

RÈGLES ENCADRANT LA GOUVERNANCE DU CENTRE DE SERVICES SCOLAIRE DES PREMIÈRES-SEIGNEURIES À L'ÉGARD DES RENSEIGNEMENTS PERSONNELS

Responsabilité		Adopté le
Direction générale	✓	4 décembre 2024 par le Comité sur l'accès à l'information et la protection des renseignements personnels
Direction du Service des affaires publiques, des communications et du secrétariat général	✓	
Direction des Services éducatifs		Résolution numéro
Direction du Service des ressources financières et du transport scolaire		N/A
Direction du Service des ressources humaines		Entrée en vigueur le
Direction du Service des ressources matérielles		4 décembre 2024
Direction du Service de la transformation numérique et des ressources informationnelles	✓	

Table des matières

1. CADRE JURIDIQUE.....	3
2. BUT ET OBJECTIFS DES RÈGLES	3
3. CHAMP D'APPLICATION	4
4. DÉFINITIONS.....	4
5. RÔLES ET RESPONSABILITÉS	6
5.1. Direction générale	6
5.2. Comité sur l'accès.....	7
5.3. Responsable.....	7
5.4. Direction d'établissements et de service	8
5.5. Employés.....	9
6. COLLECTE, UTILISATION, COMMUNICATION, CONSERVATION ET DESTRUCTIONS DES RENSEIGNEMENTS PERSONNELS.....	9
6.1. Collecte	10
6.2. Utilisation	11
6.3. Accès au renseignements personnels dans l'exercice des fonctions.....	11
6.4. Communication	12
6.5. Conservation et destruction	12
6.6. Projets particuliers nécessitant la réalisation d'une Évaluation des facteurs à la vie privée.....	13
7. MESURES DE PROTECTION PARTICULIÈRES LORS DE SONDAGE	13
7.1. Sondage visé	13
7.2. Nécessité.....	13
7.3. Mesures de protection.....	14
7.4. Approbation et consultation	14
8. ACTIVITÉS DE FORMATION ET DE SENSIBILISATION.....	14
8.1. Activités de formation et de sensibilisation.....	14
9. PROCESSUS DE TRAITEMENT DES PLAINTES	14
9.1. Dépôt d'une plainte et contenu	14
9.2. Traitement de la plainte	15
10. DIFFUSION	15
11. ENTRÉE EN VIGUEUR.....	15
ANNEXE 1 - Directive concernant la communication d'un renseignement personnel sans le consentement de la personne concernée dans certains cas prévus par la loi ..	16
ANNEXE 2 - Formulaire de communication de renseignements personnels en vue de prévenir un acte de violence, dont un suicide.....	19

ANNEXE 3 - Procédure relative à la réalisation d'une Évaluation des facteurs relatifs à la vie privée (EFVP)	20
ANNEXE 4 - Directive relative à la gestion des incidents de confidentialité impliquant des renseignements personnels	32

1. CADRE JURIDIQUE

Les présentes règles encadrant la gouvernance du Centre de services scolaire des Premières-Seigneuries à l'égard des Renseignements personnels (ci-après : « règles ») découlent des articles 52.2 et 63.3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A- 2.1, ci-après « LAI »).

Les présentes règles doivent être lues en concordance avec les orientations, encadrements ou autres outils en vigueur au Centre de services scolaire des Premières-Seigneuries (ci-après : « CSSPS ») concernant la protection des renseignements personnels.

2. BUT ET OBJECTIFS DES RÈGLES

Les présentes règles ont pour but de doter le CSSPS de règles encadrant sa gouvernance à l'égard des renseignements personnels de manière à permettre à tous les employés visés par les règles de connaître et de comprendre les exigences légales ainsi que les principes de protection des renseignements personnels applicables en vertu de la LAI.

Elles ont également pour but d'informer toute personne susceptible de transmettre des renseignements personnels au CSSPS des règles applicables à leur cueillette, utilisation, communication, conservation et destruction.

Les objectifs des règles sont les suivants :

- Déterminer les rôles et responsabilités de tous les employés visés par les présentes règles ;
- Énoncer les obligations et les principes sur lesquels repose la protection des renseignements personnels collectés, utilisés, communiqués, conservés et détruits dans le cadre de l'exercice des fonctions du CSSPS ;
- Déterminer les mesures de protection particulières applicables l'égard des renseignements personnels collectés ou utilisés dans le cadre d'un sondage ;
- Établir un processus de traitement des plaintes relatives à la protection des renseignements personnels au CSSPS ;
- Décrire les activités de formation et de sensibilisation à la protection des renseignements personnels offerts aux employés du CSSPS ;
- Établir un processus de gestion des incidents de confidentialité impliquant des renseignements personnels ;
- Déterminer des règles encadrant la réalisation d'une Évaluation des facteurs relatifs à la vie privée ;
- Établir les conditions et les modalités suivant lesquelles le CSSPS peut communiquer un renseignement personnel, sans le consentement de la personne concernée, en vue de prévenir un acte de violence, dont un suicide.

3. CHAMP D'APPLICATION

Les présentes règles s'appliquent à l'ensemble des employés du CSSPS (établissements et services). Elles s'appliquent également aux membres du conseil d'administration, aux membres des conseils d'établissements et aux membres des différents comités du CSSPS.

4. DÉFINITIONS

Dans les présentes règles, on entend par :

Acte de violence : Un acte appréhendé qui engendre un risque sérieux de mort ou de blessures graves ;

Comité sur l'accès : Comité sur l'accès à l'information et la protection des renseignements personnels du CSSPS composé de la direction générale, du responsable de l'accès aux documents et de la protection des renseignements personnels, du Chef de la sécurité de l'information organisationnelle, d'un gestionnaire des ressources humaines, d'un gestionnaire du secrétariat général et d'un membre de la gestion documentaire ;

Commission : Commission d'accès à l'information du Québec ;

Consentement : Accord, acquiescement, assentiment volontaire d'une personne autorisée à la cueillette, l'utilisation ou la communication de renseignements personnels. Pour être valide, sous réserve d'autres exigences prévues par la loi, ce consentement doit être manifeste, libre, éclairé et donné à des fins spécifiques. Il doit être demandé en des termes clairs. Il ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il est demandé ;

Critère de nécessité : Applicable notamment dans le cadre de la collecte d'un Renseignement personnel ou dans le contexte où un employé souhaite avoir accès à un tel renseignement dans l'exercice de ses fonctions, le critère de nécessité va au-delà de la simple utilité. De façon générale, le critère de nécessité est démontré si la collecte ou l'utilisation d'un renseignement personnel répond à toutes ces conditions :

- Son objectif est légitime, important et réel ;
- L'atteinte à la vie privée de la personne est proportionnelle à l'objectif poursuivi ;
- L'atteinte au droit à la vie privée est minimisée, de sorte qu'il n'existe pas d'autres moyens d'atteindre les mêmes objectifs d'une façon qui porte moins atteinte à la vie privée ;
- La collecte, l'utilisation ou la communication du renseignement personnel est nettement plus utile au CSSPS que préjudiciable à la personne concernée.

