE :

- Un aperçu de l'inventaire et de la cartographie des renseignements personnels.

2.5. Évaluer l'ampleur de l'EFVP à réaliser

Si une situation vous oblige légalement à réaliser l'EFVP (voir section 1), vous devez le faire, sans exception. Cependant, l'ampleur de l'EFVP peut varier en fonction de l'envergure du projet, de ses objectifs, de la nature des renseignements personnels impliqués et de la manière dont ils sont utilisés et communiqués. Il peut y avoir des variations dans :

- Le nombre d'acteurs à impliquer;
- Le temps à investir;
- Le niveau de détail d'un éventuel rapport (voir section 4);
- La documentation annexe à élaborer;
- La quantité de mesures prévues pour atténuer ou éliminer les risques;
- Le niveau de détail de ces mesures.

Ainsi, la Loi sur l'accès et la Loi sur le privé prévoient que l'EFVP doit être proportionnée[11] à :

1. La **sensibilité** des renseignements concernés;
2. La **finalité** de leur utilisation;
3. Leur **quantité**;
4. Leur **répartition**;
5. Leur **support.**

C'est à vous de déterminer l'ampleur de votre EFVP. Il est important de documenter les éléments qui guident votre décision à cet égard.

Sans être exhaustive, cette section propose des éléments de réflexion pertinents pour déterminer l'ampleur de votre EFVP.

2.5.1. Évaluer le degré de sensibilité des renseignements personnels

À quel point les renseignements personnels impliqués sont-ils **sensibles**?

Un renseignement personnel est sensible lorsqu'il suscite un haut degré d'attente raisonnable en matière de vie privée, en raison de sa nature ou du contexte de son utilisation ou de sa communication[12].

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 biométriques;
- Certains identifiants uniques.

Les renseignements peuvent aussi être considérés comme sensibles s'ils servent dans un projet affectant spécifiquement une population vulnérable (p. ex. personnes mineures, minorités ethnoculturelles, minorités sexuelles).

2.5.2. Évaluer la finalité de l'utilisation ou de la communication des renseignements personnels

Pour **quelle(s) fin(s)** les renseignements personnels seront-ils utilisés ou communiqués? Ces fins sont-elles généralement risquées pour les individus? Produisent-elles des effets importants (p. ex. juridiques) sur eux?

Exemples de finalités :

- Profiler, localiser ou identifier une personne;
- Effectuer une surveillance systématique ou généralisée;
- Établir le profil d'une personne (profil de consommateur, de conducteur, etc.) en combinaison avec d'autres renseignements;

[11] Loi sur l'accès, article 63.5; Loi sur le privé, article 3.3.
[12] Loi sur l'accès, article 65.1; Loi sur le privé, article 12.

- Rendre une décision automatisée à l'endroit d'une personne;
- Mener une étude ou une recherche ou produire des statistiques;
- Alimenter une nouvelle technologie aux effets moins connus.

2.5.3. Évaluer la quantité de renseignements personnels

Combien de renseignements personnels seront impliqués dans votre projet? Leur quantité influence-t-elle l'ampleur des risques prévisibles?

Exemples de questions à vous poser :

- Combien de personnes sont concernées par votre projet (nombre absolu ou proportion)?
- Quel est le volume ou l'étendue des renseignements personnels concernés (toutes catégories confondues : recueillis, observés, inférés, créés)?
- Quelle est la durée envisagée du projet? Est-il permanent ou temporaire?
- Quelle est l'extension géographique projetée?

2.5.4. Évaluer la répartition des renseignements personnels

Comment seront **répartis** les renseignements personnels impliqués dans votre projet? Considérez notamment les dimensions suivantes :

- **Spatiale –** Par exemple, où seront localisés les renseignements personnels (au sein ou à l'extérieur de l'organisation [conservation centralisée, décentralisée])? Dans quel pays seront hébergés les renseignements personnels impliqués dans votre projet?
- **Humaine ou administrative –** Par exemple, à qui seront communiqués les renseignements personnels impliqués dans le projet (p. ex. un prestataire de services)?
- **Quantitative –** Par exemple, combien de personnes auront accès à ces renseignements? Sur combien de supports ceux-ci seront-ils hébergés?

2.5.5. Évaluer le support de conservation des renseignements personnels

Sur quel(s) type(s) de **support(s)** seront conservés, momentanément ou à long terme, les renseignements personnels impliqués dans votre projet?

Ce critère est évalué en fonction de la nature des éléments matériels ou virtuels permettant de consigner, de conserver et de consulter l'information.

Exemples de caractéristiques de supports :

- Physique (tangible) ou numérique (ex. hébergement en infonuagique)
- Sécurisé ou non sécurisé
- Connecté avec d'autres systèmes ou non
- En mesure de préserver leur intégrité et leur confidentialité

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET D'Y INCLURE :

- Un aperçu des éléments justifiant l'ampleur de l'EFVP réalisée

2.6. Dresser la liste de vos obligations

Vos obligations en matière de protection des renseignements personnels 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 la Loi sur l'accès et la Loi sur le privé.

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

- *Code civil du Québec*;
- *Loi sur les archives*;
- *Loi concernant le cadre juridique des technologies de l'information*;
- *Code des professions*;
- *Loi sur l'administration fiscale*;
- *Code de la sécurité routière*;
- *Loi sur la protection de la jeunesse*;
- *Loi sur les services de santé et les services sociaux*;
- *Loi sur l'assurance maladie*.

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;
- La gestion du consentement est particulière pour les mineurs et les personnes majeures inaptes;
- La collecte et l'utilisation de renseignements biométriques[13] sont régies de manière spécifique et complémentaire par la *Loi concernant la cadre juridique des technologies de l'information*.

Sur les plans fédéral et 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

[13] Pour obtenir plus d'information, voir la section *Biométrie* du site Web de la Commission.

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 en 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 étrangers, informez-vous et considérez les effets que ces lois pourraient avoir sur votre projet.

