SOCIÉTÉ QUÉBÉCOISE DU CANNABIS
SECRÉTARIAT GÉNÉRAL

GUIDE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Dernière mise à jour : 31 août 2023 (V1.0)

PLAN DU DOCUMENT :

Présentation du document 3
Introduction 4
- La SQDC 4
- La protection des renseignements personnels - définitions 4
  - Qu'est-ce qu'un renseignement personnel? 4
- Le cadre réglementaire 5
  - Les principes derrière la réglementation 5
  - Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels 6
- Le cadre de protection des renseignements personnels à la SQDC 6
  - Une gestion décentralisée 6
  - Le périmètre de gestion de la sqdc en protection des renseignements personnels 7
  - Cybersécurité et gouvernance 7
  - Formation et sensibilisation du personnel 8

Planification et gestion des renseignements personnels 8
- Fichiers de renseignements personnels 8
- Cartographie des systèmes, des accès et des traitements de la donnée 9
- Évaluation des facteurs relatifs à la vie privée (efvp) 9
  - Qu'est-ce qu'une efvp? 10
  - Réalisation de l'efvp 10

Le cycle de vie du renseignement personnel 11
- Collecte ou création des renseignements personnels 11
  - Limitation de la collecte 11
  - Mesures de protection particulières à l'égard des sondages 12
  - Consentement et informations à communiquer 13
- Utilisation des renseignements personnels 15
- Communication des renseignements personnels 17

Accès aux renseignements, rectification et intégrité 18
Conservation et destruction 18
Garanties de sécurité 19
Gestion des incidents 21
Définition de l'incident 21
Priorités en cas d'incident 22
Équipe et plan de gestion d'incident 22
Processus de traitement des plaintes 24
Annexe 1 : lexique et abbréviations 25

PRÉSENTATION DU DOCUMENT

Le présent document présente le cadre de la protection des renseignements personnels (la « **PRP** ») à la Société québécoise du cannabis (SQDC).

Il sert à encadrer les pratiques de PRP à travers toutes les activités de la SQDC. Il sert aussi, à la fois, d'aide-mémoire et de document explicatif pour favoriser la compréhension et l'application à tous les niveaux de la société.

Le document reprend les principaux éléments de l'encadrement législatif, des pratiques reconnues à appliquer, ainsi que les choix organisationnels de la SQDC.

Ce document vise à satisfaire à l'exigence article 63.3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « **Loi** ») :

> **63.3.** Un organisme public doit publier sur son site Internet des règles encadrant sa gouvernance à l'égard des renseignements personnels. Ces règles doivent être approuvées par son comité sur l'accès à l'information et la protection des renseignements personnels.
>
> Elles peuvent prendre la forme d'une politique, d'une directive ou d'un guide et doivent notamment prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements ainsi qu'un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles incluent une description des activités de formation et de sensibilisation que l'organisme offre à son personnel en matière de protection des renseignements personnels.
>
> Ces règles incluent également les mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage, dont une évaluation de :
>
> 1° la nécessité de recourir au sondage;
>
> 2° l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

La SQDC a adopté des pratiques de gouvernance robustes, qui traduisent l'importance qu'elle accorde à la vie privée de ses clients, employés et partenaires, ainsi qu'à la confidentialité des renseignements personnels (les « **RP** »).

INTRODUCTION

LA SQDC

La SQDC a pour mission d'assurer la vente de cannabis conformément à la loi, dans une perspective de protection de la santé, afin d'intégrer les consommateurs au marché licite du cannabis et de les y maintenir et ce, sans favoriser la consommation de cannabis.

En tant qu'entreprise du gouvernement, la PRP à la SQDC est régie par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Elle doit s'y conformer et répondre à un niveau élevé d'attentes du public face à la PRP.

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS - définitions[1]

Qu'est-ce qu'un renseignement personnel?

« Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent, directement ou indirectement, de l'identifier. »[2]

Un renseignement personnel est un actif informationnel confidentiel au sens de la *Politique de sécurité de l'information*.

La possibilité d'identification indirecte s'apprécie selon le contexte. En cas de doute, il est recommandé de s'adresser à l'équipe des affaires juridiques.

Dépersonnalisation et réidentification. Lorsqu'un renseignement personnel ne contient pas le nom et le prénom de la personne, on dit généralement qu'il est « dépersonnalisé ». Le renseignement dépersonnalisé demeure généralement un renseignement personnel, car il permet toujours d'identifier indirectement la personne. L'action d'utiliser un renseignement ou une combinaison de renseignements pour identifier la personne qu'ils concernent s'appelle la « réidentification ».

Anonymisation. Il est possible de modifier un renseignement de manière qu'il ne permette plus d'identifier une personne. On parle alors d'« anonymisation »[3]. Un renseignement anonymisé cesse d'être considéré comme un renseignement personnel, puisqu'il ne correspond plus à la définition. L'anonymisation peut être utilisée pour des applications statistiques ou comptables, lorsque l'information personnelle source elle-même n'est plus nécessaire.

[1] Pour plus de définitions, voir l'Annexe 1.
[2] Loi, art. 54
[3] Art. 73 de la Loi

Exceptions à la nature et à la confidentialité des renseignements personnels.

De manière générale, lorsqu'un RP a un caractère public en vertu de la loi, il n'est pas soumis aux règles de PRP.

Par exemple, le nom d'une personne physique n'est un renseignement personnel que s'il est associé à d'autres renseignements sur cette personne ou lorsque la mention de ce nom dans un contexte particulier aurait pour effet de dévoiler un renseignement à propos de la personne. L'article 58 de la Loi indique que « Le fait qu'une signature apparaisse au bas d'un document n'a pas pour effet de rendre personnels les renseignements qui y apparaissent. » De plus, l'article 53 identifie deux situations où les renseignements personnels peuvent ne pas être considérés comme confidentiels :

> 1° la personne concernée par ces renseignements consent à leur divulgation;
>
> 2° ils portent sur un renseignement obtenu par un organisme public dans l'exercice d'une fonction juridictionnelle; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis-clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.

Les coordonnées professionnelles ne sont généralement pas protégées par la Loi, bien qu'elles pourraient être confidentielles pour d'autres raisons.

LE CADRE RÉGLEMENTAIRE

La PRP à la SQDC est principalement encadrée par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

Les principes derrière la réglementation

- Principe de la limitation en matière de collecte.
- Principe de la qualité des données.
- Principe de la spécification des finalités.
- Principe de la limitation de l'utilisation.
- Principe des garanties de sécurité.
- Principe de la transparence.
- Principe de la participation individuelle.
- Principe de la responsabilité.

Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels

La Loi assujettit la SQDC à des obligations précises, dont notamment :

- L'obtention des consentements spécifiques pour la collecte et l'usage de RPs
- L'obligation d'inclure des obligations contractuelles de PRP dans ses contrats avec ses fournisseurs
- L'obligation de procéder à des Évaluations des facteurs relatifs à la vie privée (« **EFVP** »),
- La désignation d'un Responsable de la protection des renseignements personnels (le « **RPRP** ») et la formation d'un Comité sur la protection des renseignements personnels (le « **CPRP** »).
- Et plusieurs autres.

Plusieurs exigences de la Loi sont d'ordre plus général. Par exemple, elle rend la SQDC responsable de maintenir la confidentialité des renseignements personnels qu'elle détient.

Pour cette raison, chaque organisation prend des mesures adaptées à sa réalité pour atteindre les objectifs de la Loi. La SQDC doit prendre les moyens raisonnables pour protéger les RPs qu'elle détient. Le responsable de chaque fichier de renseignement personnel exerce cette responsabilité à l'égard du fichier en question.

LE CADRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS À LA SQDC

Une gestion décentralisée

La SQDC gère les renseignements personnels de manière décentralisée. Ce choix correspond à ses valeurs de simplicité et de responsabilité.

