



Réaliser une évaluation des facteurs relatifs à la vie privée

Guide d'accompagnement à la
démarche et à sa documentation

Avril 2024

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.

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.

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'EFVP¹ 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'impact². 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 destruction³. 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	Étape 2	Étape 3	Étape 4	Étape 5	Étape 6
Déterminer si une évaluation est requise	Définir votre projet et l'objet de l'évaluation	Préparer l'évaluation	Évaluer les facteurs relatifs à la vie privée et adopter les stratégies appropriées	Rédiger un rapport	Maintenir l'évaluation à jour
<u>Pages 10-13</u>	<u>Pages 14-18</u>	<u>Pages 19-30</u>	<u>Pages 31-42</u>	<u>Pages 43-46</u>	<u>Page 47</u>

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

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

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.

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.

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

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
Informers 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



1. Déterminer si une évaluation est requise

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

Avant de vous lancer dans une démarche d'EFVP, vous devez évaluer si celle-ci est requise. Au cours de cette étape, vous vérifierez si votre projet est concerné par une obligation légale de réaliser une EFVP. Dans le cas contraire, vous pourrez tout de même choisir de mener une EFVP à titre de bonne pratique.

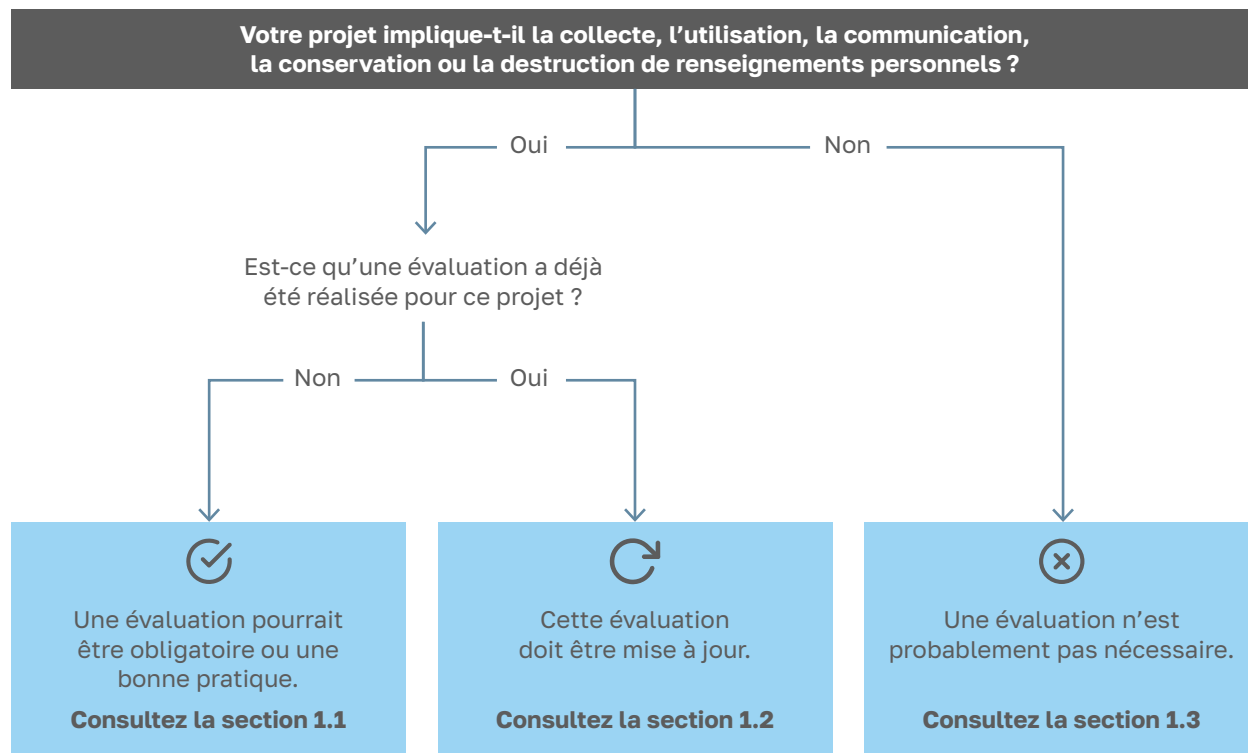


Incluez dans la section récapitulative de votre rapport :

- **La raison pour laquelle vous réalisez une EFVP, avec la référence légale, au besoin.**



La première étape d'une démarche d'EFVP est de vérifier si elle est requise.



