Réaliser une évaluation des facteurs relatifs à la vie privée

Guide d’accompagnement à la démarche et à sa documentation

Avril 2024

Commission d'accès à l'information du Québec

Version 3.1 – Avril 2024

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

Cette version 3.1 a été révisée aux plans visuel et structurel, mais le contenu demeure essentiellement le même.

Ce guide concerne la Loi sur l'accès et la Loi sur le privé

Ce guide porte sur la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès) et sur la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé).

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 sa publication. Les organisations publiques et privées doivent respecter le cadre juridique en vigueur en matière de protection des renseignements personnels.

Ce guide est explicatif et ne remplace pas les lois

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 icônes utilisées dans ce guide

Dans le guide, vous retrouverez des bandeaux informatifs de quatre types, identifiés par leur icône :

- Terminologie
- Particularité juridique
- Recommandation ou bonne pratique
- Mise en garde

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

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.

Introduction

Quel est l'objectif de ce guide ?

Ce guide vise à vous accompagner pour :

- Déterminer si vous avez l'obligation de réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) pour un projet donné;
- Réaliser l'EFVP;
- Rédiger un rapport d'EFVP, au besoin;
  - Le guide permet de mieux utiliser le modèle générique de rapport proposé par la Commission.

> Dans ce guide, le terme « **projet** » désigne tout projet, technologique ou autre, susceptible d'impliquer la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Il peut s'agir, par exemple, du stockage de renseignements personnels en infonuagique à l'extérieur du Québec, de l'achat d'un système d'information ou d'un projet de communication de renseignements personnels à un chercheur.

À qui s'adresse ce guide ?

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

> Dans ce guide, le terme « **organisation** » désigne les entreprises et organisations privées et les organismes publics soumis aux lois sur la protection des renseignements personnels.

De manière secondaire, ce guide pourra aussi être utile à plusieurs autres personnes, selon le cas, par exemple le dirigeant de l'organisation, les responsables des affaires juridiques, de la gestion des risques, de la sécurité, de l'éthique ou de la gestion documentaire, ou encore les chercheurs.

Est-il obligatoire de suivre ce guide ?

Non. La loi ne précise pas comment réaliser une EFVP. Elle ne détermine pas non plus le contenu et la forme d'un rapport qui rendrait 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, votre rapport.

Qu'est-ce qu'une EFVP ?

L'EFVP[1] 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[2]. 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 sur la vie privée** des personnes concernées. Ces facteurs sont les suivants :

A. Conformité à la législation et aux principes

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

B. Analyse des risques

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

C. Stratégies d'atténuation

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

Typiquement, l'EFVP est documentée dans un rapport, qui peut être mis à jour au fil de son évolution. **La Commission propose un modèle générique de rapport d'EFVP, que vous gagnez à consulter en même temps que ce guide.**

1. En anglais, l'EFVP est généralement appelée *privacy impact assessment* (PIA) ou *data protection impact assessment* (DPIA).
2. 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 environnementale, de l'évaluation d'incidence algorithmique ou de l'étude d'impact sur les droits de la personne. Toutes impliquent des étapes similaires.

Pourquoi réaliser une EFVP ?

L'EFVP est une **obligation légale dans plusieurs situations**. C'est donc souvent une question de conformité ! Elle peut toutefois être menée à titre de bonne pratique.

L'EFVP permet de **protéger les personnes** concernées par un projet, de la collecte de leurs renseignements personnels à leur destruction[3]. Elle mène aussi à la **mise en place de stratégies appropriées pour respecter vos obligations** en matière de protection de ces renseignements. Enfin, elle est un outil important pour **éviter ou atténuer les conséquences** que causerait une gestion inadéquate de ces renseignements (incidents de confidentialité, poursuites, atteintes à l'image, etc.).

Par essence, l'EFVP constitue donc un outil précieux pour réfléchir à la **nécessité** et à la **proportionnalité** de votre projet et les démontrer, en tenant compte de ses objectifs et des risques d'atteinte à la vie privée qu'il engendre. Ces deux notions sont fondamentales en matière de protection des renseignements personnels et sont des **conditions incontournables de légalité**.

Si vous ne pouvez justifier la nécessité et la proportionnalité de votre projet au terme de l'EFVP, en tenant compte des stratégies d'atténuation envisagées, vous devrez y apporter des modifications plus substantielles ou prendre la décision d'y mettre un terme.

À quel moment 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.