Ainsi, en conformité avec la *Politique de sécurité de l'information*, chaque département est responsable des renseignements personnels qu'il détient dans le cadre de ses activités. C'est le plus haut dirigeant de l'unité administrative qui est le propriétaire désigné de ces renseignements, comme pour les autres actifs informationnels de la SQDC. À titre de propriétaire, il détient l'essentiel des responsabilités de protection à l'égard de ces renseignements. Le RPRP et le CPRP assurent que les propriétaires et leurs équipes reçoivent l'encadrement et le soutien qu'ils nécessitent.

Responsable de la protection des renseignements personnels. La tâche du responsable lui est officiellement déléguée par le plus haut dirigeant de l'organisme, en vertu de la Loi. La Loi lui assigne certaines responsabilités directement. Il met notamment en place le cadre de gestion de la PRP, et prend des moyens raisonnables pour mobiliser les propriétaires de chaque fichier de renseignements.

Comité de protection des renseignements personnels. Le comité exerce plusieurs rôles. Particulièrement, il s'assure qu'une évaluation des facteurs relatifs à la vie privée est réalisée pour chaque projet qui implique des renseignements personnels. Pour cette raison, tout porteur de projet comportant des RPs doit s'adresser, au tout début du projet, au comité.

De plus, le CPRP fait le pont entre les départements concernés. Cela permet de s'assurer que chacun comprend ses rôles et responsabilités. Cela permet aussi de former les membres comme ambassadeurs du comité dans leurs équipes. Le comité comprend des représentants des T.I. et de la gouvernance, à titre

d'experts sur les volets gouvernance et sécurité de la PRP. Il comprend aussi des représentants des équipes qui détiennent des fichiers de renseignements personnels.

Avec le RPRP, le comité veille donc au respect du droit à la vie privée et à la protection des renseignements personnels au sein de la SQDC en :

- Assurant la promotion de la PRP en conformité avec le cadre juridique et le droit à la vie privée des citoyens;
- Mettant en place un cadre normatif qui reprend les règles de la Loi et qui les précise.
- Exerçant une fonction-conseil auprès des responsables pour assurer que la PRP est intégrée dans leurs activités;
- Soutenant la réalisation des activités administratives et opérationnelles liées à la PRP à chaque étape du cycle de vie des renseignements personnels.
- Assurant la formation nécessaire au sein des équipes et la disponibilité d'outils nécessaires.

Responsables de fichiers de renseignements personnels. Les responsables des fichiers de renseignements personnels le sont d'abord à titre de propriétaires d'actifs informationnels en application des politiques sur la sécurité de l'information de la Société. Les responsables de fichiers de renseignements personnels sont responsables d'en assurer la gestion et la protection à l'intérieur du cadre de la Loi et des politiques de la SQDC. Sauf exception, le responsable d'un fichier est la personne qui détient la plus haute autorité au sein du département qui le détient (*Politique de sécurité de l'information*).

Le périmètre de gestion de la SQDC en protection des renseignements personnels

La gestion de la PRP à la SQDC s'étend à tous les RPs qu'elle détient directement, mais aussi à ceux que des tiers détiennent pour son compte. La SQDC gère la protection des ces renseignements par un ensemble de mesures de gestion, par son cadre contractuel ainsi que par des mesures de suivi de la conformité au cours de la relation contractuelle.

Cybersécurité et gouvernance

La cybersécurité est un aspect important de la protection des renseignements personnels. Elle permet notamment d 'en préserver la confidentialité à l'encontre de cyberattaques ou d'autres divulgations non-intentionnelles. La cybersécurité favorise aussi la continuité des affaires.

Certains principes de gouvernance sont nécessaires pour assurer la sécurité de l'information. En effet, même si le périmètre technologique de la SQDC est sécurisé par des moyens techniques, le comportement des utilisateurs peut renforcer, mais aussi compromettre la confidentialité.

La PRP comprend aussi des mesures de gouvernance qui lui sont spécifiques, en plus de celles qui s'appliquent à la sécurité de l'information. Parmi les mesures supplémentaires, on peut penser à la limitation de la collecte, à l'obtention du consentement, à la limitation de l'usage des renseignements, à la limitation des communications externes de renseignements. De plus, la conception des systèmes technologiques devrait viser l'accessibilité des renseignements personnels dans un format pratique, et la

possibilité de rectifier cette information. Il s'agit d'un exemple d'équilibre entre la cybersécurité et une autre exigence de PRP, en l'occurrence, l'accessibilité.

Le présent document vise principalement à établir les règles et principes de gouvernance qui sont propres à la protection et la gouvernance des renseignements personnels. Elles doivent être appliquées en conjonction avec les règles de sécurité de l'information établies à l'égard de tous les actifs informationnels, notamment celles de *la Politique de sécurité de l'information*.

Formation et sensibilisation du personnel

Un programme de formation en sécurité de l'information est suivi par les employés de la SQDC sur une base trimestrielle. Le programme est assorti de tests administrés sur une base régulière.

Tous les nouveaux employés administratifs de la SQDC sont sensibilisés à la protection des renseignements personnels au moment de leur intégration.

Annuellement, un rappel est présenté au personnel administratif de la SQDC concernant le présent guide et la protection des renseignements personnels.

Chaque département responsable d'au moins un fichier de PRP délègue l'un de ses équipiers à titre de membre du comité de PRP. Ces délégués reçoivent une formation adaptée à leur fonction d'ambassadeur de la PRP au sein de leurs équipes respectives.

Les moyens de formation en matière de gestion des incidents sont prévus à la procédure portant sur cette question.

Finalement, d'autres activités de formation et de sensibilisation sont offertes en fonction des besoins et changements.

Les partenaires d'affaires de la SQDC, lorsqu'ils sont appelés à traiter des renseignements personnels, sont sensibilisés par les propriétaires de leur contrat et par les mesures de conformité d'application pour chacun de leurs contrats.

PLANIFICATION ET GESTION DES RENSEIGNEMENTS PERSONNELS

FICHIERS DE RENSEIGNEMENTS PERSONNELS

Le fichier de renseignements personnels est l'emplacement où l'on sauvegarde obligatoirement l'ensemble des renseignements personnels recueillis pour une fin particulière, ou un certain nombre de fins particulières.

Chaque département tient à jour un inventaire des fichiers de renseignements personnels qu'il détient. Cet inventaire est le point de départ de la PRP et sert de support pour appliquer les mesures nécessaires aux fichiers et aux systèmes dans lesquels ils sont stockés. L'inventaire permet notamment de gérer les accès à un fichier, d'appliquer les règles de conservation et de suppression des renseignements, ainsi que d'identifier le propriétaire du fichier. Une attention particulière doit être portée à tout projet pouvant mener à la création d'un nouveau fichier de RP. La réalisation d'une Évaluation des facteurs relatifs à la vie privée (EFVP) permettra de générer le nouveau fichier, tel qu'il sera détaillé ci-après.

L'inventaire doit être transmis par son propriétaire au RPRP. Le RPRP est chargé maintenir à jour les inventaires de mettre à jour l'inventaires des fichiers de RP requis par la Loi[4] et d'en faire la diffusion sur SQDC.ca.

En plus des fichiers, les communications de renseignements personnels sans le consentement de la personne concernée doivent être consignées dans un registre public, en indiquant la raison de chaque communication.

CARTOGRAPHIE DES SYSTÈMES, DES ACCÈS ET DES TRAITEMENTS DE LA DONNÉE

Pour faciliter davantage la gestion, l'enregistrement des fichiers de RP est complété par un suivi administratif des Traitements de données. Les Traitements incluent les usages de l'information, mais aussi les manipulations et les communications de renseignements tout au long du cycle de vie de la donnée.

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (EFVP)

L'évaluation des facteurs relatifs à la vie privée est un outil de gestion des RP en fonction du risque. Cet outil est d'usage commun et obligatoire dans un nombre croissant de juridictions.