Droit d'accès et de rectification : Conformément à la LAI et sauf exception, toute personne concernée par des renseignements personnels détenus par le CSSPS dispose notamment des droits suivants lorsqu'elle en fait la demande :

- Le droit de recevoir communication d'un tel renseignement en lui permettant d'en prendre connaissance sur place pendant les heures habituelles de travail ou à distance et d'en obtenir une copie ;
- Le droit de demander la rectification d'un fichier qui contient un renseignement personnel qui la concerne si celui-ci est inexact, incomplet ou équivoque ou si sa collecte, sa communication ou sa conservation n'est pas autorisée par la LAI.

Employés : Personnes membres du personnel du CSSPS, incluant les stagiaires et les bénévoles ;

Évaluation des facteurs relatifs à la vie privée (EFVP) : Démarche préventive d'évaluation qui consiste à considérer tous les facteurs d'un projet qui entraîneraient des conséquences positives et négatives sur le respect de la vie privée des personnes concernées afin d'identifier des mesures propres à mieux protéger leurs renseignements personnels et à respecter davantage leur vie privée ;

Incident de confidentialité : Il peut s'agir selon le cas :

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 ;
5. Toute autre atteinte à la protection d'un tel renseignement.

Personne concernée : Personne physique concernée par le renseignement personnel collecté, utilisé ou communiqué qui est apte à consentir, ou lorsqu'applicable, son représentant légal ou le titulaire de l'autorité parentale. Sans limiter la généralité de ce qui précède, et sauf exception, le titulaire de l'autorité parentale consent pour un mineur de moins de 14 ans. Le mineur de 14 ans et plus ou le titulaire l'autorité parentale consent pour le mineur de 14 ans et plus ;

Plus haute autorité : Directeur général ou directrice générale ;

Renseignement personnel : Renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier. Le terme « renseignement personnel » inclut en tout temps les renseignements personnels anonymisés, dépersonnalisés et sensibles. Les renseignements personnels peuvent être classés par regroupements, dont voici des exemples :

- Renseignements d'identification : nom, numéro de fiche, code permanent, adresse, numéro de permis de conduire, date de naissance, numéro d'assurance sociale, numéro d'assurance maladie, numéro de passeport, etc. ;
- Renseignements de nature financière : numéro de carte de crédit, numéro de carte de débit, renseignement bancaire (hypothèque, numéro de compte, placement, numéro d'identification personnel (NIP)), contrat de travail, salaire, etc. ;

- Renseignements scolaires/académiques : résultats, niveaux de difficultés, plan d'intervention, difficulté de comportement, etc. ;
- Renseignements de nature médicale ou génétique : diagnostic médical, historique médical, arrêt de travail, etc. ;
- Renseignements démographiques : orientation sexuelle, identité de genre, religion, origine ethnique, niveau de scolarité, état matrimonial, etc.

Renseignement personnel anonymisé : Renseignement personnel dont il est en tout temps raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement la personne concernée ;

Renseignement personnel dépersonnalisé : Renseignement personnel qui ne permet plus d'identifier directement la personne concernée ;

Renseignement personnel sensible : Renseignement personnel qui, par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée ;

Requérant : Personne qui transmet une demande d'accès aux documents, une demande de communication de renseignements personnels ou de rectification en vertu de la LAI ;

Responsable : Personne désignée comme responsable de l'accès aux documents et de la protection des renseignements personnels ;

Sondage : Méthode statistique de collecte de données visant à interroger une partie d'une population en utilisant des concepts, des méthodes ou des procédures généralement reconnus dans le domaine des statistiques. Aux fins des présentes règles, les sondages incluent aussi les questionnaires ou formulaires transmis à un ensemble de personnes ainsi que les entrevues individuelles ou en groupe ;

Traitement des renseignements personnels : désigne l'ensemble des étapes du cycle de vie d'un renseignement personnel (la collecte, l'utilisation, la conservation, la communication et la destruction) ou chacune d'elle distinctement.

5. RÔLES ET RESPONSABILITÉS

5.1. Direction générale

- 5.1.1. Déléguer par écrit les fonctions de Responsable¹ ;
- 5.1.2. Veiller à faciliter l'exercice des fonctions du Responsable et à préserver son autonomie ;
- 5.1.3. Aviser dès que possible la Commission par écrit du titre, des coordonnées et de la date d'entrée en fonction de la personne qui

¹ Art. 8 de la LAI;

- exerce la fonction de Responsable²;
- 5.1.4. Transmettre avec diligence au Responsable toute demande d'accès aux documents, demande de communication ou de rectification qui lui est adressée par écrit³;
 - 5.1.5. S'assurer de la mise en place et du bon fonctionnement du Comité sur l'accès⁴ ;
 - 5.1.6. Adopter toute directive ou encadrement qui relève de sa compétence et qui est requis pour assurer le respect de la LAI, et voir à leur mise à jour.

5.2. Comité sur l'accès

- 5.2.1. Soutenir le CSSPS dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la LAI⁵ ;
- 5.2.2. Approuver les présentes règles et voir à leurs mises à jour⁶ ;
- 5.2.3. Être consulté au début de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels⁷ ;
- 5.2.4. Suggérer, à toute étape d'un projet visé à l'article 5.2.3., des mesures de protection des renseignements personnels applicables à ce projet⁸ ;
- 5.2.5. Exercer toute autre fonction en lien avec la protection de renseignements personnels à la demande de la direction générale.

5.3. Responsable

- 5.3.1. Recevoir les demandes d'accès aux documents, de communication ou de rectification de renseignements personnels et s'assurer qu'elles sont traitées selon les dispositions de la LAI⁹ ;
- 5.3.2. Participer selon les besoins à l'Évaluation des facteurs relatifs à la vie privée pour les projets du CSSPS qui le requièrent ;
- 5.3.3. Exercer les responsabilités qui lui sont dévolues lorsque survient un incident de confidentialité impliquant des renseignements personnels ;
- 5.3.4. S'assurer de la mise en place, de la tenue et de l'inscription des données requises aux différents registres prévues dans la LAI¹⁰ ;
- 5.3.5. Établir et tenir à jour, en collaboration avec les établissements et les services, l'inventaire des fichiers de renseignements personnels, incluant

² Art. 8 de la LAI;

³ Arts. 43, 94 de la LAI ;

⁴ Art. 8.1 de la LAI ;

⁵ Art. 8.1 de la LAI;

⁶ Art. 63.3 de la LAI;

⁷ Art. 63.5 de la LAI;

⁸ Art. 63.6 de la LAI;

⁹ Arts. 45 à 52, 97 à 102 de la LAI ;

¹⁰ Arts. 41.3, 60, 60.1, 63.8, 63.11, 64, 65.1, 67.3, 91 de la LAI ;

notamment, les catégories d'employés qui ont accès à chaque fichier dans l'exercice de leurs fonctions¹¹ ;

- 5.3.6. Participer à l'établissement et la mise à jour du plan de classification des documents et du calendrier de conservation¹²;
- 5.3.7. Traiter les plaintes relatives à la protection des renseignements personnels en conformité aux présentes règles ;
- 5.3.8. Veiller, en collaboration avec les directions d'établissements et de services, à la sensibilisation et à la formation des employés en matière de protection des renseignements personnels en conformité aux présentes règles ;
- 5.3.9. Veiller au développement, à la mise en place et à la diffusion d'outils, de documents modèles, de documents de référence ou autres pour favoriser le respect de la LAI par le CSSPS et tous les employés ;
- 5.3.10. Assurer un rôle de soutien et de conseil relativement à toute question touchant l'accès aux documents ou à la protection des renseignements personnels ;
- 5.3.11. Agir à titre de représentant auprès des autres organismes publics et de la Commission pour toutes les questions relatives à l'accès aux documents et à la protection des renseignements personnels ;
- 5.3.12. Exercer toute autre fonction prévue à la LAI ou à la demande de la direction générale.