3. Les lois prévoient désormais la possibilité d'anonymiser les renseignements personnels au lieu de les détruire, dans certains cas.

Aperçu de la démarche d'EFVP

Étape 1

Déterminer si une évaluation est requise

Pages 10-13

Cette étape vous permettra de savoir si vous devez faire une évaluation.

Étape 2

Définir votre projet et l'objet de l'évaluation

Pages 14-18

Cette étape vous permettra de partir du bon pied en définissant votre projet et en décidant ce que vous devez inclure dans votre évaluation.

Étape 3

Préparer l'évaluation

Pages 19-30

Cette étape vous permettra de faire l'inventaire des renseignements personnels, de tracer leur parcours et de déterminer l'ampleur de votre évaluation. Vous devrez aussi recenser les obligations de votre organisation.

Étape 4

Évaluer les facteurs relatifs à la vie privée et adopter les stratégies appropriées

Pages 31-42

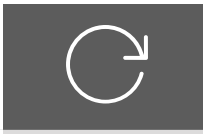
Cette étape vous permettra d'évaluer la conformité de votre projet et les risques associés, et de déterminer les mesures à mettre en place pour éliminer ou atténuer ces risques.

Étape 5

Rédiger un rapport

Pages 43-46

Cette étape vous permettra de documenter votre démarche et de démontrer le respect de vos obligations.

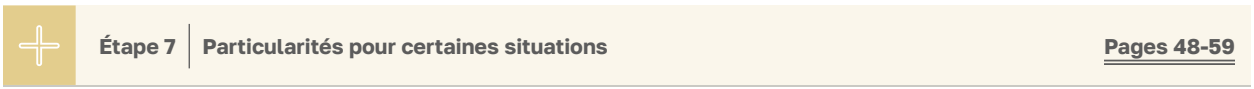


Étape 6

Maintenir l'évaluation à jour

Page 47

Cette étape vous permettra de réviser votre évaluation et de la tenir à jour au fil du temps.



Étape 7 | **Particularités pour certaines situations**

Pages 48-59

Table des matières

1. Déterminer si une évaluation est requise **10**

1.1 Une évaluation est obligatoire dans cinq situations principales **11**

1.2 Si vous avez déjà réalisé une évaluation, mettez-la à jour **13**

1.3 Si votre projet n'implique pas de renseignements personnels, une évaluation n'est pas obligatoire **13**

2. Définir votre projet et l'objet de l'évaluation **14**

2.1 Définir votre projet et ses objectifs **15**

Présenter le projet et son contexte 15

Expliquer les objectifs du projet 15

Évaluer d'emblée la nécessité et la proportionnalité du projet 16

2.2 Déterminer l'objet de l'évaluation **17**

2.3 Définir les rôles et les responsabilités **17**

À qui revient la responsabilité de réaliser l'évaluation ? 18

Qui doit être impliqué dans l'évaluation ? 18

3. Préparer l'évaluation **19**

3.1 Faire l'inventaire des renseignements personnels impliqués **20**

Pourquoi faire l'inventaire des renseignements personnels ? 20

Comment structurer l'inventaire ? 21

Comment regrouper les renseignements personnels ? 22

Quand mettre à jour l'inventaire des renseignements personnels ? 22

3.2 Tracer le parcours des renseignements personnels **23**

Identifier les points d'interaction avec les renseignements personnels 23

Tracer le parcours des renseignements personnels tout au long du projet 24

3.3 Déterminer l'ampleur de l'EFVP à réaliser **26**

Évaluer le degré de sensibilité des renseignements personnels 27

Évaluer la finalité de l'utilisation ou de la communication des renseignements personnels 27

Évaluer la quantité de renseignements personnels 28

Évaluer la répartition des renseignements personnels 28

Évaluer le support de conservation des renseignements personnels 28

3.4 Dresser la liste de vos obligations **29**

Obligations provinciales 29

Obligations fédérales et internationales 30

Pratiques organisationnelles 30

Normes 30

4. Évaluer les facteurs relatifs à la vie privée et adopter les stratégies appropriées **31**