La Loi exige la réalisation d'EFVP dans plusieurs situations, soit, en règle générale, au moment de planifier les projets impliquant des renseignements personnels. Par exemple :

1. Projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels.
2. Communication de renseignements personnels à l'extérieur du Québec,
3. Sondages recueillant ou utilisant des renseignements personnels.
4. Mise en place de vidéosurveillance.

Toutefois, elle est aussi exigée avant d'appliquer différentes exceptions permettant la communication de renseignements sans nécessité de consentement de la personne concernée (à des fins de statistiques, ou pour la mise en œuvre de programmes gouvernementaux ou dans l'intérêt manifeste de la personne, par exemple).

Le propriétaire de tout projet qui impliquera le traitement de renseignements personnels doit, dès l'étape de la conception du projet, réaliser une EFVP. Pour ce faire, il complète la formule prévue à cette fin. Il peut en tout temps demander l'aide et l'accompagnement du RPRP et de son équipe.

L'EFVP doit être présentée dès que possible au Comité de protection des renseignements personnels. Le CPRP l'étudie et formule ses recommandations sur la conception du projet, sur sa conformité à la Loi et aux normes de la SQDC, sur le caractère adéquat des mesures de mitigation prévues et des risques identifiés, et peut également recommander toute mesure additionnelle de protection.

[4] Art. 76 de la Loi

L'EFVP facilite l'inventaire des fichiers de RPs, synthétise les mesures de mitigation en place dans l'organisation et leur impact sur les risques d'incident, et identifie les mesures à mettre en place dans l'organisation et au cours du projet en particulier.

La SQDC a mis en place un processus simple et efficace pour réaliser les EFVP. Elle a formé des ambassadeurs à son utilisation au sein des équipes propriétaires de renseignements personnels.

Qu'est-ce qu'une EFVP?

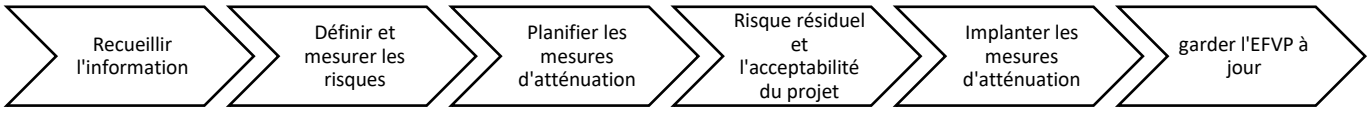
L'EFVP est un outil pour identifier et gérer les risques en PRP d'un projet, d'un système technologique, d'un processus, d'une analyse, d'une relation d'affaires, etc. Dans sa plus stricte définition, l'EFVP consiste en une analyse qui :

1) Identifie sommairement le projet ou le système, les besoins d'affaires et les buts recherchés.
2) Identifie les renseignements personnels qui seront recueillis, incluant les « champs de formulaire ».
3) Identifie les risques du projet ou du système, et évalue chaque risque selon la probabilité qu'il se matérialise et l'impact de sa matérialisation.
4) Identifie les mesures de mitigation du risque, et quantifie l'effet des mesures sur la probabilité et/ou l'impact.
5) Le cas échéant, répondent aux questionnements prescrits par la Loi selon la nature du projet visé
6) Si les équipes le souhaitent, l'EFVP peut être supplémentée par l'identification des processus de collecte de renseignements et des consentements à obtenir, ou par l'identification d'autres éléments de conformité utiles à la planification en amont.

L'EFVP est tenue à jour en cas d'évolution du projet, ce qui permet d'adapter les mesures de protection et de les documenter pour référence ultérieure.

Réalisation de l'EFVP

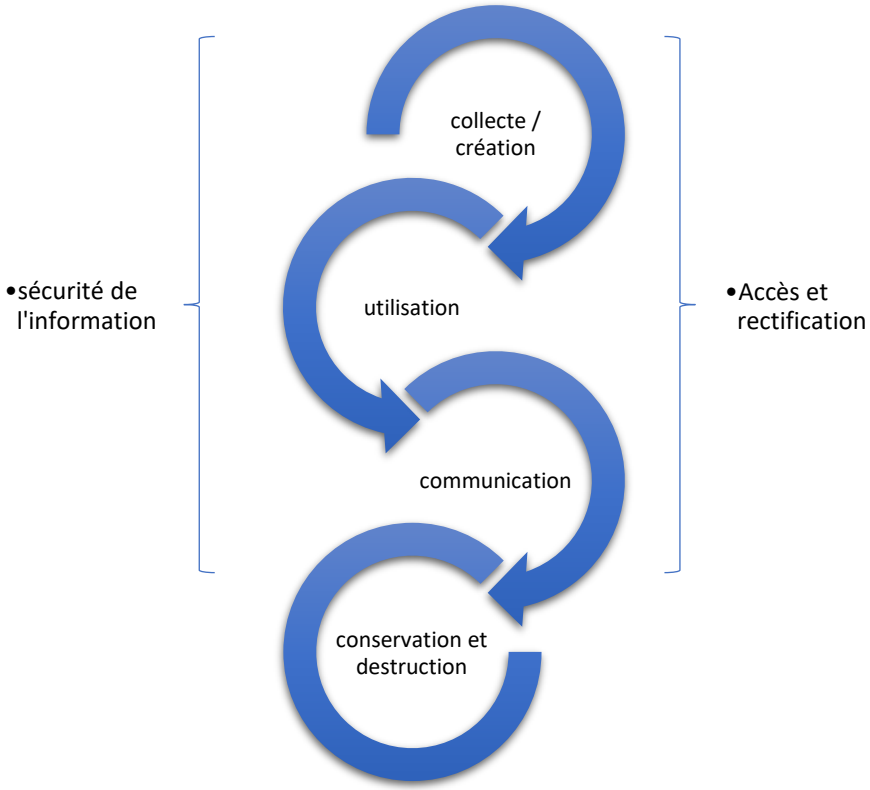
Les étapes de la réalisation d'une EFVP sont les suivantes :



Le responsable du projet est responsable de préparer un projet d'EFVP le plus tôt possible et avant le début du projet. De plus, il doit aviser le comité dès qu'il commence à préparer l'EFVP et présenter celle-ci au comité dès qu'une première version est préparée.

LE CYCLE DE VIE DU RENSEIGNEMENT PERSONNEL

Le renseignement personnel doit être géré à toutes les étapes de son cycle de vie. Il ne suffit pas de le placer dans un fichier sécurisé et de l'y oublier.



COLLECTE OU CRÉATION DES RENSEIGNEMENTS PERSONNELS

La collecte de RPs est la manière classique par laquelle ceux-ci entrent dans le périmètre de responsabilité de la SQDC. La création de RPs réfère le plus souvent à la création de nouveaux renseignements à partir de ceux qui existent déjà, sans le concours de la personne concernée. On peut penser à l'ajout d'un rapport d'évaluation au dossier d'un employé, ou d'une compagnie qui utiliserait des profils-client existants afin de classer ceux-ci selon une segmentation de marché. Évidemment, plus on collecte ou crée de RPs, plus on en a à gérer et protéger.

Limitation de la collecte

La collecte de RPs doit être la plus limitée possible. La limitation de la collecte peut résulter de la conception d'un projet, d'un processus ou d'un système. Elle peut aussi résulter des exigences légales. La limitation de la collecte exige que les finalités d'utilisation aient été déterminées avec précision *avant* de procéder à la collecte.

Limitation par la loi. En plus du principe général, la SQDC est limitée par la Loi. Celle-ci prévoit :

> **64.** Nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a la gestion.