5.4. Direction d'établissement et de service

- 5.4.1. Veiller au respect des présentes règles par les employés sous leur responsabilité ;
- 5.4.2. Identifier, pour leur établissement ou service, les renseignements personnels détenus et participer à la mise à jour de l'inventaire de ces renseignements ;
- 5.4.3. Identifier les catégories d'employés sous leurs responsabilités qui ont accès aux renseignements personnels, ainsi que les catégories de renseignements personnels qui leur sont accessibles ;
- 5.4.4. Mettre en place dans leur établissement ou service des mesures de protection des renseignements personnels qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité, de leur utilisation, de leur quantité, de leur répartition et de leur support, voir à leur diffusion et à leur application par les employés sous leur responsabilité ;
- 5.4.5. Sous réserve du calendrier de conservation du CSSPS ou de toute loi applicable, mettre en place dans leur établissement ou service une procédure de destruction sécuritaire d'un renseignement personnel lorsque les fins pour lesquelles il a été collecté ou utilisé sont accomplies¹³ ;

¹¹ Art. 76 de la LAI ;

¹² Art. 16 de la LAI ;

¹³ Art. 73 de la LAI ;

- 5.4.6. Exercer les responsabilités qui leur sont dévolues lorsque survient un incident de confidentialité impliquant des renseignements personnels ;
- 5.4.7. En collaboration avec le Responsable, veiller à ce que les formations et les activités de sensibilisation prévues aux présentes règles soient offertes aux employés sous leur responsabilité et s'assurer que ces dernières y participent ;
- 5.4.8. Collaborer avec le Responsable au développement, à la mise en place et à la diffusion d'outils, de modèles de documents, de documents de référence ou autres pour favoriser le respect de la LAI dans leur établissement ou service ;
- 5.4.9. Communiquer au besoin avec le Responsable pour toute question relative aux demandes d'accès à des documents ou à la protection des renseignements personnels dans leur établissement ou service.

5.5. Employés

- 5.5.1. Prendre connaissance et respecter les présentes règles ;
- 5.5.2. Participer aux formations et aux activités de sensibilisation prévues dans les présentes règles ;
- 5.5.3. Utiliser les outils, les modèles de documents, les documents de référence ou tout autre document mis à leur disposition pour favoriser le respect des présentes règles ;
- 5.5.4. Collaborer, sur demande, avec le Responsable lors du traitement d'une demande d'accès à des documents, de communication ou de rectification de renseignement personnel ou de toute autre démarche de même nature au regard de la LAI ;
- 5.5.5. Collaborer, sur demande, avec le Responsable lors du traitement d'une plainte visée par les présentes règles ;
- 5.5.6. Informer le Responsable de tout incident de confidentialité concernant des renseignements personnels et collaborer avec celui-ci dans l'analyse de la situation ;
- 5.5.7. Communiquer, au besoin, avec leur supérieur relativement aux présentes règles pour obtenir des précisions, des conseils ou l'informer d'une problématique dans l'application des présentes règles ou d'un cas particulier en matière de protection des renseignements personnels.

6. COLLECTE, UTILISATION, COMMUNICATION, CONSERVATION ET DESTRUCTIONS DES RENSEIGNEMENTS PERSONNELS

À chaque étape du cycle de vie des renseignements personnels, des mesures propres à assurer leur protection doivent être mises en place. Ainsi, le traitement de tels renseignements doit être réalisé dans le respect des exigences et principes décrits ci-dessous.

6.1. Collecte

- 6.1.1. Un employé doit collecter uniquement les renseignements personnels nécessaires à l'exercice de ses fonctions¹⁴ ;
- 6.1.2. Une collecte effectuée à un autre titre sera permise dans les cas prévus par la LAI et doit être préalablement autorisée par la direction d'établissement ou de service ;
- 6.1.3. Généralement, la collecte est effectuée auprès de la personne concernée, ou son représentant, et les informations suivantes doivent être transmises¹⁵ :
 - 6.1.3.1. Le nom de l'organisme public au nom de qui la collecte est faite ;
 - 6.1.3.2. Les fins auxquelles ces renseignements sont collectés ;
 - 6.1.3.3. Les moyens par lesquels les renseignements sont collectés ;
 - 6.1.3.4. Le caractère obligatoire ou facultatif de la demande ;
 - 6.1.3.5. Les conséquences d'un refus de répondre à la demande ou, le cas échéant, d'un retrait de son consentement à la communication ou à l'utilisation des renseignements collectés suivant une demande facultative ;
 - 6.1.3.6. Les droits d'accès et de rectification prévus par la LAI ;
 - 6.1.3.7. S'il y a lieu, le nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer ces renseignements ;
 - 6.1.3.8. S'il y a lieu, informer la personne concernée de la possibilité que ces renseignements soient communiqués à l'extérieur du Québec ;
 - 6.1.3.9. Le cas échéant, toutes autres informations requises par la LAI et qui sont applicables à la situation en cause.
- 6.1.4. Si la collecte est effectuée auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci, elle doit, au préalable, être informée :
 - 6.1.4.1. Du recours à une telle technologie ;
 - 6.1.4.2. Des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage¹⁶.
- 6.1.5. Toute collecte de renseignements personnels concernant un mineur de moins de 14 ans ne peut être effectuée auprès de celui-ci sans le consentement du titulaire de l'autorité parentale ou du tuteur, sauf lorsque cette collecte est manifestement au bénéfice de ce mineur¹⁷ ;
- 6.1.6. Toute collecte de renseignements personnels en offrant au public un produit ou un service technologique disposant de paramètres de confidentialité doit être effectuée de manière que par défaut, ces paramètres assurent le plus

¹⁴ Art. 64 de la LAI ;

¹⁵ Art. 65 de la LAI ;

¹⁶ Art. 65.0.1 de la LAI ;

¹⁷ Art. 64.1 de la LAI ;

haut niveau de confidentialité, sans aucune intervention de la personne concernée. Les paramètres de confidentialité d'un témoin ne sont toutefois pas visés¹⁸.

6.2. Utilisation

- 6.2.1. Un employé peut utiliser un renseignement personnel pour les fins pour lesquelles il a été collecté¹⁹ ;
- 6.2.2. Une utilisation à une autre fin sera permise avec le consentement de la personne concernée²⁰ ;
- 6.2.3. Lorsqu'il s'agit d'un renseignement personnel sensible, le consentement à utiliser ce renseignement à une autre fin doit être obtenu par écrit²¹ ;
- 6.2.4. Une utilisation à une autre fin peut être permise, sans le consentement de la personne concernée, uniquement dans les situations prévues à la Loi²²;
- 6.2.5. Lorsqu'un renseignement personnel est utilisé afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de celui-ci, le membre du personnel responsable de la décision doit aviser la personne concernée au plus tard au moment où il l'informe de cette décision. Ce membre du personnel doit aussi, à la demande de la personne concernée, l'informer :
 - 6.2.5.1. Des renseignements personnels utilisés pour rendre la décision ;
 - 6.2.5.2. Des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision ;
 - 6.2.5.3. De son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision ;
 - 6.2.5.4. De son droit de présenter ses observations à un membre du personnel en mesure de réviser la décision²³.