4.1 Respecter vos obligations et les principes de protection des renseignements personnels **32**

4.2 Identifier les risques d'atteinte à la vie privée et évaluer leurs conséquences **32**

Identifier les risques d'atteinte à la vie privée engendrés par votre projet 32

Décrire les causes et les conséquences potentielles de chaque risque 34

Tenir compte de certaines particularités de votre projet 35

Évaluer le niveau initial de chaque risque identifié 36

4.3 Mettre en place des stratégies pour éviter ou réduire les risques **40**

Étudier plusieurs stratégies et sélectionner les meilleures 40

Réévaluer le niveau de chacun des risques 41

Réévaluer la nécessité et la proportionnalité de votre projet 41

4.4 Établir un plan d'action **42**

Préparer votre plan d'action 42

Identifier les responsables de la gestion des risques résiduels 42

Informer les autorités au sein de votre organisation 42

5. Rédiger un rapport **43**

5.1 Pourquoi rédiger un rapport ? **44**

5.2 Que devrait contenir le rapport ? **44**

5.3 Devez-vous diffuser le rapport ? **46**

5.4 Devez-vous transmettre le rapport à la Commission ? **46**

6. Maintenir l'évaluation à jour **47**

7. Particularités pour certaines situations **48**

7.1 Communication à l'extérieur du Québec **49**

7.2 Système d'information ou de prestation électronique de services **51**

7.3 Communication à des fins d'étude, de recherche ou de production de statistiques **52**

7.4 Collecte par un organisme public pour le compte d'un autre **56**

7.5 Autres types de communications sans consentement (secteur public) **57**

3.4 Dresser la liste de vos obligations

Afin d'évaluer le premier facteur relatif à la vie privée, vous gagnez à dresser d'emblée une liste de vos obligations en matière de protection des renseignements personnels. Selon la nature et l'envergure de votre projet, ces obligations peuvent provenir de sources différentes.

Identifier vos obligations et comprendre les enjeux qu'elles impliquent peuvent être des tâches complexes, en particulier si votre projet l'est lui aussi. En cas de doute, **nous vous recommandons de consulter un juriste**.

Obligations provinciales

Au Québec, la protection des renseignements personnels est principalement encadrée par la Loi sur l'accès et la Loi sur le privé. Vous trouverez des informations générales sur les obligations prévues par ces lois sur le site Web de la Commission, dans les sections appropriées :

- Ministères et organismes publics;
- Entreprises et organisations privées.

Ces sections sont organisées autour du cycle de vie des renseignements personnels, de leur collecte à leur destruction, et présentent les obligations transversales relevant de la responsabilité, du consentement et de la sécurité.

Le terme « **cycle de vie** » désigne toutes les phases par lesquelles passe un renseignement personnel au sein d'une organisation[12]. Ces phases sont la collecte, l'utilisation, la communication, la conservation et la destruction. Chacune est associée à des obligations particulières pour l'organisation.

Vous pourriez également devoir appliquer des obligations prévues dans d'autres lois ou règlements. Pour vous aider, n'hésitez pas à consulter ceux qui sont répertoriés sur le site Web de la Commission.

Exemples de particularités et d'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 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*.

12. Pour en savoir plus, consultez les pages Web sur le cycle de vie s'adressant aux entreprises et organisations privées et aux ministères et organismes publics.
13. Pour en savoir plus, consultez la section Biométrie du site Web de la Commission.

Enfin, selon la raison pour laquelle vous réalisez une EFVP (**voir section 1.1**), vous devez possiblement vous assurer que votre évaluation vous permette de satisfaire des critères particuliers ou prévoir la conclusion d'une entente formelle. Assurez-vous d'inclure ces obligations dans votre liste.

Pour en savoir plus sur les particularités associées à chacune des cinq situations obligeant la réalisation d'une EFVP dans la Loi sur l'accès et la Loi sur le privé, consultez **la section 7**.

Obligations fédérales et internationales

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

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

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

Enfin, certaines lois 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.

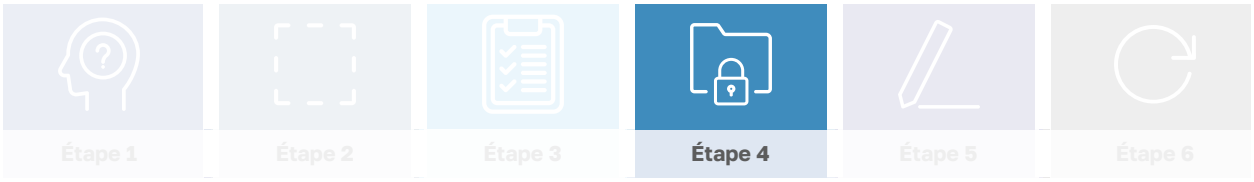
Pratiques organisationnelles

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.