Bien que l'article offre une certaine marge d'appréciation, il exige que la SQDC soit en mesure de justifier comment la collecte d'un renseignement personnel lui permet d'exercer ses attributions (par exemple, de remplir sa mission). Plus les RP sont sensible, plus le critère de la nécessité sera strict. À ce propos, la Commission d'accès à l'information (la « **CAI** ») indique :

> Ce principe doit s'interpréter au regard de la finalité poursuivie par l'entreprise privée ou par l'organisme public. Un renseignement personnel est nécessaire si la finalité poursuivie est légitime, importante, urgente et réelle et si l'atteinte au droit à la vie privée consécutive à la collecte, la communication ou la conservation de chaque élément de renseignement est proportionnelle à cette finalité (c.-à-d. la collecte des renseignements est-elle rationnellement liée aux objectifs visés, l'atteinte au droit à la vie privée est-elle minimisée et la divulgation du renseignement requis est-elle nettement plus utile à l'entreprise que préjudiciable à la personne concernée).

Cette limitation inclut également toute collecte ou création de RP pour une fin qui serait elle-même illégitime (ex : cas de surveillance qui enfreindrait lui-même, de manière non-justifiée, la vie privée des employés ou des clients). Finalement, cette limitation s'applique même si la personne concernée consent à une collecte ou une utilisation non-nécessaire.

Limitation par la conception. Dans la conception d'un système ou d'un processus, il faut limiter la collecte de renseignements personnels. Il faut toujours commencer par se demander s'il est possible d'atteindre les buts recherchés sans recueillir de renseignements personnels. De plus, il faut répondre aux besoins en recueillant le moins de renseignements possible. Par exemple, une étude pourrait éviter de demander l'adresse des répondants, si leur code postal suffit. Parfois, les trois premiers caractères du code postal suffiront. Il existe une multitude de stratégies pour limiter la collecte. La section « conservation et destruction » contient, de plus, des notions qui permettent de limiter le volume de RP en circulation en éliminant rapidement les renseignements dont l'utilité a été remplie.

Mesures de protection particulières à l'égard des sondages

Avant de recueillir ou d'utiliser des renseignements personnels à des fins de sondage, la SQDC procède à l'évaluation prévue par la Loi. Cette évaluation concerne la nécessité de recourir au sondage, l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation. Cette évaluation peut prendre la forme d'une EFVP simplifiée, qui inclut la réponse à ces questions, et dont l'ampleur pourra être réduite en fonction de la sensibilité des renseignements visés et du niveau de risque anticipé.

Consentement et informations à communiquer

Le consentement à la collecte auprès de la personne adulte[5] concernée s'obtient au moment de la collecte. L'article 53.1 de la Loi ajoute :

> Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé.

La Loi établit un mécanisme où le consentement libre et éclairé s'obtient en informant la personne concernée avant qu'elle ne fournisse ses renseignements personnels. La Loi précise, à l'article 65.0.2, que le fait de donner ses renseignements après avoir été informé conformément à la Loi équivaut à un consentement. Si c'est un tiers qui recueille des renseignements pour la SQDC, celle-ci doit s'assurer que ce tiers respecte la Loi.

Au moment de recueillir un renseignement personnel, il faut transmettre les renseignements suivants à la personne concernée pour obtenir son consentement :

Le nom de l'organisme au nom de qui la collecte est faite. Plusieurs informations peuvent être données sur les pages Web menant à une commande, par exemple, ou dans des papiers d'embauche ou de recrutement.

La ou les fins (utilisations) auxquelles ces renseignements sont recueillis. Il s'agit d'une information cruciale. Il faut être suffisamment exhaustif (préciser toutes les utilisations), clairs et précis (ex : pour la paye, les avantages sociaux, pour des fins de statistiques, etc.). La plupart des utilisations d'un renseignement seront impossibles si le consentement n'a pas été obtenu pour cette utilisation. Si une ou des utilisations sont ajoutées, il faut redemander le consentement. Il est donc important de couvrir dans le consentement toutes les utilisations raisonnablement prévisibles pour éviter de recommencer inutilement le processus de consentement. Dans la conception des consentements, il faudra par ailleurs établir un équilibre entre la précision et la surabondance d'information.

Les moyens par lesquels les renseignements sont recueillis. Identifier toutes les méthodes de collecte des renseignements. Cette information peut être évidente (ex : lorsqu'il est demandé de remplir un formulaire). Par contre, elle devient particulièrement importante lorsque des renseignements supplémentaires sont recueillis sans devoir être fournis directement par la personne concernée (ex : après vérification auprès d'anciens employeurs, etc.) .

Le caractère obligatoire ou facultatif de la collecte. La collecte est appelée « obligatoire » si on n'a pas le choix de donner le renseignement pour bénéficier d'un service. Par exemple, on ne peut pas recevoir de livraison sans donner son adresse (cela est indiqué par un astérisque à côté du champ « adresse »), ou encore, on ne peut pas recevoir un dépôt direct sans fournir un spécimen de chèque. La collecte est appelée « facultative » si on peut recevoir le service sans fournir les renseignements (par exemple, répondre à un questionnaire d'appréciation). Une collecte facultative permet à la personne concernée de

[5] La Loi stipule des règles pour les mineurs, mais elles ne s'appliquent pas à la SQDC puisque celle-ci dessert une clientèle adulte.

retirer son consentement. Lorsque cela est praticable et ne nuit pas à ses activités, la SQDC désigne la collecte comme étant « facultative ».

Les conséquences pour la personne concernée, ou, selon le cas, pour le tiers, si elle choisit de ne pas communiquer les renseignements ou de retirer son consentement. Généralement, cela est surtout applicable dans le cas d'une demande obligatoire. Il arrive souvent que la conséquence est incluse dans la demande (ex : veuillez fournir un spécimen de chèque pour recevoir un dépôt direct).

Les droits d'accès et de rectification prévus par la loi. Il faut mentionner que la personne concernée peut, sur demande, accéder aux renseignements personnels recueillis à son sujet et en demander la rectification. À titre de rappel, une telle demande est adressée, sans formalité, au responsable de l'accès à l'information de la SQDC, tel qu'indiqué à la page prévue à cet effet sur SQDC.ca.

Le nom du tiers qui recueille les renseignements au nom de la SQDC. *Lorsqu'un tiers agit comme mandataire de la SQDC et recueille des renseignements personnels en son nom, cela doit être transparent et la personne concernée doit en être informée avant la collecte.*

Le nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements pour faire usage de ceux-ci. *Par exemple, dans le cas de la livraison, il sera nécessaire de communiquer à l'entreprise de livraison les coordonnées postales et le nom du client. De plus, il faut informer la personne s'il y a une possibilité que ces renseignements soient communiqués à l'extérieur du Québec.*

Les informations qui précèdent doivent être communiquées à la personne concernée au moment de la collecte des renseignements, pour établir un consentement valide.

Sur demande de la personne concernée, il faut également lui transmettre les renseignements suivants :

Les renseignements recueillis auprès de cette personne. Identifier précisément quels sont les renseignements qui seront recueillis par la SQDC.

Les catégories de personnes qui vont avoir accès aux renseignements au sein de la SQDC. Il peut s'agir d'une direction, par exemple, ou d'une équipe au sein d'une direction (ex : l'équipe du recrutement, le service à la clientèle, etc.)

La durée de conservation des renseignements. Il faut indiquer les critères et la durée de conservation du renseignement. Évidemment, cela implique que toute nouvelle collecte de renseignements personnels doit être déclarée au responsable de la PRP et ajoutée au registre, et que sa durée de conservation doit être prévue.

Les coordonnées du responsable de la protection des renseignements personnels. Les moyens pour pouvoir communiquer avec le Responsable doivent être fournis.

Cookies et moyens de profilage. La Loi prévoit, de plus, que la cueillette de renseignements personnels à l'aide d'une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci devra :

1. Informer la personne concernée de l'utilisation de cette technologie, et
2. Informer cette personne des moyens offerts pour activer cette fonction (protection par défaut).

C'est la raison pour laquelle plusieurs sites Internet, principalement Européens, affichent une notice à l'entrée pour demander l'activation des cookies et des technologies de localisation « pour vous présenter un contenu pertinent et adapté ».