Pratiques organisationnelles

Votre organisation peut encadrer la gestion des renseignements personnels de diverses façons, notamment 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.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET :

- De structurer votre analyse de conformité (tableau, titres de sections, etc.)

3. 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 effet positif ou négatif sur le respect de la vie privée des personnes concernées.

Rappelons que **ces facteurs sont :**

1. La conformité du projet à la législation applicable en matière de protection des renseignements personnels et le respect des principes l'appuyant (section 3.1);
2. L'identification des risques d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs conséquences (section 3.2);
3. La mise en place de stratégies pour éviter ces risques ou les réduire efficacement et leur maintien dans le temps (section 3.3).

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

Pour évaluer le **premier facteur relatif à la vie privée**, vous devrez vous **assurer de la conformité de votre projet à la législation applicable** en matière de protection des renseignements personnels **et aux principes l'appuyant**.

Suivez votre liste (voir la section 2.6) et évaluez dans quelle mesure vous respectez vos obligations. Cela peut impliquer des analyses juridiques, la documentation de certaines pratiques au sein de l'entreprise, etc.

Posez-vous les questions suivantes :

- Respectez-vous les **obligations** et les **principes**[14] de protection des renseignements personnels pour chacune des catégories de renseignements personnels, à chacun des points d'interaction, et ce, tout au long du cycle de vie des renseignements?
- Sinon, quelles sont les modifications que vous devez 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**.

[14] Pour un aperçu des principes généralement reconnus en matière de protection des renseignements personnels, consultez l'annexe 3.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET D'Y INCLURE :

- Une description des moyens mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels

3.2. Identifier les risques d'atteinte à la vie privée engendrés par votre projet et évaluer leurs conséquences

Pour évaluer le deuxième facteur relatif à la vie privée, vous devrez identifier les risques d'atteinte à la vie privée engendrés par le projet et évaluer leurs conséquences pour les personnes concernées.

3.2.1. Identifier les risques d'atteinte à la vie privée engendrés par votre projet

Qu'est-ce qu'un risque d'atteinte à la vie privée? Il s'agit d'une situation ou d'un événement futur qui peut ou non se réaliser et qui causerait une perte ou un préjudice à une personne quant au respect de son intimité ou de sa vie personnelle. Le risque est une *menace potentielle*.

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 d'atteinte à la réputation des personnes concernées), où être vécues de l'intérieur par les personnes concernées (**exemple** : sentiment d'intrusion).

Dans ce contexte, certains aspects légalement conformes d'un projet peuvent quand même être perçus comme une atteinte à la vie privée par les personnes concernées.

Vous devez donc établir des scénarios de risques pouvant découler de la mise en œuvre de votre projet.

Posez-vous les questions suivantes :

- Quels sont les événements ou les situations pouvant raisonnablement survenir pour chacun des renseignements personnels, à chacun des points d'interaction et tout au long du cycle de vie des renseignements?
- Quels sont les événements ou les situations pouvant 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 :

- Collecte excessive de renseignements;
- Création excessive ou non justifiée d'informations;
- Manque d'information fournie aux individus lors de la collecte;
- Divulgation non autorisée de renseignements personnels;
- Décision fondée sur des renseignements personnels inexacts ou équivoques;
- Vol de renseignements personnels;
- Intrusion dans la vie privée disproportionnée par rapport à l'objectif visé par le projet;

- Conservation de renseignements lorsque leur utilité n'est plus démontrée;
- Réidentification de renseignements préalablement anonymisés.

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 inspirer pour produire votre EFVP.

Décrire et évaluer les conséquences potentielles

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

Les **conséquences potentielles** sont variées :

- Vols d'identité et fraudes;
- Dangers pour la vie et la sécurité des personnes (comme les possibilités de harcèlement);
- Pertes financières ou d'opportunités;
- Dommages à la réputation;
- Sollicitations non désirées;
- Intrusions et autres nuisances dans la vie privée des personnes.

Les conséquences pour votre propre organisation ne doivent pas entrer en ligne de compte dans l'EFVP, qui vise à préserver la vie privée des personnes concernées. Bien que ces conséquences soient importantes, ne considérez pas dans l'EFVP :

- Les éventuels dommages à la réputation de votre organisation;
- Les litiges susceptibles de survenir;
- Les coûts potentiels que vous pourriez encourir;
- Etc.

Identifier les causes de ces risques

Précisez quelles seraient les causes de ces situations.

Les **causes potentielles** sont également variées :

- Processus déficient;
- Erreur dans la manipulation des renseignements;
- Manque de connaissances ou de formation;
- Mécanismes de surveillance insuffisants ou inexistants;
- Distribution inadéquate des responsabilités;
- Comportement malveillant;
- Collecte excessive de renseignements;
- Technologies défaillantes ou désuètes;
- Utilisation non justifiée ou non nécessaire de renseignements sensibles;
- Absence de consentement;
- Mécanismes insuffisants pour garantir l'exactitude des renseignements personnels;

- Existence d'un moyen de rechange moins intrusif et suffisamment efficace pour atteindre l'objectif déterminé.

Tenir 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 elle n'a jamais été utilisée auparavant.

L'utilisation de données biométriques est un exemple de technologies qui suscitent des questions et des enjeux particuliers[15]. On peut aussi penser à l'intelligence artificielle, notamment générative.

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

Projets d'envergure

Les projets de grande envergure génèrent souvent davantage de risques, qui peuvent toucher un plus grand nombre 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 s'impose.

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 (voir l'annexe 1).