4. Évaluer les facteurs relatifs à la vie privée et adopter les stratégies appropriées

4.1 Respecter vos obligations et les principes de protection des renseignements personnels 32

4.2 Identifier les risques d'atteinte à la vie privée et évaluer leurs conséquences 32

4.3 Mettre en place des stratégies pour éviter ou réduire les risques 40

4.4 Établir un plan d'action 42

Vous avez maintenant décrit votre projet et l'objet de l'évaluation, déterminé les personnes et les organisations que vous devez consulter, dressé l'inventaire des renseignements personnels impliqués, tracé leur parcours, établi l'ampleur que doit prendre votre EFVP et ciblé vos obligations. Vous êtes fin prêts à analyser, en détail, les facteurs relatifs à la vie privée, c'est-à-dire tous ceux qui auront un effet positif ou négatif sur le respect de la vie privée des personnes concernées.

Au cours de cette étape, vous évaluerez si tout est en place dans votre projet pour respecter les lois et les principes applicables en matière de protection des renseignements personnels. Vous réfléchirez aussi aux risques pouvant se poser pour les personnes concernées en raison de votre projet et déterminerez des stratégies (légales, techniques, administratives, etc.) pour atténuer ou éliminer ces risques.

En tenant compte des stratégies déjà en place et de celles qui sont projetées, vous réévaluerez alors les risques résiduels et, conséquemment, le respect des notions de nécessité et de proportionnalité afin de prendre une décision sur la suite du projet. Si vous pouvez en poursuivre la réalisation, vous établirez enfin un plan d'action pour mettre en place les stratégies identifiées dans l'évaluation.

Incluez dans votre rapport :

- **Une description des moyens mis en place pour respecter les lois et les principes de protection des renseignements personnels;**
- **Une démonstration que les critères spécifiques dont l'EFVP doit tenir compte sont respectés, s'il y a lieu;**
- **Une évaluation des risques (événements, causes et conséquences, niveau de risque);**
- **Une description des stratégies nécessaires pour éliminer ou atténuer les risques;**
- **Un plan d'action pour mettre en place ces stratégies.**

4.1 Respecter vos 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 section 3.4**) et évaluez dans quelle mesure vous respectez vos obligations. Cela peut impliquer des analyses juridiques, la documentation de certaines pratiques au sein de l'organisation, 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 ?
- Pouvez-vous démontrer que vous respectez les **critères particuliers** associés à la situation légale qui vous mène à réaliser une EFVP, s'il y a lieu (**voir section 7**) ?
- 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 les différents principes. En cas de doute concernant le respect de vos obligations légales, n'hésitez pas à consulter un juriste.

4.2 Identifier les risques d'atteinte à la vie privée 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.

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

Dès que des renseignements personnels sont impliqués dans un projet, celui-ci présente nécessairement des risques d'atteinte à la vie privée des personnes qu'ils concernent.

14. Pour un aperçu des principes généralement reconnus en matière de protection des renseignements personnels, consultez la **section 7.1**.

Le terme « **risque d'atteinte à la vie privée** » désigne une situation ou un événement qui pourrait causer un préjudice à une personne en matière de vie privée ou par rapport à un autre droit, mais en lien avec sa vie privée. Le risque est une *menace potentielle* au droit à la vie privée, susceptible de se concrétiser dans le futur.

Les risques peuvent entre autres découler d'un non-respect de la loi, mais aussi d'une action extérieure (p. ex. cyberattaque). Ils peuvent aussi faire surface si l'attente raisonnable de vie privée des personnes n'est pas respectée. **Notez que certains aspects légalement conformes d'un projet peuvent quand même être perçus comme une atteinte à la vie privée par les personnes concernées.**

Pour établir des scénarios de risques associés à 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 du 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, **nous vous recommandons de vous en inspirer pour produire votre EFVP**.

Décrire les causes et les conséquences potentielles de chaque risque

Précisez les causes possibles des risques que vous avez identifiés, dans le contexte de votre organisation. Notez qu'un même risque peut être susceptible d'être causé par de multiples facteurs.

Exemples de causes :

- 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.

S'il se réalise, chacun des risques peut engendrer des conséquences pour les personnes concernées. Décrivez et évaluez les préjudices potentiels aux droits des personnes.

Une conséquence n'a pas besoin d'être tangible pour être considérée : elle peut être manifeste et externe (p. ex. en cas d'atteinte à la réputation des personnes concernées), ou être vécue de l'intérieur par les personnes concernées (p. ex. sentiment d'intrusion). De même, elle peut être liée à une atteinte à la vie privée, mais concerner d'autres droits des personnes, comme le droit à l'autonomie ou à la liberté d'expression.