6.3. Accès aux renseignements personnels dans l'exercice des fonctions

- 6.3.1. Un employé a accès, sans le consentement de la personne concernée, à un renseignement personnel lorsqu'elle a qualité pour le recevoir et qu'il est nécessaire à l'exercice de ses fonctions²⁴ ;
- 6.3.2. Les accès aux renseignements personnels consignés dans des fichiers ou des bases de données doivent faire l'objet d'une révision périodique.

¹⁸ Art. 63.7 de la LAI

¹⁹ Art. 65.1 de la LAI ;

²⁰ Art. 65.1 de la LAI ;

²¹ Art. 65.1 de la LAI ;

²² Art. 65.1 de la LAI ;

²³ Art. 65.2 de la LAI ;

²⁴ Art. 62 de la LAI ;

6.4. Communication

- 6.4.1. Un employé ne peut pas transmettre un renseignement personnel à une personne qui ne détient pas les autorisations requises pour le recevoir sans le consentement de la personne concernée²⁵ ;
- 6.4.2. Dans les mesures du possible, le consentement obtenu devrait être par écrit ;
- 6.4.3. Toutefois, lorsqu'il s'agit d'un renseignement personnel sensible, le consentement à communiquer ce renseignement doit être obtenu par écrit²⁶ ;
- 6.4.4. Un employé peut communiquer des renseignements personnels sans le consentement de la personne concernée dans les cas prévus par la loi²⁷ en tenant compte notamment de l'annexe 1 des présentes règles ;
- 6.4.5. La communication d'un renseignement personnel sans le consentement de la personne concernée dans les cas prévus par la loi doit être acheminée au Responsable.

6.5. Conservation et destruction

- 6.5.1. Un employé doit connaître et appliquer les mesures de sécurité déterminées par le CSSPS pour chaque renseignement personnel auquel il a accès²⁸ ;
- 6.5.2. À défaut, un employé doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels auxquels il a accès, et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support²⁹ ;
- 6.5.3. Lorsqu'un employé est informé ou qu'il a des motifs raisonnables de croire que les renseignements personnels qu'il conserve ne sont plus à jour, exacts et complets pour servir aux fins pour lesquelles ils sont collectés ou utilisés, il en avise rapidement sa direction d'établissement ou de service afin que les actions appropriées soient prises³⁰ ;
- 6.5.4. Un employé doit connaître et appliquer le calendrier de conservation et le plan de classification du CSSPS relevant du secteur de la gestion documentaire³¹ ;
- 6.5.5. À défaut, un employé doit prendre les mesures pour détruire de manière sécuritaire un renseignement personnel qu'il conserve lorsque les fins pour lesquelles il a été collecté ou utilisé sont accomplies. De telles mesures doivent être raisonnables en fonction notamment de la sensibilité, de la quantité et du support du renseignement personnel concerné³² ;
- 6.5.6. L'utilisation d'un renseignement personnel anonymisé est permise à des fins d'intérêt public, lorsque les fins pour lesquelles il a été collecté ou utilisé

²⁵ Art. 59 de la LAI ;

²⁶ Art. 59 de la LAI ;

²⁷ Art. 59 de la LAI ;

²⁸ Art. 63.1 de la LAI ;

²⁹ Art. 63.1 de la LAI ;

³⁰ Art. 72 de la LAI ;

³¹ Art. 73 de la LAI ;

³² Art. 73 de la LAI ;

sont accomplies³³.

6.6. Projets particuliers nécessitant la réalisation d'une Évaluation des facteurs à la vie privée

- 6.6.1. Un employé responsable d'un projet visé aux articles 63.5, 64, 65.5, 67.3.1, 68 et 70.1 de la LAI doit s'assurer qu'une Évaluation des facteurs relatifs à la vie privée est effectuée sous la coordination du Responsable et que toutes les conditions prévues dans la LAI relativement à ce projet sont respectées.
- 6.6.2. Un employé responsable d'un projet visé aux articles 64, 67.2, 67.2.1, 68 et 70.1 de la LAI doit s'assurer qu'une entente ou un contrat écrit a été conclu sous la direction du Responsable et est en vigueur avant de procéder à toute collecte, utilisation ou communication de renseignement personnel.
- 6.6.3. La réalisation d'une Évaluation des facteurs relatifs à la vie privée est encadrée par la procédure présentée en annexe 3.

7. MESURES DE PROTECTION PARTICULIÈRES LORS DE SONDAGE

7.1. Sondage visé

- 7.1.1. Seul un sondage demandant l'utilisation ou la collecte de renseignements personnels est visé par les présentes règles ;
- 7.1.2. Le cas échéant, tous les types de sondage (ex. : d'opinion, de satisfaction, de mesure de la qualité des services, études de marché) sont visés, quelle qu'en soit la forme (ex. : entrevue individuelle ou de groupe, sondage sous forme de questionnaire, sondage automatisé).

7.2. Nécessité

- 7.2.1. Un employé doit, avant de débiter un sondage, évaluer la nécessité de recourir au sondage dans le cadre de la mission du CSSPS ;
- 7.2.2. Ce faisant, un employé doit :
 - 7.2.2.1. Établir le but et les objectifs du sondage ;
 - 7.2.2.2. Vérifier la possibilité de procéder au sondage sans utiliser ou collecter des renseignements personnels ;
 - 7.2.2.3. Procéder à une évaluation de l'aspect éthique du sondage, compte tenu, notamment, de la nature du sondage, des personnes visées, de la sensibilité des renseignements personnels collectés et de la finalité de l'utilisation de ceux-ci, avec, au besoin, le soutien d'une personne détenant des connaissances en éthique.

³³ Art. 73 de la LAI ;

7.3. Mesures de protection

7.3.1. Un employé doit également, avant de débiter un sondage :

7.3.1.1. Identifier les renseignements personnels à utiliser et obtenir les autorisations nécessaires ;

7.3.1.2. S'assurer de limiter la quantité de renseignements personnels utilisés ou collectés et éviter la collecte de renseignements personnels sensibles ;

7.3.1.3. Prévoir qui aura accès aux renseignements personnels utilisés ou collectés dans le cadre du sondage, les mesures de sécurité qui seront applicables pour en assurer la protection, la durée de leur conservation et de leur destruction, le tout en fonction des exigences légales et des principes établis dans les présentes règles ;

7.3.1.4. Au besoin, procéder à une Évaluation des facteurs relatifs à la vie privée.

7.4. Approbation et consultation

7.4.1. Avant de réaliser le sondage, un employé doit obtenir l'accord de la direction d'établissement ou du service concerné ;

7.4.2. Le Responsable ou le Comité sur l'accès peut être consulté.

8. ACTIVITÉS DE FORMATION ET DE SENSIBILISATION

8.1. Activités de formation et de sensibilisation

8.1.1. Lors de l'entrée en fonction d'un employé et au besoin par la suite, le CSSPS s'assure que lui soient communiquées les présentes règles ;

8.1.2. Annuellement, la direction d'établissement ou de service, en collaboration avec le Responsable, veille à ce que tout employé sous leur responsabilité soit sensibilisé relativement aux exigences et principes entourant la protection des renseignements personnels ;

8.1.3. Les activités de sensibilisation sont effectuées de différentes manières : capsules de formation, séances de discussion, courriel d'information, etc.