1.1 Une évaluation est obligatoire dans cinq situations principales

Cette section présente toutes les situations dans lesquelles l'EFVP est obligatoire selon la loi, à la date de publication de ce guide (avril 2024).

Les étapes de la démarche proposée dans ce guide s'appliquent à toutes ces situations. Votre analyse doit cependant tenir compte du cadre légal particulier à votre situation. Les détails et les particularités de chaque situation se retrouvent à la [section 7](#) du guide.



La Loi sur l'accès et la Loi sur le privé **vous obligent** à réaliser une EFVP dans cinq situations⁴.

Situation	Secteurs	
	Privé	Public
<p>1. Vous projetez de communiquer des renseignements personnels à l'extérieur du Québec. ➤ Voir section 7.1</p> <p>Entrée en vigueur : 22 septembre 2023</p>	Article 17 Loi sur le privé	Article 70.1 Loi sur l'accès
<p>2. Vous projetez d'acquérir, de développer ou de refondre un système d'information ou de prestation électronique de services impliquant des renseignements personnels. ➤ Voir section 7.2</p> <p>Entrée en vigueur : 22 septembre 2023</p>	Article 3.3 Loi sur le privé	Article 63.5 Loi sur l'accès
<p>3. Vous projetez de communiquer des renseignements personnels dans le cadre d'une entente, sans le consentement des personnes concernées, pour une utilisation à des fins d'étude, de recherche ou de production statistiques. ➤ Voir section 7.3</p> <p>Entrée en vigueur : 22 septembre 2022</p>	Article 21 Loi sur le privé	Article 67.2.1 Loi sur l'accès
<p>4. Vous projetez de recueillir des renseignements personnels pour le compte d'un autre organisme public dans le cadre d'une entente. ➤ Voir section 7.4</p> <p>Des dispositions transitoires s'appliquent pour les ententes déjà en vigueur.</p> <p>Entrée en vigueur : 22 septembre 2023</p>		Article 64 Loi sur l'accès
<p>5. Vous projetez de communiquer des renseignements personnels à une personne ou à un organisme sans le consentement des personnes concernées dans le cadre d'une entente. ➤ Voir section 7.5</p> <p>Des dispositions transitoires s'appliquent pour les ententes déjà en vigueur.</p> <p>Entrée en vigueur : 22 septembre 2023</p>		Article 68 Loi sur l'accès

Vous devez donc réaliser une EFVP si :

- Vous commencez un nouveau projet;
- Votre projet n'était pas finalisé quand l'obligation de réaliser une EFVP est entrée en vigueur;
- Vous modifiez un projet (p. ex. modification de l'entente, refonte du système, etc.);
- Votre projet implique la communication de renseignements personnels à l'extérieur du Québec après le 22 septembre 2023.

4. 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 :

- Projet en ressources informationnelles d'intérêt gouvernemental ([article 9 de la Loi favorisant la transformation numérique de l'administration publique](#));
- Collecte, utilisation ou communication pour les fonctions d'un organisme public désigné comme source officielle de données numériques gouvernementales ([article 12.16 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement](#));
- Communication par Revenu Québec à un organisme public désigné comme source officielle de données numériques gouvernementales ([article 69.1.1 de la Loi sur l'administration fiscale](#)).



Cependant, vous n'avez pas l'obligation de réaliser une EFVP si votre projet était déjà finalisé à la date d'entrée en vigueur de l'obligation⁵. Par exemple :

- La communication à l'extérieur du Québec était terminée (situation 1);
- Le système d'information était déjà implanté (situation 2);
- L'entente de communication était déjà conclue (situations 3, 4 et 5).



Nous vous recommandons tout de même de réaliser une EFVP :

- Si vous n'êtes pas dans l'une des cinq situations où une EFVP est obligatoire;
- Si votre projet était déjà finalisé à la date d'entrée en vigueur de l'obligation.

En effet, dès qu'un projet implique des renseignements personnels, réaliser une EFVP est une bonne pratique pour protéger ces renseignements et la vie privée des personnes. Il peut donc être bénéfique d'analyser la situation à la lumière de vos obligations légales.

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

Si vous avez déjà réalisé une EFVP pour une version antérieure de votre projet et que des changements sont survenus, **vous devez la mettre à jour ou la recommencer pour tenir compte de ces changements**. Tenez compte des particularités de votre situation suivant les détails donnés à la [section 7](#) du guide.