La SQDC utilise certains témoins de connexion (*cookies*). Ils ne recueillent pas tous des renseignements personnels, mais certains pourraient permettre la réidentification des personnes concernées. Ces témoins sont divulgués dans SQDC.ca. Plusieurs sont obligatoires en ce qu'ils permettent à la SQDC de faire fonctionner son site Web.

Aspects pratiques. En pratique, la communication des informations de consentement devrait être facile et sans erreur. En effet, en complétant l'EFVP pour le processus ou le projet, les fins devraient avoir été clairement identifiées, et les informations requises pour le consentement devraient avoir été déjà documentées.

Qualité du consentement. Le consentement à la collecte et à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune des fins prévues, en termes simples et clairs. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. Par ailleurs, la Loi vient réitérer ces principes expressément à son article 53.1, qui exige aussi que l'information soit donnée distinctement de toute autre information donnée à la personne concernée.

Il en va d'ailleurs de même pour le consentement à l'utilisation et à la communication. Dès que possible, ces consentements sont obtenus au moment de la collecte, et ce, même si ces étapes surviennent plus loin dans le cycle de vie du renseignement. À défaut, il faudra retourner chercher le consentement après-coup, au moment où on doit utiliser ou communiquer le renseignement.

Documentation du consentement. Même si la Loi n'exige pas que la personne concernée signe un formulaire de consentement, il est important de prendre des moyens pour documenter le consentement. Le consentement exprès est préférable à un consentement implicite. Ainsi, l'obtention verbale du consentement doit être notée par la personne qui recueille le renseignement, avec mention de son nom. L'obtention écrite du consentement peut être une mention visible par la personne avant de compléter un formulaire Web. Alternativement, il peut s'agir d'une case que la personne doit cocher avant de transmettre ses renseignements. Lorsqu'il s'agit de supports technologiques (ex : SQDC.ca), il importe de documenter les versions des formulaires et les dates précises de leur utilisation. Il est ainsi possible de démontrer comment le consentement a été obtenu en fonction de la date où la collecte de renseignement a eu lieu.

UTILISATION DES RENSEIGNEMENTS PERSONNELS

Limitation de l'utilisation selon les fins. L'utilisation des renseignements personnels doit se limiter aux fins pour lesquelles le renseignement a été obtenu :

> **65.1** Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.

On retrouve ces fins dans l'EFVP, ainsi que dans la formule de consentement à la collecte. Un usage est jugé compatible avec ce qui a été décrit lors du consentement s'il y a « un lien pertinent et direct » entre les deux. Même si une utilisation a été envisagée, elle ne peut pas être valide si elle n'a pas été communiquée à la personne concernée au moment du consentement. La seule option disponible sera alors de demander le consentement de la personne pour le nouvel usage.

***Utilisation nécessaire pour l'application d'une loi*.** Malgré la règle générale de limitation de l'utilisation, il est possible d'utiliser un RP si cette utilisation est nécessaire à l'application d'une loi au Québec (art. 65.1 de la Loi). Cette exception doit s'appliquer dans les stricts cas qui le justifient, et elle doit être signalée immédiatement au RPRP, car celui-ci doit l'inscrire dans un registre spécial, prévu à l'article 67.3 de la Loi.

Dépersonnalisation à des fins d'étude, de recherche ou de statistiques. La SQDC peut procéder à une dépersonnalisation prudente, assortie de mesures de protection, des renseignements personnels. À cette condition, elle pourra les utiliser à des fins d'étude, de recherche ou de statistiques.

Gestion des accès. La limitation de l'utilisation ne s'étend pas seulement à ce que l'organisation fait avec le renseignement. Il faut aussi en limiter l'accès aux seules personnes qui en ont besoin pour que les fins identifiées soient accomplies. Les accès peuvent faire l'objet d'une ségrégation ou d'une limitation supplémentaire, pour des raisons de sécurité, par exemple. Les différents profils d'accès permettent de donner à chaque employé ou catégorie d'employés seulement les accès nécessaires pour faire sa tâche.

La gestion des accès suit les mêmes principes peu importe le système. Le responsable du fichier de RP est de facto responsable de la gestion des accès. En général, les systèmes offrent une interface permettant de gérer directement les accès et les profils d'accès. Même si une autre personne conserve le profil d'administratrice du système où le fichier de RP est stocké, le responsable du ficher conserve l'entière responsabilité de donner à celle-ci les instructions nécessaires pour bien gérer les accès. Une brève procédure peut remplir cette fonction.

Sécurité dans l'utilisation. L'utilisation des renseignements personnels doit être faite de manière à minimiser les risques de fuite, d'accès non-autorisé, de vol, de perte ou d'autres incidents. Le choix des mesures à prendre pour protéger un renseignement dépend de la nature du traitement qui en est fait. Lors d'un nouveau projet, l'EFVP identifie d'avance les mesures à mettre en place lors de sa réalisation.

Traitements manuels et permission : La SQDC limite autant que possible, les traitements manuels. Lorsqu'un traitement manuel ne peut être évité, d'autres mesures de contrôle sont mises en place. De plus, à moins d'une permission donnée à des fins spécifiques et pour des motifs exceptionnels, il est interdit de sauvegarder un renseignement personnel sur le disque local d'un ordinateur ou d'un appareil, ni sur un disque amovible (ex : clé USB).

Utilisation par des tiers. Les contrats de la SQDC imposent des obligations analogues à ses propres pratiques aux tiers avec qui elle fait affaire pour le traitement de renseignements personnels. Les sous-traitants et fournisseurs de la SQDC, dont notamment en matière de livraison, sont liés par des exigences contractuelles en matière de PRP, de conformité à la Loi, et de respect de bonnes pratiques reconnues ou d'attestation de conformité à des normes reconnues. La SQDC complète ces mesures, lorsque nécessaire, en faisant le suivi de l'application de ces obligations, en transmettant des demandes et précisions additionnels au fournisseur, ou en prenant toute autre mesure appropriée.

COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

La communication d'un renseignement personnel s'entend de la transmission de ce renseignement à une personne qui n'est pas la SQDC elle-même ou un de ses employés. Elle ne peut être faite que moyennant le consentement de la personne concernée. Ce consentement s'obtient au moment de la collecte, à défaut de quoi, la personne concernée devra être contactée ultérieurement afin d'obtenir son consentement à la communication avant de procéder à celle-ci.

Il existe des cas précis d'exception à la règle du consentement à la communication. Ceux-ci se limitent aux situations prévues par la Loi. Dès qu'on utilise l'une de ces exceptions, et qu'on communique des RPs sans l'autorisation de la personne concernée, on doit l'inscrire dans le Registre des communications de renseignements personnels sans consentement, qui est tenu par le responsable de la PRP. Les principales exceptions qui pourraient s'appliquer à la SQDC sont présentées ci-après. Elles doivent être interprétées de manière restrictive. Avant d'appliquer l'une de ces exceptions, le responsable du renseignement devrait toujours consulter le RPRP ou un membre de son équipe pour valider que celle-ci est employée correctement.

Communication pour l'application d'une loi au Québec. Comme pour l'usage, il n'est pas obligatoire de demander le consentement de la personne concernée pour communiquer ses renseignements personnels, si cette communication est nécessaire à l'application d'une loi au Québec.

Communication pour l'application des conditions de travail. La SQDC peut communiquer un RP, sans le consentement de la personne concernée, pour appliquer les conditions de travail prévues par une convention collective, une politique, une directive, un règlement. Cela inclut certaines communications avec le syndicat ou les gestionnaires des régimes d'avantages sociaux, ou encore, avec le RRQ.