9. PROCESSUS DE TRAITEMENT DES PLAINTES

9.1. Dépôt d'une plainte et contenu

9.1.1. Quiconque peut porter plainte auprès du Responsable relativement au non-respect, par le CSSPS de ses obligations en matière de protection des renseignements personnels ;

9.1.2. Une telle plainte sera transmise préférablement par courriel à l'adresse

suivante : secgen@cssps.gouv.qc.ca ;

9.1.3. La plainte doit comporter une description de l'évènement ayant conduit à la plainte, incluant, la période concernée, les renseignements personnels impliqués et la nature du redressement recherché ;

9.1.4. Dans le cas où la plainte implique la conduite du Responsable, elle sera adressée et traitée par la direction générale.

9.2. Traitement de la plainte

9.2.1. Le Responsable accuse réception de la plainte dans un délai de 48 heures de la réception de celle-ci ;

9.2.2. Le Responsable peut rejeter sommairement toute plainte frivole, vexatoire ou de mauvaise foi. Il doit alors en informer la personne ayant déposé la plainte ;

9.2.3. Le Responsable peut refuser de traiter une plainte si l'évènement a fait l'objet d'un recours en justice, à l'inclusion de toute demande devant la Commission ;

9.2.4. Le Responsable analyse la plainte avec diligence et transmet sa conclusion à la personne ayant déposé la plainte dans les 30 jours de la réception de celle-ci dans la mesure du possible ;

9.2.5. Le cas échéant, le Responsable s'assure de la mise en place des correctifs appropriés.

10. DIFFUSION

10.1. Le Comité sur l'accès s'assure de la diffusion des présentes règles auprès des différents services et établissements.

11. ENTRÉE EN VIGUEUR

11.1. Les présentes règles sont approuvées par le Comité sur l'accès et entrent en vigueur le 4 décembre 2024.

Directive concernant la communication d'un renseignement personnel sans le consentement de la personne concernée dans certains cas prévus par la loi

1. Communication de renseignements personnels dans le cadre de l'exécution d'un contrat de service ou d'entreprise

1.1. Conformément à l'article 67.2 LAI, un employé peut communiquer un renseignement personnel sans le consentement de la personne concernée à toute personne ou à tout organisme, si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de services ou d'entreprise. Pour ce faire, l'employé doit :

- a. S'assurer de la nécessité de communiquer un tel renseignement personnel dans le cadre du contrat ;
- b. Confier le mandat ou le contrat par écrit ;
- c. Inclure des exigences concernant la protection des renseignements personnels dans les documents d'appel d'offres ou dans le contrat écrit (ex. : obligation d'héberger les renseignements personnels au Québec, l'obligation de détruire les renseignements une fois les fins pour lesquelles ils ont été collectés ou transmis sont accomplies, transmission des politiques de confidentialité du fournisseur, etc.) ;
- d. Obtenir des engagements de confidentialité des employés du fournisseur qui pourraient avoir accès à des renseignements personnels ;
- e. Aviser le Responsable concernant toute violation ou tentative de violation d'une obligation relative à la confidentialité ;
- f. Les points c) d) et e) ne s'appliquent pas lorsque le mandataire ou l'exécutant du contrat est un autre organisme public ou un membre d'un ordre professionnel.

2. Communication de renseignements personnels exigés par les services de police ou requis par assignation, citation à comparaître, mandat ou ordonnance d'une personne ayant le pouvoir de contraindre à leur communication

2.1. Conformément à l'article 59 de la LAI, un employé peut communiquer des renseignements personnels sans le consentement de la personne concernée dans

les cas prévus par la loi ou lorsqu'il y est contraint par assignation, citation à comparaître, mandat ou ordonnance. Pour ce faire, un employé doit :

- Vérifier que l'organisme agit en vertu d'un pouvoir prévu à la LAI permettant de contraindre à la communication de tels renseignements. Le cas échéant, le Responsable peut être consulté au préalable ;
- Il doit obtenir une demande écrite et consigner l'ensemble de la documentation transmise.

3. Conditions et modalités suivant lesquelles le CSSPS peut communiquer un renseignement personnel en vue de prévenir un acte de violence, dont un suicide

3.1. Conformément aux articles 59, 59.1, 60 et 60.1 de la LAI, un employé peut communiquer un renseignement personnel sans le consentement de la personne concernée lorsqu'il existe un motif raisonnable de croire qu'un acte de violence menace une personne ou un groupe de personnes identifiables et que la nature de la menace inspire un sentiment d'urgence.

3.2. Conditions

3.2.1. Pour justifier la communication d'un renseignement personnel sans le consentement de la personne concernée, les conditions suivantes doivent être réunies :

- L'existence d'un motif raisonnable de croire qu'il existe un danger menaçant une personne ou un groupe de personnes. Le danger n'a pas à être certain, mais il faut que des circonstances ou des faits concrets permettent à une personne raisonnable, placée dans la même situation, de conclure à un danger d'acte de violence ;
- La personne ou le groupe de personnes menacées doit être identifiable ;
- Le danger auquel la personne ou le groupe de personnes est exposé doit être imminent et immédiat.

3.3. Contenu de la communication

3.3.1. Seuls les renseignements personnels nécessaires aux fins poursuivies par la communication, en l'occurrence la prévention d'un acte de violence, peuvent être divulgués ;

3.3.2. Ces renseignements personnels peuvent être, notamment : l'identité et les coordonnées de la personne en danger et de celle qui a proféré les menaces, ainsi que la nature de la menace et les circonstances dans lesquelles elles ont été proférées.

3.4. Formalités à respecter

- 3.4.1. Lorsque toutes les conditions ci-haut décrites sont réunies, l'employé peut alors communiquer les renseignements personnels à la ou aux personnes exposées à ce danger, à leur représentant ou à toute personne susceptible de leur porter secours ;
- 3.4.2. Le représentant de ces personnes peut être un parent ou, s'il s'agit d'un groupe de personnes, celle qui agit à titre de responsable ;
- 3.4.3. Les personnes susceptibles de leur porter secours peuvent être, notamment : un policier, un centre de prévention du suicide, un organisme d'aide et de soutien aux victimes d'actes de violence, un CLSC, un professionnel de la santé ou un directeur de la protection de la jeunesse ;
- 3.4.4. À défaut de s'être assuré que les renseignements personnels visés sont nécessaires pour les fins décrites au présent article, l'employé ne doit pas communiquer le renseignement personnel ;
- 3.4.5. L'employé doit, dans la mesure où les circonstances le permettent, obtenir l'autorisation de son supérieur immédiat avant de communiquer un renseignement personnel ;
- 3.4.6. Advenant qu'aucune autorisation ne puisse être obtenue promptement et qu'une décision doive être prise considérant l'urgence de la situation, l'employé doit agir selon ce qu'il juge le plus approprié compte tenu des circonstances ;
- 3.4.7. À la suite de la communication de tout renseignement personnel en vertu du présent article, l'employé qui effectue la communication doit remplir et transmettre au Responsable, dans les meilleurs délais, le formulaire joint en annexe 2 pour que ladite communication soit consignée au registre tenu à cette fin.