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

Si votre projet n'implique pas de renseignements personnels et ne présente manifestement aucun risque en matière de respect de la vie privée, **vous n'avez pas à réaliser d'EFVP**. Attention! Des renseignements peuvent, une fois croisés avec d'autres, révéler de l'information sur les personnes concernées. N'écartez pas l'EFVP trop rapidement.



Si vous ne réalisez pas d'EFVP, nous vous recommandons néanmoins de préparer un rapport très simple, témoignant de votre réflexion, dans lequel vous décrierez :

- Les grandes lignes de votre projet;
- La raison pour laquelle vous ne menez pas d'EFVP.

5. Ces dates sont inscrites sous chaque situation à la page précédente.



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

2.1 Définir votre projet et ses objectifs	15
2.2 Déterminer l'objet de l'évaluation	17
2.3 Définir les rôles et les responsabilités	17

Une fois que vous avez déterminé qu'une EFVP est requise, vous devez la préparer. À cette étape, vous devrez bien documenter le projet dans son ensemble et vous poser les bonnes questions pour bien cibler les aspects de votre projet qui doivent être considérés. Vous devrez aussi faire l'évaluation initiale de la nécessité et de la proportionnalité de votre projet.

En tenant compte de ces éléments, vous devrez prévoir l'implication des bonnes personnes dans l'évaluation et clarifier leurs responsabilités.



Incluez dans votre rapport :

- **La description du projet;**
- **L'objet de votre évaluation;**
- **La description des rôles et responsabilités.**



2.1 Définir votre projet et ses objectifs

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

Présenter le projet et son contexte

Cette étape est surtout descriptive. L'objectif est de réunir les informations importantes pour vous permettre d'évaluer les risques et les moyens d'éliminer ou de réduire ces risques (voir la [section 4.2](#) et la [section 4.3](#)).

Par exemple :

- En quoi consiste votre projet ?
- Quel était le contexte quand l'idée de ce projet est apparue ?
- Quelle est/était la situation au moment où il débute/a débuté ?
- Quel est l'échéancier de sa mise en œuvre ?
- Quelle est l'utilité du projet pour votre organisation ?

Expliquer les objectifs du projet

Ces objectifs servent à expliquer pourquoi vous lancez le projet et pourquoi ce projet implique des renseignements personnels.

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.



Évaluer d'emblée la nécessité et la proportionnalité du projet

Vous devez évaluer la **nécessité** et la **proportionnalité**⁶ tout au long du processus d'EFVP et de la mise en œuvre de votre projet. Dès cette étape, vous pouvez y réfléchir de façon préliminaire en envisageant à haut niveau et de façon intuitive les risques probables liés à votre projet.



Les termes « **nécessité** » et « **proportionnalité** » font référence à des notions légales de grande importance lorsqu'un projet touche un droit fondamental, comme celui à la vie privée.

Un projet est considéré nécessaire et proportionnel si :

- Les objectifs poursuivis sont légitimes et répondent à des préoccupations importantes et réelles;
- Il existe un lien rationnel entre le projet et ces objectifs, c'est-à-dire qu'il s'agit d'un moyen efficace de les atteindre – cette efficacité doit être basée sur des données concrètes et probantes;
- L'atteinte à la vie privée est minimisée ou s'il n'y a pas d'autres solutions efficaces moins intrusives;
- Les avantages concrets pour l'organisation surpassent les préjudices pour les personnes concernées.

Si la nécessité et la proportionnalité de votre projet sont incertaines à cette étape, la suite de l'EFVP vous aidera à y voir plus clair. Vous les réévaluerez à la fin du processus, en tenant compte des stratégies envisagées pour atténuer ou éliminer les risques pour la vie privée.

Notez qu'un projet qui n'est pas nécessaire et proportionnel n'est pas légal.

6. Pour en savoir plus, consultez les pages Web sur la nécessité s'adressant [aux entreprises et organisations privées](#) et [aux ministères et organismes publics](#).



2.2 Déterminer l'objet de l'évaluation

Vous avez intérêt à délimiter clairement ce sur quoi portera votre EFVP et à tenir votre analyse à un niveau adapté à votre projet. Vous devriez être en mesure de justifier les éléments que vous choisissez d'inclure dans votre évaluation.