Attention ! Selon l'ampleur de votre EFVP, vous devriez aussi considérer les conséquences qui paraissent relativement minimes, en particulier lorsqu'elles sont susceptibles d'être vécues par une grande quantité de personnes. En effet, un préjudice individuel de faible ampleur peut prendre une grande importance lorsqu'on considère son effet sur un groupe de personnes.

Exemples de conséquences **:**

- Vols d'identité et fraudes;
- Dangers pour la vie et la sécurité des personnes (comme les possibilités de harcèlement);
- Atteinte à l'autonomie (p. ex. manipulation);
- Pertes financières ou d'opportunités;
- Discrimination;
- Dommages à la réputation;
- Détresse psychologique;
- Autocensure en raison d'un effet dissuasif;
- 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 les droits des **personnes concernées**. Bien que ces conséquences soient importantes, ne considérez donc pas dans l'EFVP :

- Les éventuels dommages à la réputation de votre organisation;
- Les litiges qui pourraient survenir;
- Les coûts potentiels que vous pourriez devoir assumer, etc.

Tenir compte de certaines particularités de votre projet

En identifiant les risques, leurs causes et leurs conséquences potentielles, tenez compte du contexte de votre projet, notamment s'il implique de nouvelles technologies, s'il est de grande envergure ou s'il comporte des enjeux éthiques.

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 technologie qui suscite des questions et des enjeux particuliers[15]. On peut aussi penser à l'intelligence artificielle, notamment générative[16].

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

15. Pour en savoir plus concernant l'utilisation de systèmes biométriques, consultez le guide produit par la Commission.
16. Pour en savoir plus concernant le recours à l'intelligence artificielle générative, consultez le document de principes élaboré par la Commission et ses homologues canadiens.

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'elles (**voir section 3.2**). 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 section 7.3**).

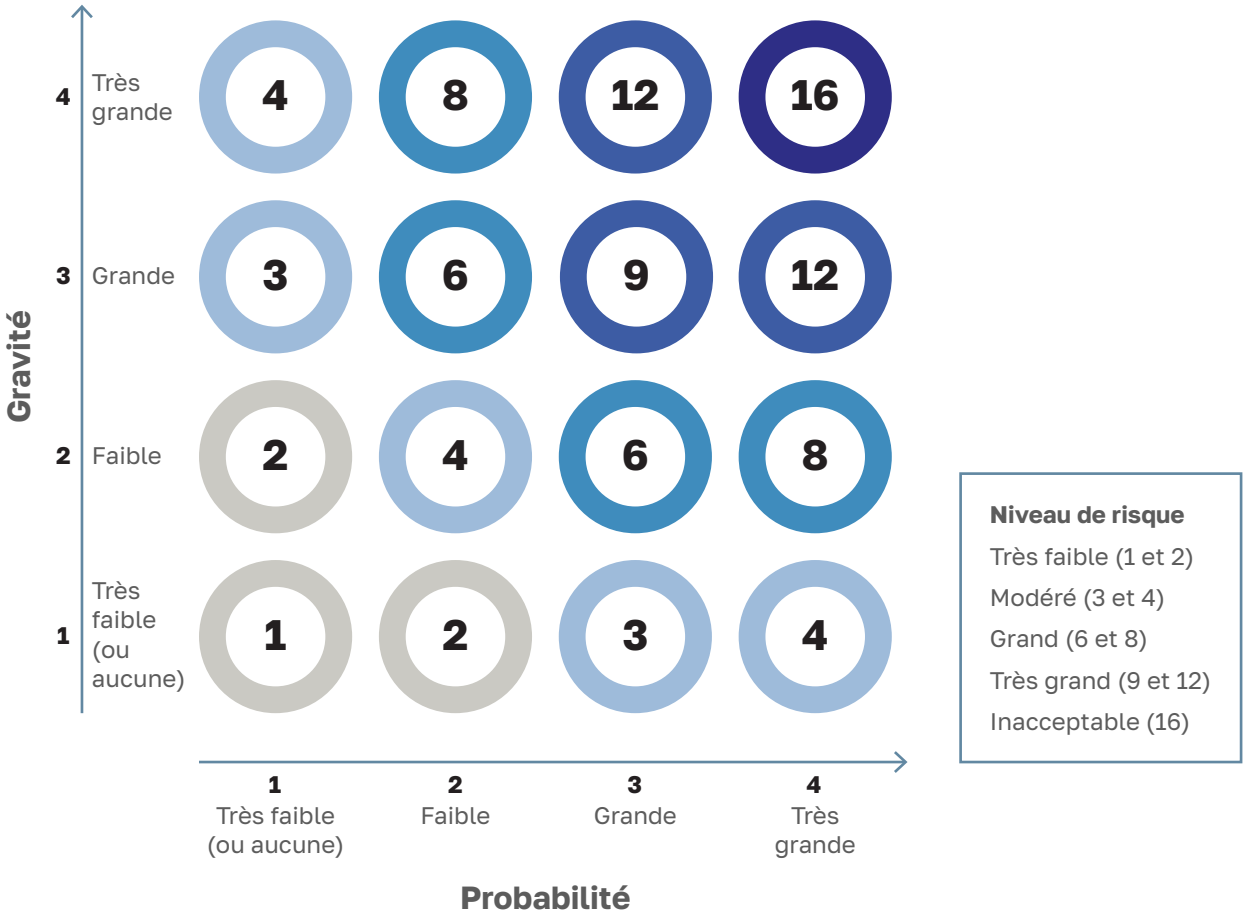
Des rapports d'évaluation éthique des nouvelles technologies sont fréquemment diffusés par des organismes indépendants, comme la Commission de l'éthique en science et en technologie, ou des chercheurs universitaires. Ces documents abordent bien souvent des questions de vie privée. Ce sont des sources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