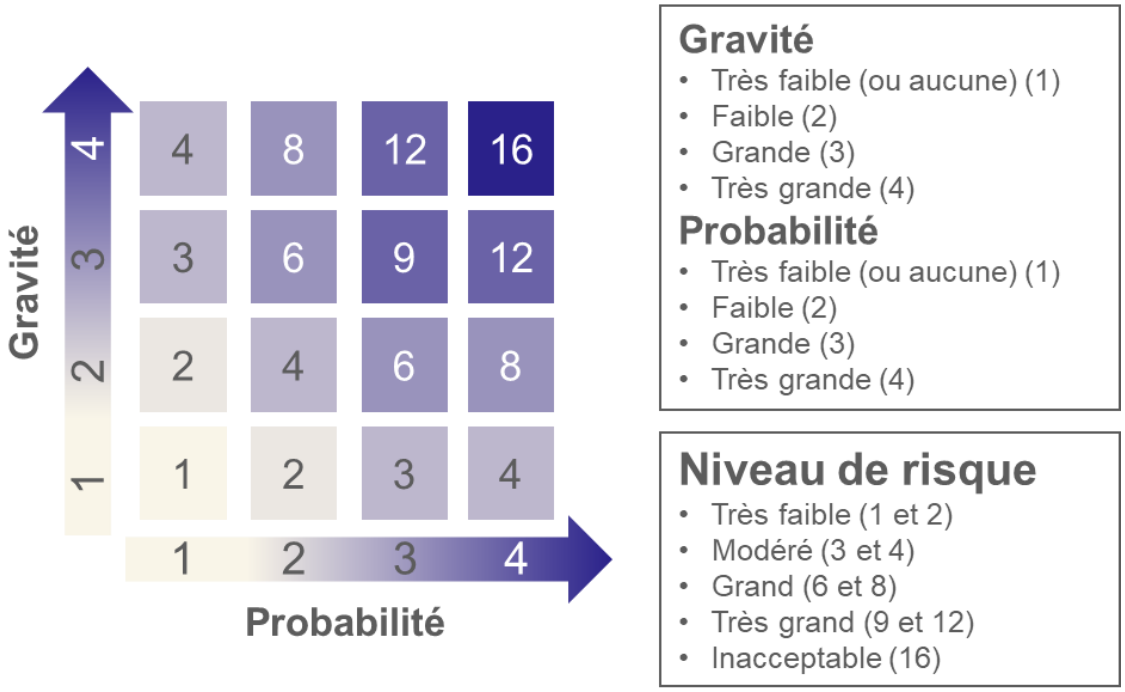
Des rapports d'évaluation éthique des nouvelles technologies sont fréquemment diffusés par des organismes indépendants ou des chercheurs universitaires. Ces documents abordent bien souvent des questions de vie privée. Ce sont des sources d'information pertinentes pour réfléchir aux enjeux et aux risques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

[15] 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.

3.2.2. Évaluer le niveau de chaque risque identifié

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 la **gravité potentielle des conséquences d'un événement** et de la **probabilité qu'il se concrétise** peut répondre aux objectifs de l'EFVP. Vous pouvez par exemple utiliser un système de cotes et une grille de niveau de risque :



L'évaluation du niveau de risque 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 la gravité des conséquences potentielles de chacun des risques identifiés

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

Exemple d'un système de cotes pour apprécier **la gravité d'un risque** :

- Très faible et/ou inexistante (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 un petit nombre de personnes;
- Grande (3) : le risque engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes;

- Très grande (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 la gravité des conséquences potentielles 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 (**exemples :** conséquences majeures pour la vie personnelle ou professionnelle des personnes concernées, conséquences sur leurs finances, procédures juridiques ou démarches qu'elles doivent mener pour résoudre la situation, danger pour leur vie ou leur sécurité);
- Le **nombre de personnes** potentiellement touchées 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 faibles et/ou inexistantes (1) : le risque n'a aucune chance de se concrétiser;
- Faibles (2) : le risque a peu de chances de se concrétiser ou un événement similaire ne s'est jamais produit;
- Grandes (3) : le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelques reprises;
- Très grandes (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 produire. **Soyez réaliste : évitez d'être trop confiant ou trop conservateur.**

Estimer le niveau de risque

Une fois que la gravité et la probabilité des risques sont estimées, vous devriez leur attribuer un niveau de risque global. Si vous utilisez un système de cotes, une façon simple de procéder est de multiplier la cote de gravité par la cote de probabilité, comme l'illustre la grille de niveau de risque en page 23.

Considérer les stratégies et les 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, communiqués 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.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET D'Y INCLURE :

- Une évaluation des risques (événements, causes, niveau de risque)

3.3. Mettre en place des stratégies pour éviter ou réduire les risques

Pour respecter le **troisième facteur relatif à la vie privée**, vous devrez **mettre en place des stratégies pour éviter ou réduire efficacement les risques** que comporte votre projet sur les personnes concernées.

Étudier les stratégies envisageables pour éviter ou réduire les risques

Les stratégies peuvent chercher à réduire soit la gravité des conséquences potentielles liées au risque, soit les probabilités que ce dernier se concrétise, soit les deux en même temps.

Ainsi, diminuer la quantité de renseignements personnels que vous collectez réduit les conséquences potentielles d'un vol de données. L'ajout de mesures de sécurité réduit plutôt les probabilités qu'un tel vol survienne.

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;
- Revoir périodiquement les paramètres de sécurité de la prestation électronique de services;
- 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 directement identificatoire 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. Songez à des solutions réalisables pour votre organisation.

Réévaluer le niveau de chacun des risques

À la lumière des stratégies et des moyens retenus, réévaluez le niveau d'importance 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 à 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. Si vous acceptez les risques du fait de leur faible probabilité ou de leur faible incidence, votre organisation doit néanmoins être en mesure d'en assumer la responsabilité.

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 projet

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 courir aux personnes concernées (voir section 2.1).