Exemple 1 – Objet trop étroit

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. **L'objet de votre évaluation est peut-être trop étroit.** 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 – Objet trop large

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. **L'objet de votre évaluation est sans doute trop large.** Des évaluations distinctes pourraient sans doute être produites pour certains sous-processus.

Exemple 3 – Niveau d'analyse trop haut

Pour le même projet, vous ne faites que la révision des politiques et des directives de votre 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 – Arrimage avec des EFVP préexistantes

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.

2.3 Définir les rôles et les responsabilités

Pour favoriser le succès de votre démarche, vous devrez généralement impliquer d'autres personnes dans l'évaluation. Précisez les rôles et les responsabilités de chacune d'entre elles et assurez-vous aussi de déterminer le moment où elles devront intervenir.



À qui revient la responsabilité de réaliser l'évaluation ?

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 (p. ex. des chercheurs qui demandent accès aux renseignements), même si ceux-ci peuvent vous aider dans la réflexion et l'analyse de certains aspects.

Au sein de cette organisation, la coordination de l'EFVP peut revenir à la personne responsable de la protection des renseignements personnels, mais elle peut être confiée, selon le projet, à d'autres membres du personnel ou être partagée avec eux.

Qui doit être impliqué dans l'évaluation ?

Certaines personnes doivent nécessairement être consultées dans le cadre d'une EFVP :

- L'organisme public doit consulter, dès le début du projet, les membres de 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**.

Vous pourrez impliquer certaines autres personnes, en raison de leur expertise particulière, en fonction de la portée du projet (voir section 2.2) et de l'évaluation de l'ampleur de l'EFVP à réaliser (voir section 3.3). Par exemple, vous pourriez consulter, à l'intérieur de votre organisation :

- Les responsables du projet;
- Les responsables des affaires juridiques;
- Les responsables de la gestion documentaire;
- Les responsables des ressources humaines;
- Les responsables des relations avec la clientèle;
- Les autorités de votre organisation devant prendre position sur la gestion des risques à la fin de la démarche (voir section 4.4).

Vous pourriez aussi consulter des parties prenantes externes, selon le contexte de votre projet, comme :

- Des représentants des personnes concernées;
- Des clients ou des partenaires corporatifs;
- Des sous-traitants;
- Le chercheur demandant accès aux renseignements.



3. Préparer l'évaluation

3.1 Faire l'inventaire des renseignements personnels impliqués	20
3.2 Tracer le parcours des renseignements personnels	23
3.3 Déterminer l'ampleur de l'EFVP à réaliser	26
3.4 Dresser la liste de vos obligations	29

Préparer l'EFVP vous garantit d'investir vos efforts au bon endroit et de couvrir les bons aspects. Puisque l'évaluation porte sur les renseignements personnels, vous devrez d'abord savoir quels renseignements votre projet impliquera. Vous devrez aussi en tracer le parcours pour comprendre comment ils seront échangés d'un système ou d'un acteur à l'autre.

Cet inventaire et ce parcours vous permettront de déterminer l'ampleur de l'EFVP à réaliser, car celle-ci doit être proportionnée au contexte : elle doit être adaptée à la sensibilité, à la quantité, à la finalité d'utilisation, à la répartition et au support des renseignements personnels.

Enfin, vous dresserez la liste des obligations légales qui vous incombent afin de vous guider dans l'évaluation elle-même.



Incluez dans votre rapport :

- **Un aperçu de l'inventaire des renseignements personnels;**
- **Un parcours schématisé des renseignements personnels;**
- **La justification de l'ampleur de l'EFVP réalisée;**
- **Des tableaux, des titres ou des outils d'analyse appropriés selon les obligations applicables.**



3.1 Faire l'inventaire des renseignements personnels impliqués

D'abord, identifiez tous les renseignements personnels impliqués dans votre projet en tenant compte de la portée de votre évaluation ([voir section 2.2](#)).

Pourquoi faire l'inventaire des renseignements personnels ?

Votre inventaire vous permet de recueillir, d'utiliser et de communiquer seulement les renseignements personnels **nécessaires** pour réaliser le projet.

En effet, même avec le consentement des personnes concernées, vous ne pouvez pas recueillir des renseignements personnels qui ne sont pas nécessaires à votre projet. Vous devez être en mesure de démontrer que les renseignements recueillis, utilisés ou communiqués sont nécessaires pour réaliser votre projet⁷.

L'inventaire des renseignements personnels vous permet également d'en connaître :

- La **sensibilité**;
- La **quantité**;
- La **finalité**.