3.5. Consultation du responsable

- 3.5.1. Le Responsable peut être consulté pour toute communication d'un renseignement personnel sans le consentement de la personne concernée dans les cas prévus à la loi.

Formulaire de communication de renseignements personnels en vue de prévenir un acte de violence, dont un suicide

(Article 59.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels)

Conformément aux modalités prévues aux présentes règles, un employé peut communiquer un renseignement personnel sans le consentement de la personne concernée lorsqu'il existe un motif raisonnable de croire qu'un acte de violence menace une personne ou un groupe de personnes et que la nature de la menace inspire un sentiment d'urgence. Lorsque les renseignements personnels ont été communiqués, l'employé concerné doit remplir et transmettre au Responsable de la protection des renseignements personnels, le présent formulaire dans les meilleurs délais.

Date ou l'employé a pris connaissance du danger menaçant une personne ou un groupe de personnes	
Date de la communication des renseignements	
Nom de la personne qui a communiqué les renseignements	
Nom de la personne consultée (le cas échéant)	

Description du danger et des circonstances de l'événement

Nature des renseignements personnels communiqués

Nom, titre et coordonnées des personnes à qui les renseignements ont été communiqués	
Date de transmission du présent formulaire au Responsable de la protection des renseignements personnels. secgen@cssps.gouv.qc.ca	

Procédure relative à la réalisation d'une Évaluation des facteurs relatifs à la vie privée (EFVP)

Étapes à suivre	
<p>1- Déterminer si une EFVP est requise</p>	<p>Il n'est pas obligatoire de mener rétroactivement une EFVP prévue par la Loi 25, c'est-à-dire si le projet était déjà finalisé à la date d'entrée en vigueur.</p> <p>Cependant, il faut réaliser une EFVP :</p> <ul style="list-style-type: none"> • Si on modifie ce projet (p. ex. amendement à l'entente, refonte du système, etc.) ; • Si le projet implique des communications de renseignements personnels à l'extérieur du Québec faites après le 22 septembre 2023.
<p>2- Présenter les grandes lignes du projet</p>	<p>L'objectif est de documenter les informations importantes pour permettre d'évaluer les risques et les moyens d'éliminer ou de réduire ces risques.</p> <p>Par exemple :</p> <ul style="list-style-type: none"> • En quoi consiste le projet ? • Quel était le contexte quand l'idée de ce projet est apparue ? • Quelle est/était la situation au moment où il a débuté ? • Quel est l'échéancier de sa mise en œuvre ?

<p>3- Expliquer les objectifs qui motivent le projet</p>	<p>Ces objectifs peuvent expliquer pourquoi vous devez mettre en place de nouvelles mesures ou pratiques impliquant la gestion des renseignements personnels.</p> <p>Un objectif doit être légitime et se rapporter à des préoccupations réelles et sérieuses.</p> <p>Évaluer la proportionnalité tout au long du processus d'EFVP et de la mise en œuvre de ce projet :</p> <ul style="list-style-type: none"> • Il existe un lien rationnel entre les objectifs et le projet, c'est-à-dire qu'il s'agit d'un moyen efficace d'atteindre l'objectif. Cette efficacité doit être basée sur des données concrètes et probantes ; • L'atteinte à la vie privée est minimale, ou il n'y a pas d'autres solutions efficaces moins intrusives ; • Les avantages concrets surpassent les conséquences ou les préjudices pour les personnes concernées. 						
<p>4- Définir les rôles et les responsabilités</p>	<p>C'est l'organisation détentrice des renseignements personnels qui a la responsabilité de réaliser l'EFVP.</p> <p>L'organisme public doit consulter, dès le début du projet, son comité sur l'accès à l'information et la protection des renseignements personnels. Certaines autres catégories de personnes peuvent aussi être consultées en fonction de la portée du projet (ex. : personne devant prendre position sur la gestion des risques à la fin de la démarche).</p>						
<p>5- Inventorier et cartographier les renseignements personnels</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #4F81BD; color: white;"> <th style="text-align: left; padding: 5px;">Questions</th> <th style="text-align: left; padding: 5px;">Sous-questions</th> </tr> </thead> <tbody> <tr> <td style="background-color: #4F81BD; color: white; vertical-align: top; padding: 5px;">Quoi ?</td> <td style="padding: 5px;"> <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 (ex. : sont-ils sensibles) ? </td> </tr> <tr> <td style="background-color: #4F81BD; color: white; vertical-align: top; padding: 5px;">Pourquoi ?</td> <td style="padding: 5px;"> <ul style="list-style-type: none"> ✓ Pourquoi souhaitez-vous recueillir, utiliser, communiquer ou conserver des renseignements personnels ? ✓ Quelle est la finalité de l'utilisation de ces renseignements dans le cadre de votre projet ? ✓ En quoi l'accès à ces renseignements est-il nécessaire à l'exercice des fonctions des personnes qui y auront accès ? </td> </tr> </tbody> </table>	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 (ex. : sont-ils sensibles) ? 	Pourquoi ?	<ul style="list-style-type: none"> ✓ Pourquoi souhaitez-vous recueillir, utiliser, communiquer ou conserver des renseignements personnels ? ✓ Quelle est la finalité de l'utilisation de ces renseignements dans le cadre de votre projet ? ✓ En quoi l'accès à ces renseignements est-il nécessaire à l'exercice des fonctions des personnes qui y auront accès ?
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 (ex. : sont-ils sensibles) ? 						
Pourquoi ?	<ul style="list-style-type: none"> ✓ Pourquoi souhaitez-vous recueillir, utiliser, communiquer ou conserver des renseignements personnels ? ✓ Quelle est la finalité de l'utilisation de ces renseignements dans le cadre de votre projet ? ✓ En quoi l'accès à ces renseignements est-il nécessaire à l'exercice des fonctions des personnes qui y auront accès ? 						

Combien ?	<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) ? ✓ Quel est le volume ou l'étendue des renseignements personnels concernés ? ✓ Quelle est la durée envisagée du projet ? ✓ Quelle est l'extension géographique projetée ?
Qui ?	<ul style="list-style-type: none"> ✓ Quelles catégories de personnes auront accès à ces renseignements 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 ?
<p>Ne recueillir, utiliser ou communiquer que les renseignements personnels nécessaires à la réalisation du projet.</p> <p>Inclure tous les renseignements personnels créés ou inférés sur les personnes (ex. : note d'évaluation, note dans un dossier, etc.). Il est important de tenir à jour l'inventaire des renseignements personnels (évolutif).</p> <p>Identifiez les points où l'organisation entre en interaction avec les renseignements personnels comme :</p> <ul style="list-style-type: none"> • Des personnes, des ensembles de personnes ou des partenaires et des tiers qui accèdent aux renseignements personnels (employés, clients, sous-traitants, firmes de consultation, chercheurs externes, équipes d'entretien de bâtiments ou de systèmes informatiques, fournisseurs de 	