À la lumière de l'ensemble de votre EFVP, **est-ce que la solution que vous proposez pour atteindre vos objectifs paraît toujours proportionnelle, compte tenu des risques résiduels?**

En cas de plainte par une personne concernée ou de vérification par un organisme de contrôle, **serez-vous prêt à répondre aux questions de la Commission sur le fait que votre solution est proportionnelle?**

Il est possible que les risques résiduels soient trop importants et que vous deviez envisager des modifications substantielles à votre projet. Cela peut impliquer de recommencer l'EFVP en tout ou en partie, ou même de remettre en question le projet.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET D'Y INCLURE :

- Une description des stratégies d'élimination ou d'atténuation des risques

3.4. Faire le suivi de votre évaluation

Une fois que les facteurs relatifs à la vie privée sont évalués, vous devriez préparer la suite concrète de l'EFVP. Pour ce faire, vous devriez réaliser les étapes suivantes.

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 courantes 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 pourraient également être 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.

→ SI VOUS RÉDIGEZ UN RAPPORT D'EFVP (VOIR SECTION 4), CETTE ÉTAPE VOUS PERMET D'Y INCLURE :

- Un plan d'action

4. Rendre compte de l'évaluation

Bien qu'il soit possible de réaliser une EFVP sans la documenter formellement, vous devriez être en mesure d'expliquer et de justifier votre démarche d'EFVP. La rédaction d'un rapport est un bon moyen pour rendre compte de votre processus de réflexion lorsqu'il se termine ou lorsqu'une étape importante est franchie. Si vous rédigez un rapport, vous devriez le mettre à jour avec l'évolution de votre EFVP.

Ce rapport devrait être simple et accessible : tout lecteur devrait pouvoir comprendre quel est le projet, comment il est susceptible d'affecter la vie privée et comment vous avez considéré, mesuré et atténué les risques identifiés.

4.1. À quoi sert le rapport?

Un rapport d'EFVP sert **à documenter et 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 menée par une autorité réglementaire. De plus, lorsque la loi prévoit une obligation de transmettre une EFVP à la Commission, le rapport est un moyen approprié.

4.2. 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 (contexte) 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 les secteurs de votre organisation qui seront responsables de gérer les risques résiduels;
- Un résumé des consultations, s'il y a lieu;
- Un aperçu de l'inventaire et de la cartographie des renseignements personnels impliqués (catégorie(s) de renseignements impliqués, source(s) des renseignements, support(s), destinataire(s), interactions avec d'autres systèmes, etc.);
- Une évaluation des critères de sensibilité, de finalité, de quantité, de répartition et de support des renseignements personnels et une justification de la profondeur d'analyse (ampleur de l'EFVP);
- Une description des moyens mis en place pour respecter les obligations et les principes de protection des renseignements personnels (y compris sectoriels ou situationnels, au besoin);
- Une liste et une catégorisation des risques identifiés pour les personnes concernées;

- Les stratégies, mécanismes et mesures déployés pour éliminer ou réduire ces risques;
- Les personnes responsables de mettre en œuvre ces stratégies, mécanismes et mesures;
- Un plan d'action avec un échéancier comprenant une réévaluation périodique des mesures mises en place (**exemple** : un audit).

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

Autrement dit, les détails de l'approbation du rapport, y compris 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;
- Un résumé des avis de sécurité produits en collaboration avec des fournisseurs ou des partenaires (**exemple :** test d'intrusion);
- Les certifications obtenues dans le cadre de votre projet (quand un organisme d'évaluation certifie que votre produit ou service est conforme à certaines exigences).

La Commission propose un gabarit générique de rapport d'EFVP, que vous pouvez adapter à vos besoins. Il peut prendre toute autre forme permettant de rendre compte adéquatement de la démarche.

4.3. Le rapport devrait-il être diffusé?

À titre de bonne pratique de transparence, votre organisation pourrait décider de diffuser une version abrégée du rapport d'EFVP sur son site Web ou par tout autre moyen. Cette démarche peut témoigner d'un souci du respect de la loi et de l'information des personnes concernées.

Les organismes publics, en particulier, peuvent envisager de divulguer proactivement des résumés des EFVP concernant les projets touchant directement les citoyens.

→ À COMPLÉTER AU BESOIN :

- Un rapport d'EFVP

Faire évoluer l’EFVP en continu

Protéger les renseignements personnels n’est pas l’affaire d’une seule journée : l’EFVP n’est efficace que si elle évolue de façon continue et doit être revue au besoin, tout au long de la vie du projet.

Pour assurer l’efficacité de vos mesures de sécurité, vous devez en surveiller l’application et les réviser en fonction des risques émergents ou des changements apportés à votre projet : développement d’une nouvelle ligne d’affaires, projet d’implanter un service complémentaire au système transactionnel implanté, etc.

Des outils de contrôle actif des mesures, comme un tableau de bord de sécurité, vous permettront de surveiller l’application cohérente et intégrée des stratégies et des mesures que vous avez mises en place.

Annexe 1 – Communication à des fins d'étude, de recherche ou de production de statistiques

Articles 67.2.1 de la Loi sur l'accès et 21 de la Loi sur le privé

La **communication de renseignements personnels sans le consentement** des personnes concernées à une personne ou à un organisme (ci-après le chercheur) souhaitant utiliser ces renseignements **à des fins d'étude, de recherche ou de production de statistiques** (ci-après la recherche) est permise seulement si une EFVP conclut au respect de certains critères.

Qui doit réaliser l'évaluation : l'organisation ou le chercheur?

C'est l'organisation détentrice des renseignements personnels qui devrait réaliser l'EFVP en se basant notamment sur les éléments fournis par le chercheur. En effet, ce dernier est bien placé, par exemple, pour décrire la façon dont les renseignements personnels seront utilisés après leur communication, en quoi ils sont nécessaires à la recherche et les mesures de sécurité applicables sur place.

Notez que la décision d'un comité d'éthique de la recherche **ne peut remplacer l'EFVP que doit réaliser l'organisation détentrice** des renseignements personnels. Toutefois, son contenu et ses recommandations peuvent être utiles lors de l'EFVP.

Comment réaliser cette EFVP?

Cette EFVP peut être réalisée en suivant la démarche générale présentée dans ce guide. Toutefois, l'EFVP devrait permettre de motiver votre conclusion quant au respect de chacun des cinq critères prévus par la loi.