Évaluer le niveau initial de chaque risque identifié

Afin d'avoir un portrait initial de l'ampleur des risques associés à votre projet, évaluez leur niveau. Cela vous guidera pour choisir des stratégies d'atténuation et vous donnera un point de comparaison utile au moment d'évaluer leur efficacité potentielle.

Se doter d'une méthode pour qualifier les risques

La loi ne prescrit pas de méthode 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, comme le graphique ci-dessous :



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 d'atteinte à la vie privée sont déjà en vigueur dans votre organisation, **nous vous recommandons de les privilégier**. Vous pourrez alors vous appuyer sur une méthodologie éprouvée dans votre contexte.

Évaluer la gravité des conséquences potentielles de chacun des risques identifiés

La première composante du niveau de risque est la gravité des conséquences qui pourraient affecter les personnes concernées s'il se réalisait. Le degré de gravité peut être évalué 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. Si vous repérez un risque présentant un tel degré de gravité, vous devez absolument l'éliminer pour poursuivre votre projet.

Certaines variables, dont celles que vous avez considérées au moment d'établir l'ampleur de l'EFVP (**voir section 3.3**), peuvent influencer la gravité des conséquences potentielles. Tenez notamment compte :

- De la **quantité** de renseignements impliqués;
- De la **nature** et de la **sensibilité** des renseignements impliqués;
- De 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);
- Du **nombre de personnes** potentiellement touchées ou du **profil** de ces personnes (**exemples :** enfants, personnes en situation de handicap, immigrants).

Estimer la probabilité que les risques se réalisent

La deuxième composante du niveau de risque est la probabilité que se concrétise la situation ou l'événement qui constitue le risque. La probabilité peut aussi être évaluée 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, l'estimation de la probabilité des risques peut être difficile à produire. **Nous vous recommandons d'être réaliste : évitez d'être trop confiant ou trop conservateur.**

Établir le niveau de risque

Une fois que vous avez estimé la gravité et la probabilité des risques, attribuez-leur 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 37**.

Considérer les stratégies et les moyens de contrôle existants

Votre organisation peut déjà avoir mis en place des mesures (outils, politiques, directives, procédures, moyens techniques, etc.) 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 protégés lorsqu'ils sont :

- Recueillis;
- Utilisés;
- Communiqués;
- Conservés;
- Détruits.

Fixez 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.

4.3 Mettre en place des stratégies pour éviter ou réduire les risques

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

Étudier plusieurs stratégies et sélectionner les meilleures

Les stratégies peuvent avoir pour objectif de 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.

Vos stratégies peuvent être de nature légale ou administrative, physique ou technique.

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;
- Restreindre l'accès aux locaux où seront conservés des documents contenant des renseignements personnels;
- 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 agréger les renseignements si leur utilisation sous une forme directement identificatoire n'est pas requise pour tous.

À partir de l'éventail de stratégies que vous aurez considérées, déterminez lesquelles 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 du risque en réfléchissant à nouveau à la gravité des conséquences qu'il pourrait engendrer et à la probabilité qu'il se concrétise. Vous pouvez de nouveau suivre la démarche présentée dans la **section 4.2**.