Ces informations vous aideront à évaluer l'ampleur de l'EFVP à réaliser ([voir section 3.3](#)).

7. Pour en savoir plus sur le critère de nécessité, consultez nos pages dédiées [aux entreprises](#) ou [aux organismes publics](#) et [la section 2.1](#).



Comment structurer l'inventaire ?

Pour structurer votre inventaire, vous pouvez répondre aux questions suivantes :

Questions	Sous-questions
Quoi ?	<ul style="list-style-type: none"> Quels types de renseignements personnels seront collectés, communiqués, utilisés ou conservés dans le cadre de ce projet ? Quelle est la nature de ces renseignements ? Sont-ils sensibles en raison de cette nature ou du contexte de leur utilisation ?
Pourquoi ?	<ul style="list-style-type: none"> Pourquoi souhaitez-vous recueillir, utiliser, communiquer ou conserver des renseignements personnels ? Quelle est la finalité (le but) de l'utilisation de ces renseignements dans le cadre de votre projet ? En quoi les personnes qui auront accès aux renseignements personnels en ont-elles besoin dans l'exercice de leurs fonctions ?
Combien ?	<ul style="list-style-type: none"> Quelle quantité de renseignements personnels sera impliquée dans votre projet ? Combien de personnes seront concernées par votre projet (nombre absolu ou proportion de la population concernée) ? Quel est le volume ou l'étendue des renseignements personnels concernés ? Quelle est la durée envisagée du projet ? Quelle est la portée géographique envisagée pour le projet ?

N'oubliez pas d'inclure dans votre inventaire **tous les renseignements impliqués**, y compris :

- Les renseignements que vous **créerez** ou que vous **déduirez** à partir d'autres renseignements, par exemple une cote de crédit ou un profil d'intérêts;
- Les renseignements **recueillis automatiquement** par les appareils et les systèmes informatiques, par exemple l'identifiant d'un appareil ou son historique de connexion;
- Les renseignements qui sont **regroupés** (aussi appelés renseignements agrégés), même s'ils ne permettent plus d'identifier un individu donné, par exemple des statistiques⁸;
- Les renseignements qui ne permettent plus d'identifier directement ou indirectement une personne (c'est-à-dire les renseignements **dépersonnalisés** et les renseignements **anonymisés**)¹⁰.

8. Vous devrez évaluer le risque de réidentification des renseignements agrégés, dépersonnalisés ou anonymisés, c'est-à-dire le risque que le lien entre un renseignement et la personne concernée soit rétabli. Les nouvelles technologies permettent souvent de le faire. Pour en savoir plus, consultez les pages Web sur la dépersonnalisation et l'anonymisation s'adressant [aux entreprises et organisations privées](#) et [aux ministères et organismes publics](#).



Comment regrouper les renseignements personnels ?

Vous n'aurez pas toujours à préparer une liste complète de tous les renseignements personnels à toutes les étapes de l'EFVP. Par exemple, une liste de regroupements de renseignements personnels pourrait suffire dans votre rapport d'EFVP. Cependant, même si vous présentez des regroupements, vous devez être en mesure de connaître l'étendue des renseignements personnels qui sont impliqués dans le projet.

Vous pouvez regrouper les renseignements personnels de différentes façons. Par exemple, vous pourriez regrouper les renseignements :

- Qui ont des caractéristiques communes;
- Qui permettent d'accomplir une même fonction ou d'atteindre un même objectif.

Si vous n'êtes pas certain qu'un regroupement contient des renseignements personnels, vous devriez le conserver et le considérer pour votre EFVP.

Notez qu'une liste de regroupements doit quand même prévoir une courte énumération du contenu de ces regroupements. Dans les exemples ci-dessous, cette énumération se trouve entre parenthèses.

Exemples de regroupements :

- Renseignement d'identité et coordonnées (nom, prénom, adresse, nom d'utilisateur, mot de passe, etc.);
- Renseignements de santé, en version électronique ou 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 d'utilisation du site Internet et outils d'analyse Web (historique des pages consultées, adresse IP, navigateur et appareil utilisé, configuration de l'affichage, etc.).

Quand mettre à jour l'inventaire des renseignements personnels ?

L'inventaire des renseignements personnels est évolutif. Tenez-le à jour pour rendre compte des changements susceptibles de survenir au sein de votre organisation (par exemple, une nouvelle collecte de renseignements personnels pour un projet). Vous pourrez ainsi planifier adéquatement vos actions et respecter toutes vos obligations.