1. L'objectif poursuivi par la recherche peut être atteint seulement si les renseignements sont communiqués sous une forme permettant d'identifier les personnes concernées

Par exemple, s'il est possible de réaliser la recherche ou l'étude à l'aide de **renseignements anonymisés**[16] ou de données synthétiques, la communication de renseignements personnels n'est pas autorisée.

Si la recherche peut être menée en utilisant des **renseignements dépersonnalisés**[17], seuls ces renseignements devraient être communiqués. Il importe de souligner que ces renseignements constituent tout de même des renseignements personnels confidentiels. Il appartient au chercheur de vous convaincre de la nécessité d'utiliser des renseignements personnels, dépersonnalisés ou non. L'utilisation de renseignements non dépersonnalisés requiert une démonstration convaincante de l'impossibilité de réaliser la recherche sans les « identifiants directs ».

2. Il est déraisonnable d'exiger que le chercheur obtienne le consentement des personnes concernées en matière de protection des renseignements personnels et de leur droit au respect de la vie privée

Comme il s'agit d'une exception au principe du consentement, l'organisation doit pouvoir conclure qu'il est déraisonnable d'exiger le consentement de toutes les personnes dont les renseignements sont requis aux fins de la recherche. Cela pourrait être le cas, notamment, dans les situations suivantes. Ces exemples ne sont pas limitatifs et, dans tous les cas, doivent être contextualisés par rapport à la recherche spécifique évaluée.

- Il peut être déraisonnable d'obtenir le consentement de milliers de personnes dont les coordonnées ne sont pas à jour;
- La recherche pourrait viser les renseignements de personnes inaptes à consentir ou encore décédées;
- La recherche pourrait s'appuyer sur des renseignements dépersonnalisés détenus par votre organisation, rendant impossible pour le chercheur d'obtenir le consentement;
- Dans certains cas, la constitution d'un échantillon représentatif pourrait nécessiter de ne pas introduire un biais en utilisant seulement les données de personnes désireuses de consentir.

3. L'objectif poursuivi l'emporte, par rapport à l'intérêt public, sur les conséquences de la communication et de l'utilisation des renseignements personnels sur la vie privée des personnes concernées

Cette partie de l'EFVP vise à pondérer l'objectif de la recherche en termes d'intérêt public et les conséquences de la communication et de l'utilisation des renseignements personnels sur la vie privée des personnes concernées.

---

[16] Un renseignement est **anonymisé** quand il est raisonnable de prévoir dans les circonstances qu'en tout temps et de façon irréversible, il ne permet plus d'identifier directement ou indirectement une personne. L'anonymisation des renseignements doit se faire selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement. Consultez la page Web *Distinguer anonymisation et dépersonnalisation* pour en apprendre davantage.

[17] Un renseignement est **dépersonnalisé** quand il empêche d'identifier directement la personne concernée.

Cette analyse doit d'abord identifier et décrire les différents éléments et les facteurs à considérer pour réaliser cette pondération.

Vous devez ensuite déterminer si l'objectif de la recherche au regard de l'intérêt public l'emporte sur ses conséquences possibles sur la vie privée des personnes concernées.

Voici quelques exemples de questions à vous poser pour évaluer la demande d'un chercheur :

- Quel est l'objectif de la recherche et en quoi est-elle d'intérêt public?
- Quels bénéfices sont attendus pour la société?
- Quelles sont les différentes conséquences sur la vie privée des personnes concernées par la communication de renseignements?
- Ces conséquences peuvent-elles être minimisées dans le cadre de la recherche? Si oui, comment?
- Les renseignements personnels demandés sont-ils sensibles?
- Les renseignements seront-ils couplés ou comparés à d'autres? Si oui, quelles en seront les conséquences sur la vie privée des personnes concernées? Est-ce que ces pratiques auront un effet sur les risques de divulgation de renseignements personnels au sujet d'une ou de plusieurs personnes?
- Qu'est-ce qui permet de croire que l'intérêt public l'emporte sur les conséquences de la communication et de l'utilisation des renseignements personnels sur la vie privée des personnes concernées?

Attention : l'évaluation de ce critère ne se limite pas à exposer l'objectif de la recherche ni à énoncer simplement un effet général, comme le fait qu'elle permettra d'accroître les connaissances dans un domaine d'activité. Il faut préciser les bénéfices attendus de la recherche en lien avec l'intérêt public et les pondérer avec les conséquences sur la vie privée des individus dont les renseignements seront utilisés aux fins de la recherche.

4. Les renseignements personnels sont utilisés de manière à en assurer la confidentialité

Dans cette partie de l'analyse, il faut évaluer si l'utilisation projetée des renseignements et les différentes mesures de protection qui seront mises en place permettent d'en assurer la confidentialité. Celle-ci doit être assurée lorsque vous les communiquez, mais aussi à toutes les étapes de la recherche. Cette évaluation devrait notamment tenir compte de la sensibilité et de la quantité des renseignements personnels.

5. Seuls les renseignements nécessaires sont communiqués

L'EFVP doit indiquer comment l'organisation s'assurera que seuls les renseignements nécessaires à la recherche seront communiqués au chercheur. Une attention particulière devrait être apportée aux « identifiants directs et indirects » (en lien avec le premier critère, par exemple : adresse, code postal complet, numéro d'assurance maladie, date de naissance ou âge) et aux renseignements particulièrement sensibles.

Quelles sont les étapes suivant l'EFVP?

Vous devez conclure avec le chercheur une entente écrite dont le contenu est précisé dans la Loi sur l'accès et la Loi sur le privé. Vous devez ensuite la transmettre à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission.

Un rapport d'EFVP devrait-il être transmis à la Commission?

Oui, il est attendu qu'un rapport d'EFVP (voir section 4) accompagne l'entente transmise à la Commission. Un document écrit attestant de la démarche d'EFVP permet à votre organisation de démontrer qu'elle a respecté son obligation. Il permet de comprendre comment chacun des critères a été analysé et quels éléments ont été considérés.