Vérifiez si vous avez atteint le seuil de tolérance que vous aviez fixé. Si le seuil est encore dépassé, 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 aviez fixé n'est pas atteint, **pensez à revoir en profondeur cet aspect de votre projet ou à le retirer.**

Tout risque qui subsiste à la fin de votre démarche, une fois que vous avez ciblé les mesures visant à diminuer ou à éliminer les risques identifiés au départ, devient un **risque résiduel**. Il est ainsi possible, et même probable, 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, **nous vous recommandons de 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 et pourra éviter de refaire la démarche complète inutilement.

Réévaluer la nécessité et la proportionnalité de votre projet

Après avoir terminé l'exercice de gestion des risques, refaites l'exercice d'évaluer la nécessité et 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 ? Est-ce que tous les renseignements personnels impliqués sont nécessaires ?**

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

Si les risques résiduels sont trop importants, vous devriez envisager des modifications substantielles à votre projet. Cela peut impliquer de recommencer l'EFVP en tout ou en partie, ou même de remettre le projet en question.

4.4 Établir un plan d'action

Une fois que les facteurs relatifs à la vie privée sont évalués, vous devriez préparer la suite concrète de l'EFVP et du projet en planifiant la mise en place des stratégies que vous avez retenues.

Préparer 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.

Votre plan d'action devrait inclure des moyens pour réévaluer périodiquement l'efficacité des stratégies que vous mettrez en place.

Identifier les responsables de la gestion des risques résiduels

Vous devriez désigner des personnes responsables de surveiller l'évolution des risques résiduels, sans quoi ils risquent d'être oubliés. Ces personnes pourraient également être responsables de gérer la situation si elle se concrétise.

Informer les autorités au sein de votre organisation

Les hautes autorités de votre organisation ont une responsabilité particulière en matière de respect des lois sur la protection des renseignements personnels. Vous devriez donc les tenir 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.

5. Rédiger un rapport

5.1 Pourquoi rédiger un rapport ? 44

5.2 Que devrait contenir le rapport ? 44

5.3 Devez-vous diffuser le rapport ? 46

5.4 Devez-vous transmettre le rapport à la Commission ? 46

Vous devriez être en mesure d'expliquer et de justifier votre démarche d'EFVP en cas de besoin. La rédaction d'un rapport, même si elle n'est pas obligatoire, est un excellent 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.

La Commission propose un modèle 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.

Rédigez votre rapport pour documenter votre démarche.

5.1 Pourquoi rédiger un 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, dont la Commission. Il constitue également une trace utile pour la mémoire organisationnelle. Si vous devez mettre à jour l'EFVP ou en réaliser une autre semblable, le rapport sera alors une source d'information précieuse.

Le rapport est l'option la plus commune et complète pour documenter votre démarche. Il peut être plus ou moins long et étoffé selon l'ampleur de votre EFVP (**voir section 3.3**). Il n'est toutefois pas obligatoire, et n'est pas non plus l'unique méthode à votre disposition. Pour des projets d'ampleur plus limitée, vous pourriez rendre compte de l'EFVP de différentes manières, par exemple à l'aide de comptes rendus ou de courriels faisant état de votre réflexion.

Notez toutefois que la multiplication des pièces justificatives peut être nuisible. Le suivi de votre évaluation, de l'évolution des risques et de la mise en place des stratégies que vous avez ciblées peut être plus difficile à faire en l'absence d'un document qui réunit toutes les informations pertinentes. De même, si la Commission doit faire des vérifications quant à votre EFVP, les pièces multiples peuvent compliquer l'exercice, à votre désavantage.

Vous gagnez donc, dans la majorité des cas, à opter pour un rapport, et en particulier si vous devez attester de votre EFVP auprès de la Commission, par exemple pour appuyer une entente de communication de renseignements personnels.

5.2 Que devrait contenir le rapport ?

Votre rapport devrait d'abord présenter l'essentiel de votre projet, du cadre dans lequel il s'inscrit et de votre analyse. Il devrait également contenir une mention de l'approbation de votre rapport par les hautes instances de votre organisation.

Enfin, votre rapport devrait inclure des informations complémentaires sous forme d'annexes, s'il y a lieu :

- 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 (p. ex. test d'intrusion);
- Une entente de communication conclue après l'EFVP;
- 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), etc.