3.2 Tracer le parcours des renseignements personnels

Une fois que vous connaissez les renseignements impliqués dans votre projet, vous devez en préciser le parcours.



Le terme « **parcours** » désigne une représentation ou une description structurée des étapes de traitement des renseignements de leur collecte à leur destruction, qui précise les organisations, les personnes, les systèmes et les supports concernés. On parle parfois de « cartographie des données » ou de « diagramme de flux de données ».

Le parcours des renseignements personnels vous permet entre autres d'en préciser :

- La **répartition**;
- Le **support**.

Ces informations vous aideront à évaluer l'ampleur de l'EFVP à réaliser ([voir section 3.3](#)).

Identifier les points d'interaction avec les renseignements personnels

Dans un premier temps, à la lumière de votre inventaire ([voir section 3.1](#)), identifiez les **points où votre organisation (ou une autre organisation/personne) 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, qui se chargent de les recueillir, qui approuvent leur destruction, etc. (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 **recueillir** des renseignements personnels (formulaires d'abonnement, boîtes de courriels, messagerie téléphonique, 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, bases de données, 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.



Pour vous aider, vous pouvez répondre aux questions suivantes :

Questions	Sous-questions
Qui ?	<ul style="list-style-type: none"> Quelles catégories de personnes auront accès aux renseignements personnels dans l'organisation ou à l'extérieur (tiers) ?
Comment ?	<ul style="list-style-type: none"> 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 ?	<ul style="list-style-type: none"> 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 ?	<ul style="list-style-type: none"> Quand les renseignements seront-ils détruits ou anonymisés ?

Tracer le parcours des renseignements personnels tout au long du 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.

Ce parcours peut prendre diverses formes, comme un tableau, un processus schématisé ou un texte descriptif. Voici un exemple de tableau pour rendre compte d'un parcours dans un projet simple :

Renseignement ou regroupement de renseignements	Collecte (responsables, source, moment, lieu, moyen...)	Utilisation (responsables, moment, lieu, moyen, finalités...)	Communication (responsables, destinataires, situations, moyen, raisons...)	Conservation (responsables, moyen, durée, lieu)	Destruction (responsables, moment, lieu, moyen, déclencheur)
Regroupement 1					
Regroupement 2					
...					

Vous pourriez également préparer un tableau pour préciser les personnes et les organisations qui auront accès au renseignement pendant son cycle de vie, en y indiquant le type d'accès et les raisons justifiant cet accès⁹.

9. Le [modèle générique de rapport proposé par la Commission](#) contient un exemple d'un tel tableau à la section 3.



Le parcours sera plus complexe pour les projets de plus grande envergure, de sorte qu'un découpage par processus pourrait s'avérer préférable, dans ces cas.

Par exemple, 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.

Si votre projet comporte de telles phases et qu'elles se distinguent nettement en matière de gestion des renseignements personnels, vous devriez représenter le parcours des renseignements séparément pour chacune de ces phases.

Exemple 1 : Vous assurez la direction commerciale d'une entreprise qui fabrique des vêtements sur mesure. Vous aimeriez proposer un outil de commande en ligne disponible pour vos clients. Vous embaucherez une firme spécialisée durant la **phase de développement**. Vous devez prévoir que les consultants entreront en contact avec certains renseignements concernant vos vendeurs et vos 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, vous devez considérer que les risques de bogues informatiques seront plus élevés durant cette période.

Exemple 2 : Vous dirigez le département de ressources humaines d'une grande organisation gouvernementale. Vous allez faire changer le logiciel de gestion des ressources humaines. Le fournisseur du logiciel vous avise que le système est mis à jour fréquemment et vous informe que des refontes plus importantes sont à prévoir dans la prochaine année. Vous devez anticiper ces éventuelles refontes qui arriveront en **phase d'exploitation**. Vous devez mettre des moyens en place afin que ces opérations de maintenance n'aient pas d'incidence sur les renseignements personnels des employés.



3.3 Déterminer 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 cette EFVP doit être adaptée à 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 ainsi y avoir des variations dans :

- Le nombre d'acteurs à impliquer ([voir section 2.3](#));
- Le temps à investir;
- Le niveau de détail d'un éventuel rapport ([voir section 5](#));
- La documentation annexe à élaborer;
- La quantité de stratégies prévues pour atténuer ou éliminer les risques ([voir section 4.3](#));
- Le niveau de détail de ces stratégies.