Annexe 2 – Acquisition, développement ou refonte d'un système d'information ou de prestation électronique de services

Articles 63.5 de la Loi sur l'accès et 3.3 de la Loi sur le privé

Une EFVP est requise pour tout projet lié à un **système d'information ou de prestation électronique de services** impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Il peut s'agir d'un projet :

- D'acquisition;
- De développement;
- De refonte.

Un **système d'information** peut revêtir de multiples formes. Il n'est pas nécessairement informatisé, quoique cela soit fréquent. Il peut s'agir entre autres d'un :

- Système informatique de traitement des dossiers;
- Logiciel de vidéoconférence ou de collaboration;
- Système biométrique;
- Système d'intelligence artificielle;
- Système de cartes à puce/RFID;
- Système de vidéosurveillance;
- Système statistique;
- Système de gestion de la paie.

Un **système de prestation électronique de services** peut notamment prendre la forme :

- D'une borne libre-service;
- D'un service de paiement par RFID/NFC;
- D'une zone membre d'un site Web;
- D'un dossier électronique;
- D'une application mobile.

Droit à la portabilité des renseignements personnels

En plus de réaliser une EFVP, vous devez vous assurer que votre projet permette qu'un renseignement personnel informatisé recueilli auprès de la personne concernée lui soit communiqué dans un format technologique structuré et couramment utilisé.

En effet, à partir du 22 septembre 2024[18], si la personne concernée le demande, votre organisation aura l'obligation de lui communiquer, dans un format technologique structuré et couramment utilisé, un renseignement personnel informatisé recueilli auprès d'elle.

Cette communication pourra aussi se faire à une personne ou à un organisme autorisé à recueillir le renseignement, à la demande de la personne concernée.

[18] Cette obligation, apportée par la Loi 25, sera intégrée aux articles 84 de la Loi sur l'accès et 27 de la Loi sur le privé.

Annexe 3 – Communication de renseignements personnels à l'extérieur du Québec

Articles 70.1 de la Loi sur l'accès et 17 de la Loi sur le privé

Une EFVP est requise :

- Avant de **communiquer** un renseignement personnel à **l'extérieur du Québec**;
- Avant de **confier à une personne ou à un organisme à l'extérieur du Québec** la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour votre compte un tel renseignement.

Aux fins de votre évaluation, vous devez notamment tenir compte des éléments suivants :

- La sensibilité du renseignement;
- La finalité de son utilisation;
- Les mesures de protection, y compris celles qui sont contractuelles, dont le renseignement bénéficierait;
- Le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables.

Vous pouvez communiquer les renseignements si l'EFVP démontre que le renseignement bénéficierait d'une **protection adéquate**, notamment au regard des **principes de protection des renseignements personnels généralement reconnus**.

Qu'entend-on par « principes de protection des renseignements personnels généralement reconnus »?

La Loi sur l'accès et la Loi sur le privé ne définissent pas ce que sont les « principes de protection des renseignements personnels généralement reconnus ».

On peut toutefois penser qu'il s'agit de règles générales permettant d'assurer la protection des renseignements personnels, mais également le respect des droits et des intérêts des personnes concernées en cette matière.

Sans être exhaustive ou définitive, la liste suivante présente des principes intégrés dans de nombreuses lois sur la protection des renseignements personnels et dans d'autres documents significatifs en cette matière, comme des normes ou des lignes directrices[19] :

- **Responsabilité :** les organisations sont imputables quant à leur gestion des renseignements personnels. Elles mettent en place des politiques et des pratiques propres à les protéger et déploient les moyens financiers et humains nécessaires pour ce faire, notamment en désignant une personne responsable. Elles documentent leur conformité et leurs décisions en matière de protection des renseignements personnels.
- **Détermination des fins :** les fins pour lesquelles les organisations recueillent des renseignements personnels sont légitimes et établies avant la collecte.
- **Limitation de la collecte :** les organisations recueillent uniquement les renseignements nécessaires aux fins déterminées. La collecte se fait par des moyens licites et équitables. Elle minimise l'atteinte à la vie privée.
- **Consentement :** les personnes sont adéquatement informées des fins déterminées et y consentent librement, à moins d'exception.
- **Protection dès la conception et par défaut :** les produits/services sont conçus dans le respect de la vie privée des personnes. S'ils incluent des paramètres de confidentialité, ceux-ci protègent la vie privée par défaut.
- **Limitation de l'utilisation, de la communication et de la conservation :** les organisations utilisent et communiquent les renseignements personnels recueillis aux fins déterminées ou à des fins compatibles, sauf consentement ou exception légale. Elles limitent l'accès à ces renseignements personnels aux personnes autorisées et ne les conservent pas plus longtemps que nécessaire.
- **Exactitude :** les organisations tiennent les renseignements personnels à jour et s'assurent qu'ils sont exacts et complets au moment où elles les utilisent ou les communiquent.
- **Sécurité :** les organisations prennent des mesures de sécurité appropriées pour protéger en tout temps les renseignements qu'elles détiennent contre la perte, le vol ou la modification, la communication ou la destruction non autorisée. Ces mesures sont appropriées à la sensibilité des renseignements et au contexte. En cas d'incident, les organisations réagissent promptement et avertissent les personnes concernées et les autorités, sauf exception.
- **Transparence :** les organisations fournissent les informations pertinentes aux personnes concernées au moment de la collecte ou du consentement. Elles diffusent au public leurs coordonnées et des informations claires sur leurs politiques et pratiques de gestion des renseignements personnels.
- **Droits des personnes concernées :** les personnes peuvent accéder aux renseignements personnels qui les concernent et en demander la rectification ou, dans certains cas, la suppression. Les organisations établissent des processus accessibles pour permettre l'exercice de ces droits.