Le tableau suivant présente un aperçu des éléments qui pourraient figurer dans votre rapport, avec les références appropriées aux sections de ce guide et au modèle générique de rapport proposé par la Commission.

Élément	Section du guide	Section du modèle générique de rapport
Situation légale qui motive l'EFVP, s'il y a lieu	Section 1.1	Résumé de l'évaluation
Description du projet, de ce qui l'a motivé (contexte) et de ses objectifs	Section 2.1 Section 2.2	Section 1. Description du projet et de l'objet de l'EFVP
Parties prenantes à l'EFVP, y compris la description de leur rôle et de leurs responsabilités	Section 2.3	Résumé de l'évaluation Section 2. Rôles et responsabilités
Résumé des consultations réalisées dans le cadre de l'EFVP, s'il y a lieu	Section 2.3	Section 2. Rôles et responsabilités
Aperçu de l'inventaire des renseignements personnels impliqués (catégories, finalités, quantité, etc.)	Section 3.1	Section 3. Renseignements personnels impliqués et ampleur de l'évaluation
Aperçu du parcours des renseignements personnels impliqués (sources, supports, destinataires, systèmes utilisés, personnes y ayant accès, etc.)	Section 3.2	
Évaluation des critères de sensibilité, de finalité, de quantité, de répartition et de support des renseignements personnels et justification de l'ampleur de l'EFVP	Section 3.3	
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)	Section 3.4 Section 4.1	Section 4. Conformité aux obligations et aux principes de protection des renseignements personnels
Justification du respect des critères particuliers associés à la situation légale qui motive la réalisation de l'EFVP, s'il y a lieu	Section 7	
Liste et catégorisation des risques identifiés pour les personnes concernées	Section 4.2	Section 5. Identification des risques et des stratégies pour les atténuer
Stratégies, mécanismes et mesures déployés pour éliminer ou réduire ces risques	Section 4.3	
Personnes responsables de mettre en œuvre ces stratégies et personnes ou secteurs responsables de gérer les risques résiduels	Section 4.4	Section 6. Plan d'action
Plan d'action avec un échéancier comprenant une réévaluation périodique des mesures mises en place	Section 4.4	
Approbation du rapport par les hautes autorités de l'organisation (y compris noms, titres, signatures, date, etc.)	Section 4.4	Section 7. Approbation du rapport et versions
Toute pièce jointe pertinente	s.o.	Documents joints

5.3 Devez-vous diffuser le rapport ?

À titre de bonne pratique en matière 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.

5.4 Devez-vous transmettre le rapport à la Commission ?

Il est attendu que vous transmettiez un rapport d'EFVP à la Commission lorsque celle-ci précède la signature d'une entente (voir section 7.3, section 7.4, section 7.5). 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 de connaître les éléments qui ont été considérés.

Dans les autres cas, il n'est pas nécessaire de transmettre proactivement un rapport d'EFVP à la Commission. Celle-ci pourrait toutefois demander à en prendre connaissance dans le cadre de ses activités de surveillance.

6. Maintenir l’évaluation à jour

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 stratégies, 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, 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.

Étape 7

7. Particularités pour certaines situations

7.1 Communication à l'extérieur du Québec 49

7.2 Système d'information ou de prestation électronique de services 51

7.3 Communication à des fins d'étude, de recherche ou de production de statistiques 52

7.4 Collecte par un organisme public pour le compte d'un autre 56

7.5 Autres types de communications sans consentement (secteur public) 57

La démarche générale d'EFVP est toujours la même. Cependant, vous devrez tenir compte de certaines particularités selon la situation légale qui justifie votre évaluation.

Dans cette section, vous trouverez des précisions sur certains concepts inclus dans la loi, sur la conclusion d'ententes et sur l'évaluation de critères spécifiques dans certaines situations.

Incluez dans votre rapport :

- **Une démonstration que les critères spécifiques dont l'EFVP doit tenir compte sont respectés, s'il y a lieu.**

7.1 Communication à l'extérieur du Québec

Ces précisions concernent la situation prévue aux 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, dans cette situation, vous devez notamment tenir compte des éléments suivants :

- La sensibilité du renseignement communiqué;
- 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[17] :

- **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.

17. 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.

- **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 comprennent 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 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.
- **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.

- 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 ?

⚠ **Attention !** 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 ». **Vous devez 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 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 de connaître les éléments qui ont été considérés.

Cet outil d'information vous a-t-il été utile ?
Complétez notre court sondage de satisfaction !

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

Avril 2024