***Communication à un avocat ou un membre d'un ordre professionnel*.** Lorsque la SQDC communique un renseignement personnel à son procureur dans le cadre d'un litige, elle n'a pas à demander le consentement ni à l'inscrire au registre des communications. Lorsqu'elle communique un renseignement à un avocat en-dehors d'un litige, ou à un membre d'un autre ordre professionnel, elle doit indiquer ces communications dans son registre, de même que confier le mandat par écrit à ce professionnel.

Communications à la police. La SQDC peut communiquer à la police ou des inspecteurs en matière pénale, lorsque la communication est nécessaire à une poursuite pour une infraction à une loi applicable au Québec. Un formulaire est publié sur le site Internet et doit être complété par la police et conservé par la SQDC. Par contre, la communication ne requiert pas de consentement de la personne concernée, et ne doit pas être inscrite au registre.

Communication à un fournisseur de services. La SQDC peut, à certaines conditions, communiquer des renseignements personnels à une personne à qui elle a confié un mandat ou un contrat de service. Il est à noter que les dispositions de la Loi en matière de consentement exigent la transmission de certaines informations à cet égard.

Le mandat donné à un fournisseur qui manipulera des renseignements personnels doit être bien encadré. Si le fournisseur n'est pas un organisme public ou un membre d'un ordre professionnel, l'article 67.2 de la Loi exige qu'il soit confié par écrit et qu'il comprenne, au minimum, les protections prévues à cet article.

Communications pour des fins de recherche. Certaines exceptions au consentement obligatoire sont prévues par la Loi dans un but d'étude, de recherche ou de production de statistiques. Ce type de

communication intervient sur demande du chercheur ou de l'organisme, et doit rencontrer plusieurs critères prévus aux articles 67.2.1 à 67.2.3 de la Loi.

Communication et sécurité. Toute communication de renseignements personnels à un tiers ne doit être faite que par des moyens sécurisés.

Communication hors Québec. Une communication hors Québec doit faire l'objet d'une EFVP pour évaluer les risques d'une telle communication. La SQDC doit s'assurer que le degré de protection du renseignement n'est pas diminué du fait de sa communication, de son traitement ou de son stockage à l'extérieur du Québec.

ACCÈS AUX RENSEIGNEMENTS, RECTIFICATION ET INTÉGRITÉ

Les renseignements doivent être facilement accessibles. Cela est vrai pour assurer le droit d'accès et de rectification de la personne concernée. Par contre, c'est aussi vrai pour assurer l'accès aux employés qui en ont besoin pour offrir des services à la personne concernée.

Il est donc important de s'assurer que les renseignements personnels contenus dans un fichier présentent des garanties d'intégrité suffisantes et proportionnelles à l'importance des fins pour lesquelles ces renseignements seront utilisés.

Pour les besoins des demandes d'accès et de rectification, les renseignements à propos d'une personne et qui sont détenus dans un système doivent pouvoir en être extraits facilement et dans un format communément employé.

Les demandes visant l'accès à des renseignements personnels ou la rectification de ceux-ci peuvent être faites par toute personne à l'attention de la personne responsable de la PRP et responsable de l'accès à l'information, dont les coordonnés sont publiées dans la section « accès à l'information » du site SQDC.ca. Le responsable procédera à l'identification de la personne qui fait la demande, à la recherche des renseignements visés, ainsi qu'à la détermination de la recevabilité de la demande conformément à la Loi. Sa réponse fera état de sa décision et, le cas échéant, des actions prises pour donner suite à la demande.

CONSERVATION ET DESTRUCTION

Conservation. La conservation d'un renseignement personnel a lieu tant qu'elle est utile pour les fins auxquelles le renseignement a été recueilli. La conservation peut être partielle ou totale, et être à l'état actif ou semi-actifs (archivé). Un renseignement conservé pour archivage (ex : en cas de vérification comptable ou de litige) peut être conservé dans un format et d'une manière qui réduit les risques liés à la sécurité de l'information, surtout si l'exigence d'accessibilité devient moins pertinente en raison de son état semi-actif. Par exemple, cette information pourrait être dépersonnalisée. Si certaines informations doivent être conservées, mais que les renseignements personnels qu'elles contiennent ne sont plus requis, elles sont anonymisées. De cette façon, l'information n'est plus soumise aux règles de protection des renseignements personnels.

La conservation vise notamment à prévenir la destruction accidentelle, la dégradation ou l'accès non autorisé aux données.

Lorsque le renseignement est à l'état actif, il importe, de plus, de s'assurer qu'il demeure d'une qualité et d'une intégrité suffisante pour servir aux fins pour lesquelles il a été recueilli et pour lesquelles il est conservé. L'effort déployé pour soutenir l'intégrité d'un renseignement doit être proportionnel à l'importance de l'utilisation de ce renseignement (par exemple, la mention d'une allergie mortelle dans la liste des invités à un banquet).

Destruction. En règle générale, un renseignement personnel devrait être conservé le moins longtemps possible. Le consentement de la personne concernée expire lorsque l'usage envisagé et divulgué a été atteint. De plus, la destruction ne vise pas seulement un fichier dans son entièreté ou toute la ligne concernant une personne dans un chiffrier Excel ou une base de données. Même si une partie des renseignements personnels d'un fichier demeurent utiles, il pourrait être approprié d'élaguer le nombre de renseignements conservés, par exemple, en détruisant une colonne d'un chiffrier ou certains documents qui, eux, ne sont plus utiles.

Le calendrier de conservation de documents prévoit plusieurs délais de conservation pour la plupart des types de documents détenus à la SQDC, incluant les fichiers de renseignements personnels.

Limitation des renseignements conservés. Comme pour la conception de la collecte, on peut limiter les RP que l'on conserve, et détruire ceux qui n'étaient nécessaires que temporairement, pour un traitement particulier. Une collecte plus large a alors lieu pour répondre à des besoins, mais l'identification des usages, et de leur durée dans le temps, permet de raccourcir la durée de conservation de l'ensemble ou d'une partie des renseignements collectés.

GARANTIES DE SÉCURITÉ

Les renseignements personnels étant des actifs informationnels, leur sécurité est régie par la *Politique de sécurité de l'information* et la *Directive de sécurité de l'information*. Les renseignements personnels sensibles sont considérés, pour les fins de la politique, comme des actifs informationnels critiques.

La sécurité des systèmes eux-mêmes est assurée par plusieurs mesures. Ces mesures sont mises en place par les experts de nos équipes T.I. et par les fournisseurs des solutions utilisées.

Les propriétaires d'actifs informationnels sont responsables de l'application des mesures de gouvernance en matière de sécurité de l'information (par exemple, la journalisation avec ou sans surveillance, ou le blocage par défaut de fonctionnalités à risque). Ils sont également responsables des mesures de gouvernance spécifiques à la protection des renseignements personnels. Celles-ci sont prévues au présent guide, étant entendu que les responsables ne sont pas tenus de s'y limiter.

Sécurité des fournisseurs et mandataires externes. Les questions liées à la sécurité des fournisseurs sont gérées par le responsable du fichier de renseignements, avec le soutien des équipes de sécurité de l'information, d'approvisionnement en biens et services et des affaires juridiques. Les clauses contractuelles nécessaires sont mises en place afin de se conformer à la Loi, et que le fournisseur ait les obligations nécessaires pour assurer la sécurité des renseignements. Ces clauses incluent des mécanismes permettant leur bonne application. Elles peuvent comprendre, selon le cas, les garanties techniques jugées suffisantes par les équipes de sécurité de l'information, des exigences de certification avec ou sans audit, en lien avec des normes ou des paramètres de protection généralement reconnus, ou encore la possibilité de réaliser un audit indépendant. La nature des clauses requises varie en fonction du bien ou service fourni et du risque posé.

Dès le début du contrat, le fournisseur est sensibilisé par le responsable du contrat concernant ses obligations en matière de PRP. Le responsable du contrat maintient une attitude vigilante lors des suivis de la relation contractuelle.