Ainsi, la Loi sur l'accès et la Loi sur le privé prévoient que l'EFVP doit être proportionnée¹⁰ 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. L'inventaire ([voir section 3.1](#)) et le parcours des renseignements personnels ([voir section 3.2](#)) que vous avez préparés devraient vous aider grandement dans cette réflexion.

10. Loi sur l'accès, [article 63.5](#); Loi sur le privé, [article 3.3](#).



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 communication¹¹.

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).

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 :

- Vérifier l'identité des clients lorsqu'ils souhaitent accéder à leur dossier et effectuer des transactions;
- Calculer et verser la paie des employés;
- Établir le profil d'une personne (profil de consommateur, de conducteur, etc.) en combinaison avec d'autres renseignements;
- Rendre une décision automatisée à l'endroit d'une personne;
- Mener une étude ou une recherche ou produire des statistiques;
- Améliorer un modèle d'intelligence artificielle.

11. Loi sur l'accès, [article 65.1](#); Loi sur le privé, [article 12](#).



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 de la population concernée) ?
- 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 la portée géographique projetée ?

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 ?

Évaluer le support de conservation des renseignements personnels

Quel(s) type(s) de **support(s)** permettront-ils de consulter, de consigner ou de consulter, momentanément ou à long terme, les renseignements personnels impliqués dans votre projet ?

Exemples de caractéristiques de supports :

- Matériel (tangibles) ou numérique (p. ex. hébergement en infonuagique);
- Sécurisé ou non sécurisé;
- Connecté avec d'autres systèmes ou non.



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 organisation¹². 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 biométriques¹³ 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;
- Divulcation 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 défectueuses 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 minimales, 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 particuliers¹⁵. On peut aussi penser à l'intelligence artificielle, notamment générative¹⁶.

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.

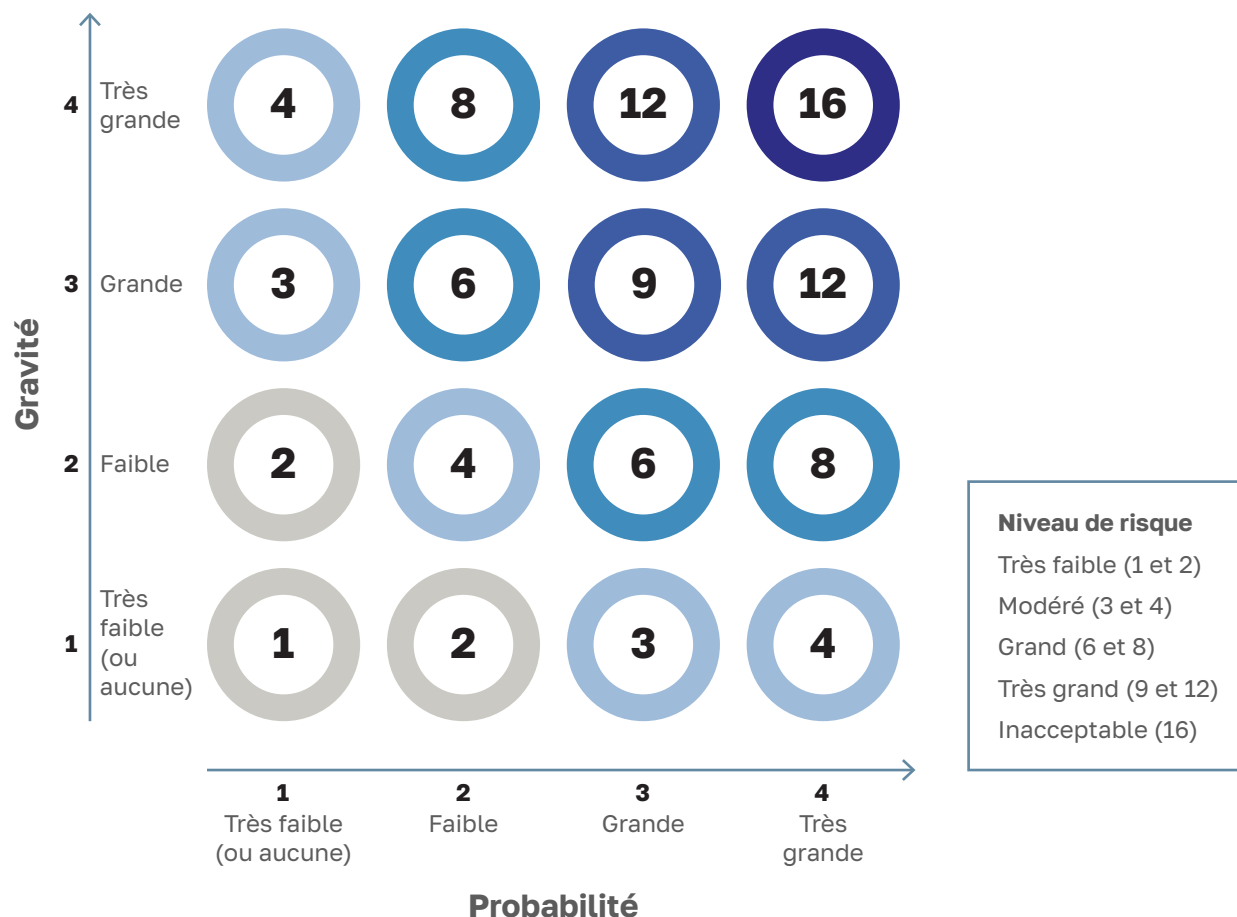
Évaluer le niveau initial de chaque risque identifié