	<p>télécommunication, etc.) ;</p> <ul style="list-style-type: none"> • Des moyens utilisés pour collecter des renseignements personnels (formulaires d'abonnement, boîtes de courriels, messageries téléphoniques, plateformes collaboratives, sondages, questionnaires, etc.) ; • Des moyens utilisés pour communiquer des renseignements personnels (prestations électroniques de services, échanges par courriel, service à la clientèle, sites Web, interfaces d'échange informatisées [API] ou liens électroniques sécurisés, etc.) ; • Des moyens utilisés pour traiter et conserver des renseignements personnels (systèmes informatiques, services infonuagiques, copies de sauvegarde, outils de télécommunication, salles et classeurs d'entreposage des dossiers papier, etc.) ; • Des moyens utilisés pour détruire ou anonymiser des renseignements personnels.
<p>6- Identifier les particularités de chaque phase du projet</p>	<p>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 :</p> <ul style="list-style-type: none"> • Phase de développement : le projet prend forme, des solutions sont élaborées pour résoudre les problèmes qui émergent, des personnes interviennent ponctuellement durant cette phase (ex. : des consultants), périodes d'essais sur différents produits, le projet peut être modifié en cours de route. • Phase d'exploitation : le projet est vivant et produit les résultats escomptés, des événements peuvent survenir spécifiquement durant cette phase, comme des mises à jour du système, des employés peuvent quitter, des personnes peuvent faire des demandes d'accès à l'information.
<p>7- Évaluer l'ampleur de l'EFVP à réaliser</p>	<p>L'ampleur de l'EFVP peut varier en fonction de l'envergure du projet, de ses objectifs, de la nature des renseignements personnels et de la manière dont ils sont utilisés et communiqués.</p> <p>Il peut y avoir des variations dans :</p> <ul style="list-style-type: none"> • Le nombre d'acteurs à solliciter ; • Le temps à investir ; • Le niveau de détail d'un éventuel rapport ; • La documentation annexe à élaborer ; • La quantité de mesures prévues pour atténuer ou éliminer les risques ; • Le niveau de détail de ces mesures. <p>L'EFVP doit être proportionnée à :</p> <ul style="list-style-type: none"> • La sensibilité des renseignements concernés ; • La finalité de leur utilisation ;

	<ul style="list-style-type: none"> • Leur quantité ; • Leur répartition ; • Leur support.
8- Évaluer le degré de sensibilité des renseignements personnels	<p>Un renseignement personnel est sensible lorsqu'il suscite un haut degré d'attente raisonnable en matière de vie privée, en raison de sa nature ou du contexte de son utilisation ou de sa communication.</p> <p>Exemples de renseignements sensibles :</p> <ul style="list-style-type: none"> • 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. <p>Les renseignements peuvent aussi être considérés comme sensibles s'ils servent dans un projet affectant spécifiquement une population vulnérable (ex. : personnes mineures, minorités ethnoculturelles, minorités sexuelles).</p>
9- Évaluer la finalité de l'utilisation ou de la communication des renseignements personnels	<p>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 (ex. : juridiques) sur eux ?</p> <p>Exemples de finalités :</p> <ul style="list-style-type: none"> • Profiler, localiser ou identifier une personne ; • Effectuer une surveillance systématique ou généralisée ; • Établir le profil d'une personne (ex. : 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 ; • Alimenter une nouvelle technologie aux effets moins connus.
10- Évaluer la quantité de renseignements personnels	<p>Combien de renseignements personnels seront utilisés dans le projet ? Leur quantité influence-t-elle l'ampleur des risques prévisibles ?</p> <p>Exemples de questions à se poser :</p> <ul style="list-style-type: none"> • Combien de personnes sont concernées par le projet (nombre absolu ou proportion) ? • Quel est le volume ou l'étendue des renseignements personnels concernés (toutes catégories confondues : recueillis, observés, inférés, créés) ? • Quelle est la durée envisagée du projet ? Est-il permanent ou temporaire ? • Quelle est l'extension géographique projetée ?

<p>11- Évaluer la répartition des renseignements personnels</p>	<p>Comment seront répartis les renseignements personnels utilisés dans le projet ?</p> <p>Considérer notamment les dimensions suivantes :</p> <ul style="list-style-type: none"> • 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 utilisés dans le projet ? • Humaine ou administrative – Par exemple, à qui seront communiqués les renseignements personnels utilisés dans le projet (ex.: un prestataire de services) ? • Quantitative – Par exemple, combien de personnes auront accès à ces renseignements ? Sur combien de supports seront-ils hébergés ?
<p>12- Évaluer le support de conservation des renseignements personnels</p>	<p>Sur quel(s) type(s) de support(s) seront conservés, momentanément ou à long terme, les renseignements personnels utilisés dans le projet ? Quelle est la nature des éléments matériels ou virtuels permettant de consigner, de conserver et de consulter l’information ?</p> <p>Exemples :</p> <ul style="list-style-type: none"> • Physique (tangible) ou numérique (ex. : hébergement en infonuagique) ; • Sécurisé ou non sécurisé ; • Connecté avec d’autres systèmes ou non.
<p>13- Dresser la liste des obligations</p>	<p>Au Québec, l’utilisation de renseignements personnels est encadrée principalement par la Loi sur l’accès et la Loi sur le privé.</p> <p>Voici une liste non exhaustive d’autres lois qui contiennent des particularités en matière de protection des renseignements personnels :</p> <ul style="list-style-type: none"> • <i>Code civil du Québec ;</i> • <i>Loi sur les archives ;</i> • <i>Loi concernant le cadre juridique des technologies de l’information ;</i> • <i>Code des professions ;</i> • <i>Loi sur l’administration fiscale ;</i> • <i>Code de la sécurité routière ;</i> • <i>Loi sur la protection de la jeunesse ;</i> • <i>Loi sur les services de santé et les services sociaux ;</i> • <i>Loi sur l’assurance maladie.</i> <p>Exemples de particularités et exceptions précisées dans des lois :</p>

	<ul style="list-style-type: none"> • La collecte et l'utilisation du numéro de permis de conduire et du numéro d'assurance maladie sont régies par des lois, des règlements ou des directives sectorielles ; • La gestion du consentement est particulière pour les mineurs et les personnes majeures inaptes ; • La collecte et l'utilisation de renseignements biométriques sont régies de manière spécifique et complémentaire par la <i>Loi concernant la cadre juridique des technologies de l'information</i>.
<p>14- Analyser et évaluer les facteurs relatifs à la vie privée</p>	<p>Considérer tous les facteurs qui auront un effet positif ou négatif sur le respect de la vie privée des personnes concernées.</p> <p>Ces facteurs sont :</p> <ol style="list-style-type: none"> 1. La conformité du projet à la législation applicable en matière de protection des renseignements personnels et le respect des principes l'appuyant ; 2. L'identification des risques d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs conséquences ; 3. La mise en place de stratégies pour éviter ces risques ou les réduire efficacement et leur maintien dans le temps.
<p>15- Respecter les obligations et les principes de protection des renseignements personnels</p>	<p>Déterminer la conformité du projet à la législation applicable en matière de protection des renseignements personnels et aux principes l'appuyant comme :</p> <ul style="list-style-type: none"> • La responsabilité : les organisations sont imputables quant à leur gestion des renseignements personnels. Elles mettent en place des politiques, des règles 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. • La détermination des fins : les fins pour lesquelles les organisations recueillent des renseignements personnels sont légitimes et établies avant la collecte. • La 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. • Le consentement : les personnes sont adéquatement informées des fins déterminées et y consentent librement, à moins d'exception. • La protection dès la conception et par défaut : les produits/services sont conçus dans le respect de la vie privée