GESTION DES INCIDENTS

Définition de l'incident

La Loi définit comme suit un incident en PRP :

63.8. Pour l'application de la présente loi, on entend par « incident de confidentialité » :

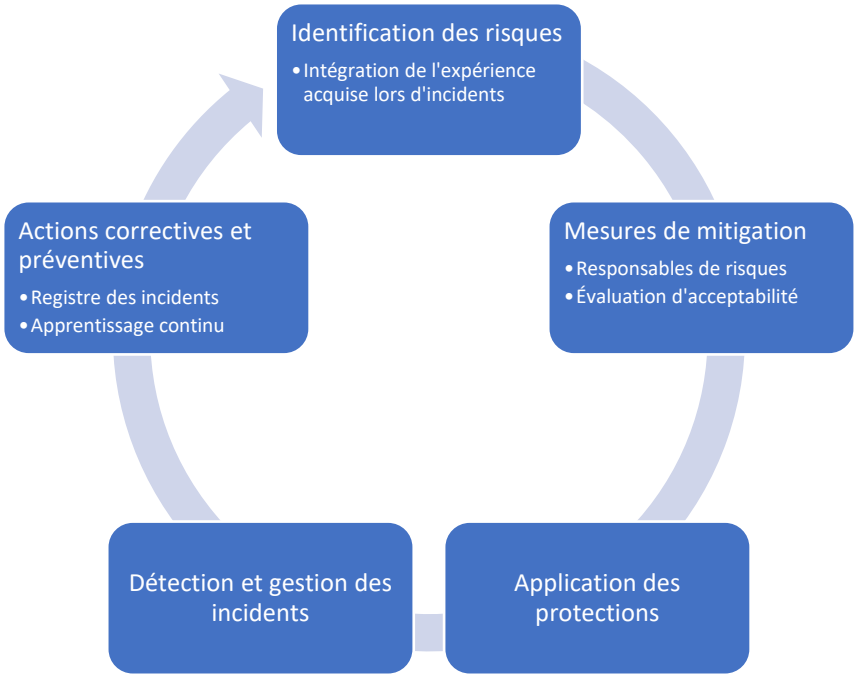
1° l'accès non autorisé par la loi à un renseignement personnel;

2° l'utilisation non autorisée par la loi d'un renseignement personnel;

3° la communication non autorisée par la loi d'un renseignement personnel;

4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

La SQDC possède un cadre obligatoire de gestion des incidents de confidentialité, incluant le signalement à la CAI et aux personnes concernées s'il y a un risque de préjudice, ainsi que la mise en place d'actions pour corriger la situation à l'origine de l'incident et prévenir les incidents futurs. Le RPRP maintient un registre des incidents de confidentialité. La gestion d'incident forme donc le cycle suivant :



Priorités en cas d'incident

La priorité absolue en cas d'incident est le signalement. Toute personne qui détecte ou soupçonne un incident de confidentialité doit immédiatement inscrire cet incident dans le système de gestion des incidents, et aviser le RPRP. S'il s'agit d'un tiers ou d'un membre du public, il est invité à le communiquer à toute personne à la SQDC, dont le RPRP (accesalinformation@sqdc.ca) ou au centre de relations client.

Une fois l'incident signalé, la SQDC l'évalue le plus vite possible, et identifie les renseignements et les personnes touchés.

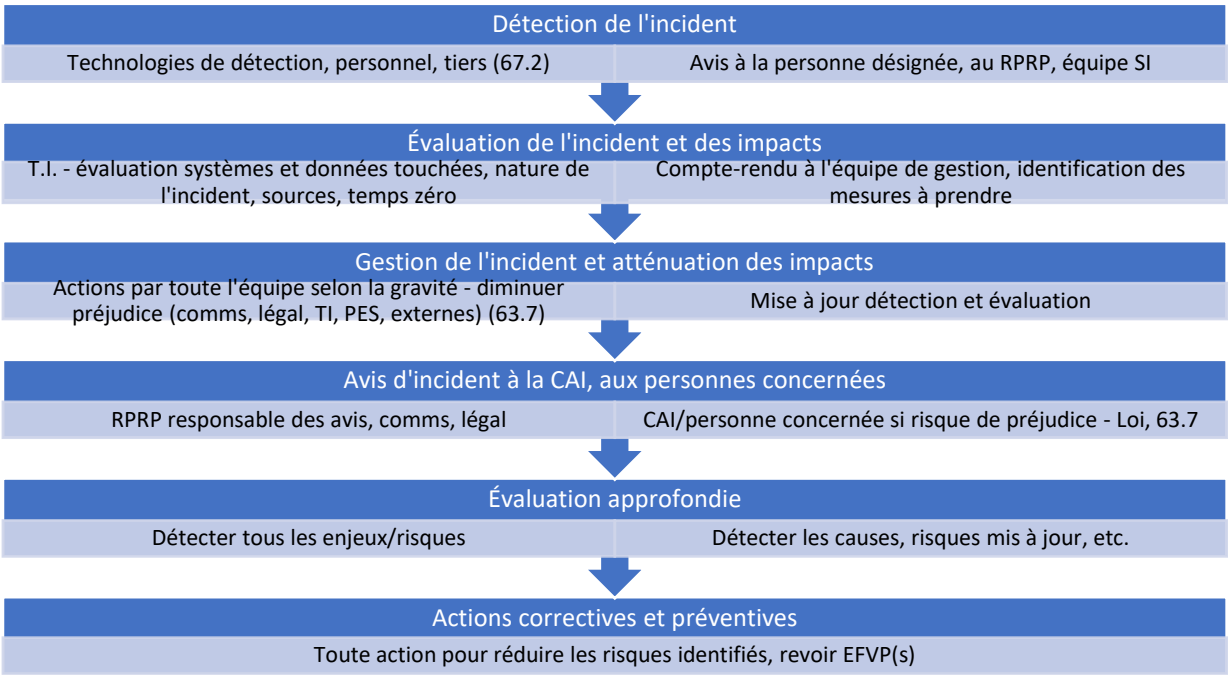
Le cadre de gestion des incidents prévoit les autres rôles et responsabilités en cas d'incident. Cela inclut la manière dont le RPRP évalue la gravité de l'incident et le risque de préjudice, les actions à prendre en conséquence en conformité avec la Loi, ainsi que l'enregistrement des incidents et la mise en place des action correctives et préventives.

Équipe et plan de gestion d'incident

Le cadre de gestion des incidents prévoit à l'avance quelles sont les personnes et les étapes nécessaires pour la résolution et la gestion de l'incident.

Au sein de sa procédure, la SQDC prévoit des équipes plus réduites et opérationnelles dans les cas d'incidents mineurs ou techniques, auxquelles s'ajoute une cellule de gestion de crise en cas d'incident majeur, afin de gérer les retombées importantes tout en protégeant la disponibilité des équipes de résolution de l'incident.

Le graphique qui suit présente les étapes de gestion d'incident de manière séquentielle. À noter, que les étapes peuvent se répéter de manière cyclique. Par exemple, une détection supplémentaire de l'incident et de son ampleur sera faite en continu, et permettra de réévaluer constamment l'incident et ses impacts, identifier de nouvelles mesures de gestion et d'atténuation, et possiblement devoir modifier les avis ou en émettre des nouveaux.



La Procédure de gestion des incidents de confidentialité reprend ces étapes pour guider les actions des impliqués.

PROCESSUS DE TRAITEMENT DES PLAINTES

Une personne concernée peut porter plainte auprès de la SQDC si elle a des raisons de croire qu'il s'est produit, à la SQDC et à l'égard de renseignements personnels qui la concernent :

1. Un incident de confidentialité,
2. Une contravention aux lois applicables, au présent guide ou à un autre engagement de protection des renseignements personnels pris par la SQDC à son égard,
3. Un événement ou une pratique survenue dans le cadre du traitement de ses renseignements personnels détenus par la SQDC et qu'elle estime contraire à ses droits, à ses intérêts légitimes, ou aux bonnes pratiques de protection des renseignements personnels.