[19] Voir notamment les Lignes directrices de l'OCDE régissant la protection de la vie privée, les Fair Information Practice Principles (FIPPs) de la Federal Trade Commission américaine, et les principes qui sous-tendent des lois comme la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada et le *Règlement général sur la protection des données* de l'Union européenne.

- **Recours :** en cas d'insatisfaction, les personnes peuvent contester un refus d'exercice d'un droit ou porter plainte auprès de l'organisation ou d'une instance compétente.

Qu'est-ce qu'une « protection adéquate »?

Encore ici, la Loi sur l'accès et la Loi sur le privé ne définissent pas l'expression « protection adéquate ».

On peut penser qu'il s'agit d'une protection offrant des garanties **juridiques** (législation de l'État de destination) et **contractuelles** (entente avec l'organisation destinataire) respectant l'ensemble des principes de protection généralement reconnus et appropriés en regard de la sensibilité et de la finalité des renseignements impliqués.

Si vous concluez que les renseignements personnels ne bénéficieront pas d'une protection adéquate, vous devez refuser de les communiquer ou vous abstenir de les confier à un tiers hors du Québec.

Que doit contenir l'entente écrite faisant suite à l'EFVP?

La communication de renseignements personnels hors du Québec doit faire l'objet d'une entente écrite entre le tiers et vous. Celle-ci doit tenir compte notamment des résultats de l'EFVP. Au besoin, elle doit inclure des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation afin de parvenir à une protection adéquate.

Annexe 4 – Collecte par un organisme public pour le compte d'un autre

Article 64 de la Loi sur l'accès

Une EFVP est requise lorsqu'un organisme public :

- Recueille un renseignement personnel nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme d'un autre organisme public avec lequel il collabore;
- Recueille ce type de renseignement pour la prestation de services ou la réalisation d'une mission commune.
    - Par exemple, un organisme peut recueillir un renseignement personnel aux fins de vérifier l'admissibilité de personnes à un programme qu'il administre.

Des dispositions transitoires s'appliquent pour les ententes déjà en vigueur à la date où cette EFVP devient obligatoire, à savoir le 22 septembre 2023[20].

Qui doit réaliser l'évaluation?

C'est l'organisme qui sera ultimement détenteur des renseignements personnels, c'est-à-dire celui qui demande à un autre organisme public de recueillir des renseignements personnels pour son compte, qui devrait réaliser l'EFVP, en collaborant, au besoin, avec l'organisme qui l'assiste. En effet, ce dernier est bien placé, par exemple, pour décrire la façon dont les renseignements personnels seront recueillis, avec quelles mesures de sécurité, etc.

Quelles sont les étapes suivant l'EFVP?

Les organismes qui collaborent doivent conclure une entente écrite dont le contenu est précisé à l'article 64 de la Loi sur l'accès. Ils doivent ensuite la transmettre à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission.

[20] Les ententes conclues en vertu des articles 64 et 68 de la Loi sur l'accès avant le 22 septembre 2023 demeurent en vigueur jusqu'au 22 septembre 2025 ou jusqu'à leur date d'expiration, selon la première de ces dates (article 174 de la Loi 25). Pour **reconduire** ou **modifier** l'entente, il sera désormais nécessaire de réaliser une EFVP.

Un rapport d'EFVP devrait-il être transmis à la Commission?

Oui, il est attendu qu'un rapport d'EFVP (voir section 4) accompagne l'entente transmise à la Commission. Un document écrit attestant de la démarche d'EFVP permet à votre organisation de démontrer qu'elle a respecté son obligation.

Annexe 5 – Autres types de communications sans consentement (secteur public)

Article 68 de la Loi sur l'accès

Une EFVP doit aussi être menée et conclure au respect de certains critères avant qu'un **organisme public communique un renseignement personnel sans consentement** :

- À un autre organisme public, au Québec ou ailleurs :
  - Pour l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion;
  - Lorsque la communication est manifestement au bénéfice de la personne concernée;
- À toute personne ou à tout organisme :
  - Lorsque des circonstances exceptionnelles le justifient;
  - Pour la prestation, par un organisme public, d'un service à rendre à la personne concernée, notamment à des fins d'identification.

Des dispositions transitoires s'appliquent pour les ententes déjà en vigueur à la date où cette EFVP devient obligatoire, à savoir le 22 septembre 2023[21].

Qui doit réaliser l'évaluation?

C'est l'organisation détentrice des renseignements personnels qui devrait réaliser l'EFVP, en collaborant, au besoin, avec le destinataire de la communication. En effet, ce dernier est bien placé, par exemple, pour décrire la façon dont les renseignements personnels seront utilisés après leur communication et les mesures de sécurité applicables sur place.

Comment réaliser cette EFVP?

Pour que ces autres types de communication puissent être effectués, l'EFVP doit permettre de conclure que les quatre critères suivants sont respectés :

[21] Les ententes conclues en vertu des articles 64 et 68 de la Loi sur l'accès avant le 22 septembre 2023 demeurent en vigueur jusqu'au 22 septembre 2025 ou jusqu'à leur date d'expiration, selon la première de ces dates (article 174 de la Loi 25). Pour **reconduire** ou **modifier** l'entente, il sera désormais nécessaire de réaliser une EFVP.

1. L'objectif ne peut être atteint que si le renseignement est communiqué sous une forme permettant d'identifier la personne concernée

Par exemple, s'il est possible d'atteindre l'objectif de la communication à l'aide de **renseignements anonymisés** ou de données synthétiques, la communication de renseignements personnels n'est pas autorisée.

Si l'objectif de la communication peut être atteint en utilisant des **renseignements dépersonnalisés**, seuls ces renseignements devraient être communiqués. Il importe de souligner que ces renseignements constituent tout de même des renseignements personnels confidentiels. Il appartient à l'organisme public de justifier la nécessité d'utiliser des renseignements personnels, dépersonnalisés ou non.