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 mettez 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.

Informez 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	<u>Section 1.1</u>	Résumé de l'évaluation
Description du projet, de ce qui l'a motivé (contexte) et de ses objectifs	<u>Section 2.1</u> <u>Section 2.2</u>	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	<u>Section 2.3</u>	Résumé de l'évaluation Section 2. Rôles et responsabilités
Résumé des consultations réalisées dans le cadre de l'EFVP, s'il y a lieu	<u>Section 2.3</u>	Section 2. Rôles et responsabilités
Aperçu de l'inventaire des renseignements personnels impliqués (catégories, finalités, quantité, etc.)	<u>Section 3.1</u>	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.)	<u>Section 3.2</u>	
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	<u>Section 3.3</u>	
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)	<u>Section 3.4</u> <u>Section 4.1</u>	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	<u>Section 7</u>	
Liste et catégorisation des risques identifiés pour les personnes concernées	<u>Section 4.2</u>	Section 5. Identification des risques et des stratégies pour les atténuer
Stratégies, mécanismes et mesures déployés pour éliminer ou réduire ces risques	<u>Section 4.3</u>	
Personnes responsables de mettre en œuvre ces stratégies et personnes ou secteurs responsables de gérer les risques résiduels	<u>Section 4.4</u>	Section 6. Plan d'action
Plan d'action avec un échéancier comprenant une réévaluation périodique des mesures mises en place	<u>Section 4.4</u>	
Approbation du rapport par les hautes autorités de l'organisation (y compris noms, titres, signatures, date, etc.)	<u>Section 4.4</u>	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.



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 directrices¹⁷ :

- **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.



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 comprendre des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation afin de parvenir à une protection adéquate.

7.2 Système d'information ou de prestation électronique de services



Ces précisions concernent la situation prévue aux 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.

Qu'est-ce qu'un « système d'information ou de prestation électronique de services » ?

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.

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



Ces précisions concernent la situation prévue aux 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.



Que doit démontrer cette EFVP ?

Cette EFVP peut suivre 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**¹⁸ ou de données synthétiques, la communication de renseignements personnels n'est pas autorisée.

Si la recherche peut être menée en utilisant des **renseignements dépersonnalisés**¹⁹, 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 incapables de 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.



Attention! Le manque de ressources humaines, financières ou matérielles n'est pas un motif suffisant pour démontrer que l'obtention d'un consentement est déraisonnable.

18. 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.

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



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.

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 pour la société sont-ils attendus ?
- 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. **Vous devez 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 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.



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



Ces précisions concernent la situation prévue à l'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 2023²⁰.

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, les mesures de sécurité mises en place, 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.

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.

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.



7.5 Autres types de communications sans consentement (secteur public)



Ces précisions concernent les situations prévues à l'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 2023²¹.

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.

Que doit démontrer 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 :

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.

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.



Si l'objectif de la communication peut être atteint avec l'utilisation de **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.



Attention! Le manque de ressources humaines, financières ou matérielles n'est pas un motif suffisant pour démontrer que l'obtention d'un consentement est déraisonnable.

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 être précédée par une identification et une description des 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 pour les personnes concernées et la société sont-ils attendus ?
- 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 ?



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