Cette plainte doit être adressée par écrit au Responsable de la protection des renseignements personnels, aux coordonnées suivantes :

Société québécoise du cannabis (SQDC)
Responsable de la protection des renseignements personnels
7355, rue Notre-Dame Est, Montréal (QC) H1N 3S7
@ : accesalinformation@sqdc.ca
T : 514-379-5000, poste 6940

Important : toute personne qui a des raisons de croire qu'un incident de confidentialité à la SQDC, que les renseignements la concernent ou non, est fortement encouragée à le signaler immédiatement au responsable, comme s'il s'agissait d'une plainte. Si vous estimez que l'incident justifie une réponse immédiate pour en limiter les impacts, prière d'ajouter la mention « URGENT » dans l'objet de votre courriel, ou de le mentionner au responsable.

Le Responsable de la protection des renseignements personnel traitera la plainte d'une manière similaire au traitement donné aux demandes d'accès et de rectification et, dans la mesure du possible, dans les mêmes délais. La personne plaignante recevra un accusé de réception dans un délai de quelques jours de la réception de la plainte, et pourrait devoir faire la preuve de son identité afin de pouvoir recevoir une réponse concernant ses renseignements personnels. Une fois la validation d'identité complétée, elle recevra une réponse du responsable dans un délai variant de 20 ou 30 jours.

Si l'auteur de la plainte ne s'identifie pas, la plainte sera néanmoins traitée par le responsable. Cependant, l'auteur de la plainte ne sera pas informé des actions prises à l'égard des renseignements personnels faisant l'objet de sa plainte.

ANNEXE 1 : LEXIQUE ET ABBRÉVIATIONS

Actif informationnel – Actif informationnel décrit dans la *Politique de sécurité de l'information*. (Information, savoir, ou document détenu par la SQDC ou pour son compte, incluant les actifs physiques et les systèmes, incluant les logiciels, utilisés pour son traitement, son utilisation, son stockage, sa conservation ou sa communication. Cette définition est applicable sans égard à la nature du support employé et de la technologie employée.)

Actif informationnel critique – Actif informationnel critique défini dans la *Politique de sécurité de l'information*. (Actif informationnel que la direction ou le propriétaire désigne comme étant critique en raison d'une évaluation : de sa valeur pour la SQDC, des risques qu'il présente, des exigences légales, de sa sensibilité, de sa confidentialité, de son exposition à la perte, au vol ou à la diffusion accidentelle, et d'autres considérations fondées sur les bonnes pratiques de gestion des systèmes de management de la sécurité de l'information.)

Anonymisation – Retrait des informations liées à un renseignement personnel, d'une manière qui rend la réidentification raisonnablement impossible.

CAI – la Commission d'accès à l'information du Québec. La CAI est un tribunal administratif et exerce un rôle de supervision et d'enquête en matière de PRP.

Communication de RP – Transmission d'un renseignement personnel à l'extérieur de la SQDC (ex : à un fournisseur, à un tiers)

CPRP – Comité de protection des renseignements personnels.

Cybersécurité – La sécurité des systèmes informatiques et des réseaux de la SQDC. Il s'agit d'un des principaux volets de la sécurité de l'information.

Dépersonnalisation – Retrait des informations nominatives contenues dans un renseignement personnel, mais sans nécessairement rendre impossible la réidentification de la personne concernée.

Document – Un document est constitué d'information délimitée portée par un support. Pour la définition de document, la nature du support n'a pas d'importance (par exemple, un support papier ou sur tout format informatique). De plus, la nature de l'information n'a pas d'importance, étant entendu que l'information soit intelligible d'une manière quelconque. Une banque de données est assimilée à un document, et la création de documents à partir d'une banque de données se fait en utilisant ses éléments structurants pour délimiter et structurer l'information qui y est contenue. Un dossier ou fichier peut être composé d'un ou de plusieurs documents.

EFVP – Évaluation des facteurs relatifs à la vie privée.

Fichier de RP – Fichier contenant tous les renseignements personnels servant à un même usage ou concernant un même sujet ou un même projet.

Loi ou LADOPPRP – Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels, RLRQ, c. A-2.1. Cette loi a été mise à jour en 2021 par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25 (aussi appelée « loi 25 » ou « projet de loi 64 »).

OCDE – Organisation de coopération et de développement économique.

Personne concernée – S'entend de la personne à propos de qui le renseignement personnel est susceptible de dévoiler de l'information. La personne concernée par le renseignement personnel est au centre de la PRP, laquelle répond à plusieurs de ses droits, dont le droit à la vie privée, lequel est protégé par la *Charte des droits et libertés de la personne*.

Il est à noter que les renseignements personnels de plusieurs personnes concernées peuvent être présents dans le même document ou dans la même donnée. Cependant, un renseignement personnel ne concerne qu'une seule personne concernée. Dans l'exemple donné, on dit que le document contient plusieurs renseignements personnels, le document n'étant pas lui-même un renseignement personnel.

Processus – Pour les fins du présent guide, réfère à un processus impliquant des renseignements personnels, et est défini au sens large comme étant un ensemble d'actions posées afin d'atteindre un objectif d'affaire de la SQDC. Ces actions sont appelées « Traitements » de renseignement personnels.

Renseignement personnel sensible – Renseignement personnel qui, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée. (Loi, art. 59). Un renseignement personnel sensible est automatiquement défini comme un actif informationnel critique.

Responsable d'un fichier de PRP – Personne qui, à l'égard d'un fichier de PRP, est désignée pour en être le propriétaire ou, à défaut d'une telle désignation, le plus haut gestionnaire de l'unité administrative qui est est responsable. Le responsable d'un fichier de PRP est défini de la même manière que le propriétaire d'un actif informationnel au sens de la *Politique de sécurité de l'information* et assume, en plus des responsabilités spécifiques à la PRP, les mêmes obligations que tout propriétaire d'actif informationnel en vertu de la *Politique de sécurité de l'information*.

RP – Renseignement personnel.

PRP – Protection des renseignements personnels. La protection des renseignements personnels comprend la sécurité de l'information à l'égard de ces renseignements, mais aussi un certain nombre de responsabilités et d'autres exigences en matière d'accès, d'exactitude, de reddition de comptes et de gestion de la vie privé.

RPRP – Responsable de la protection des renseignements personnels.

Réidentification – Action de retrouver une personne spécifique en utilisant des renseignements dépersonnalisés, par exemple en les croisant avec d'autres renseignements disponibles ou en croisant les renseignements disponibles l'un avec l'autre.

Sécurité de l'information – la sécurité des actifs informationnels de la SQDC. Elle comprend la cybersécurité, ainsi qu'un ensemble de mesures de gouvernance pour assurer la gestion des accès, la conformité des fournisseurs, la gestion des incidents et le partage des responsabilités.

TI – Les technologies de l'information. Désigne en général toutes les technologies électroniques, les ordinateurs, les serveurs, etc.

Traitement – Toute manipulation d'un renseignement personnel, humaine ou automatisée, consistant à le copier, le télécharger, le téléverser, en faire l'utilisation, l'interpréter, le communiquer, le collecter, le détruire, y donner accès, l'anonymiser, le supprimer, etc. En règle générale, le recensement de l'ensemble des traitements d'un renseignement personnel devrait permettre de visualiser l'ensemble du cycle de vie de ce renseignement.

Pour les fins de leur recensement, ces traitements sont regroupés au sein de Processus, dont ils composent les différentes étapes. Un même renseignement peut être utilisé dans différents processus.

Utilisation prévue, usage prévu ou finalité de la collecte – raison pour laquelle on recueille le renseignement personnel, la chose que l'on veut faire avec. Celle-ci diffère d'une simple « utilisation » en ce qu'elle doit être définie avant même de collecter ou de créer le renseignement, notamment à des fins de planification et d'obtention du consentement de la personne concernée.