L'utilisation de renseignements non dépersonnalisés requiert une démonstration convaincante de l'impossibilité de réaliser la communication sans les « identifiants directs ».

2. Il est déraisonnable d'exiger l'obtention du consentement de la personne concernée

Comme il s'agit d'une exception au principe du consentement, vous devez pouvoir conclure qu'il est déraisonnable d'exiger le consentement de toutes les personnes dont les renseignements sont requis aux fins de la communication envisagée.

3. L'objectif poursuivi l'emporte, par rapport à l'intérêt public, sur les conséquences de la communication et de l'utilisation des renseignements personnels sur la vie privée des personnes concernées

Cette partie de l'EFVP vise à pondérer l'objectif de la communication en termes d'intérêt public et les conséquences de la communication et de l'utilisation des renseignements personnels sur la vie privée des personnes concernées.

Cette analyse doit d'abord identifier et décrire les différents éléments et facteurs à considérer pour réaliser cette pondération.

Vous devez ensuite déterminer si l'objectif de la communication au regard de l'intérêt public l'emporte sur les conséquences possibles sur la vie privée des personnes concernées.

Voici quelques exemples de questions à vous poser pour évaluer la communication envisagée auprès d'un autre organisme public :

- Quel est l'objectif de la communication et en quoi est-elle d'intérêt public?
- Quels bénéfices sont attendus pour les personnes concernées et pour la société?
- Quelles sont les différentes conséquences sur la vie privée des personnes concernées par la communication de renseignements?
- Ces conséquences peuvent-elles être minimisées dans le cadre de la communication? Si oui, comment?
- Les renseignements personnels impliqués sont-ils sensibles?
- Les renseignements seront-ils couplés ou comparés à d'autres? Si oui, quelles en seront les conséquences sur la vie privée des personnes concernées? Est-ce que ces pratiques auront une

influence sur les risques de divulgation de renseignements personnels au sujet d'une ou de plusieurs personnes?

- Qu'est-ce qui permet de croire que l'intérêt public l'emporte sur les conséquences de la communication et de l'utilisation des renseignements personnels sur la vie privée des personnes concernées?

Ainsi, l'évaluation de ce critère ne se limite pas à exposer l'objectif de la communication ni à énoncer simplement un effet général, comme « l'amélioration des services ». Il faut préciser les bénéfices attendus de la communication envisagée en lien avec l'intérêt public et les pondérer avec les conséquences sur la vie privée des individus dont les renseignements seront communiqués.

4. Le renseignement personnel est utilisé de manière à en assurer la confidentialité

Dans cette partie de l'analyse, il faut déterminer si l'utilisation projetée des renseignements et les différentes mesures de protection qui seront mises en place lors de leur communication par l'organisation permettent d'en assurer la confidentialité. Cette évaluation devrait notamment tenir compte de la sensibilité et de la quantité des renseignements personnels.

Quelles sont les étapes suivant l'EFVP?

Vous devez conclure avec le tiers une entente écrite dont le contenu est précisé à l'article 68 de la Loi sur l'accès. Vous devez ensuite la transmettre à la Commission. L'entente entre en vigueur 30 jours après sa réception par la Commission.

Un rapport d'EFVP devrait-il être transmis à la Commission?

Oui, il est attendu qu'un rapport d'EFVP (voir section 4) accompagne l'entente transmise à la Commission. Un document écrit attestant de la démarche d'EFVP permet à votre organisation de démontrer qu'elle a respecté son obligation. Il permet de comprendre comment chacun des critères a été analysé et quels éléments ont été considérés.

Annexe 6 – Inventaire et cartographie des renseignements personnels : aide à la réflexion

Pour faire l'inventaire des renseignements personnels et dresser une cartographie, les questions suivantes peuvent guider votre réflexion. Elles peuvent vous aider à indiquer le parcours des renseignements identifiés tout au long du projet.

Questions	Sous-questions
Quoi?	✓ Quels **types de renseignements** personnels seront collectés, communiqués, utilisés ou conservés dans le cadre de ce projet? ✓ Quelle est la nature de ces renseignements (ex. sont-ils **sensibles**)?
Pourquoi?	✓ Pourquoi souhaitez-vous recueillir, utiliser, communiquer ou conserver des renseignements personnels? ✓ Quelle est la **finalité** de l'utilisation de ces renseignements dans le cadre de votre projet? ✓ En quoi l'accès à ces renseignements est-il nécessaire à l'exercice des fonctions des personnes qui y auront accès?
Combien?	✓ Quelle **quantité** de renseignements personnels sera impliquée dans votre projet? ✓ Combien de personnes seront concernées par votre projet (nombre absolu ou proportion)? ✓ Quel est le volume ou l'étendue des renseignements personnels concernés? ✓ Quelle est la durée envisagée du projet? ✓ Quelle est l'extension géographique projetée?
Qui?	✓ Quelles catégories de personnes auront accès à ces renseignements dans l'organisation ou à l'extérieur (tiers)?
Comment?	✓ Comment ou par quels moyens les renseignements personnels seront-ils collectés, utilisés, communiqués ou conservés au sein (ou à l'extérieur) de l'organisation? ✓ Comment l'organisation disposera-t-elle de ces renseignements une fois que la finalité justifiant leur collecte (ou leur communication ou leur utilisation) sera atteinte? ✓ Quelle sera la méthode de destruction (ou d'anonymisation) utilisée?
Où?	✓ Où ces renseignements seront-ils **répartis** et conservés au sein (ou à l'extérieur) de l'organisation? ✓ Sur quel(s) type(s) de **support** et dans quelles conditions seront-ils conservés?
Quand?	✓ Quand les renseignements seront-ils détruits ou anonymisés?

Montréal
2045, rue Stanley
Bureau 900
Montréal (Québec) H3A 2V4
Téléphone : 514 873-4196

Québec
525, boul. René-Lévesque Est
Bureau 2.36
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741

Commission d'accès à l'information du Québec

1 888 528-7741 | cai.gouv.qc.ca