	<p>des personnes. S'ils incluent des paramètres de confidentialité, ceux-ci protègent la vie privée par défaut.</p> <ul style="list-style-type: none"> • La 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. • L'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. • La 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. • La transparence : les organisations fournissent les informations pertinentes aux personnes concernées au moment de la collecte ou du consentement. Elles diffusent au public leurs coordonnées et des informations claires sur leurs règles et pratiques de gestion des renseignements personnels. • Les 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. • Le 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.
<p>16- Identifier les risques d'atteinte à la vie privée engendrés par votre projet et évaluer leurs conséquences</p>	<p>Qu'est-ce qu'un risque d'atteinte à la vie privée?</p> <p>Il s'agit d'une situation ou d'un événement futur qui peut ou non se réaliser et qui causerait une perte ou un préjudice à une personne quant au respect de son intimité ou de sa vie personnelle. Le risque est une <i>menace potentielle</i>.</p> <p>La perte ou le préjudice n'a pas besoin d'être tangible : les effets de l'atteinte à la vie privée peuvent être manifestes et externes (ex. : en cas d'atteinte à la réputation des personnes concernées), ou être vécues de l'intérieur par les personnes concernées (ex. : sentiment d'intrusion). Certains aspects légalement conformes d'un projet peuvent donc quand</p>

même être perçus comme une atteinte à la vie privée par les personnes concernées.

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 ;
- Divulgateion non autorisée de renseignements personnels ;
- Décision fondée sur des renseignements personnels inexacts ou équivoques ;
- Vol de renseignements personnels ;
- Intrusion dans la vie privée disproportionnée par rapport à l'objectif visé par le projet ;
- Conservation de renseignements lorsque leur utilité n'est plus démontrée ;
- Réidentification de renseignements préalablement anonymisés.

Décrire et évaluer les conséquences potentielles :

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

NOTE : Les conséquences pour notre organisation ne doivent pas entrer en ligne de compte dans l'EFVP qui vise à préserver la vie privée des personnes concernées.

Identifier les causes de ces risques :

- Processus déficient ;
- Erreur dans la manipulation des renseignements ;
- Manque de connaissances ou de formation ;
- Mécanismes de surveillance insuffisants ou inexistantes ;
- 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.

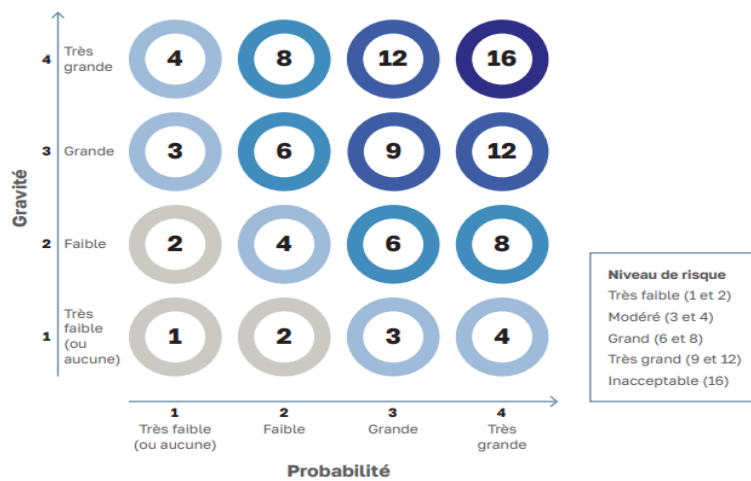
Tenir compte de certaines particularités :

- Projets impliquant de nouvelles technologies ;
- Projets d'envergure ;
- Projets comportant des enjeux éthiques.

Évaluer le niveau de chaque risque identifié :

Il n'y a pas de méthode prescrite pour qualifier ou évaluer les risques ni pour présenter les résultats de votre analyse. 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.

Par exemple :



L'évaluation de la gravité des conséquences potentielles peut être influencée par certaines variables :

- La quantité de renseignements impliqués ;
- La nature et la sensibilité des renseignements impliqués ;
- La gravité et la nature des préjudices qui pourraient être causés (ex. : conséquences majeures pour la vie personnelle ou professionnelle des personnes concernées, conséquences sur leurs finances, procédures juridiques ou démarches qu'elles doivent mener pour résoudre la situation, danger pour leur vie ou leur sécurité) ;
- Le nombre de personnes potentiellement touchées ou le profil de ces personnes (ex. : enfants, personnes en situation de handicap, immigrants).

	<p>Considérer les stratégies et les moyens de contrôle existants : Voir si des outils, des règles, des politiques, des directives, des procédures ou d'autres moyens existants peuvent atténuer ou éliminer le risque sans que des mesures supplémentaires soient requises.</p> <p>Déterminer le seuil acceptable de tolérance pour chaque risque : Se mettre dans la peau des personnes concernées et se demander comment elles pourraient s'attendre à ce que leurs renseignements personnels soient utilisés, communiqués et protégés. Se fixer des seuils à atteindre selon ce qui pourrait paraître acceptable pour ces personnes.</p>
<p>17-Mettre en place des stratégies pour éviter ou réduire les risques</p>	<p>Étudier les stratégies envisageables pour éviter ou réduire les risques.</p> <p>Exemples de stratégies :</p> <ul style="list-style-type: none"> • Prévoir une révision périodique des différentes collectes de renseignements personnels ; • Mettre en place un système de gestion documentaire qui permet l'application automatisée du calendrier de conservation ; • Revoir les processus d'attribution et de gestion des accès informatiques ; • Revoir périodiquement les paramètres de sécurité de la prestation électronique de services ; • Revoir les clauses des contrats en matière de confidentialité ; • Établir un calendrier de formation et d'activités de sensibilisation pour vos employés ; • Faire une campagne d'information concernant votre nouvelle utilisation des renseignements personnels ; • Journaliser les accès et exploiter les journaux pour détecter les anomalies ; • Dépersonnaliser ou anonymiser les renseignements si leur utilisation sous une forme directement identificatoire n'est pas requise pour tous. <p>Choisir les stratégies à adopter : Déterminer quelles stratégies et quels moyens mettre en place pour éliminer ou réduire un risque. Choisir des solutions réalisables pour notre organisation.</p> <p>Réévaluer le niveau de chacun des risques : À la lumière des stratégies et des moyens retenus, réévaluer le niveau d'importance du risque et la probabilité qu'il se concrétise. Vérifier si le seuil de tolérance fixé est respecté. Sinon, réévaluer le choix de stratégies ou de moyens.</p> <p>Si on ne parvient toujours pas à éliminer un risque important ou que le seuil de tolérance fixé n'est pas respecté, <i>revoir cet aspect du projet ou le retirer.</i></p>

	<p>Tout risque qui persiste à la fin, une fois que les mesures visant à diminuer ou à éliminer les risques identifiés au départ ont été prises, devient un risque résiduel. Il est possible que des risques d'atteinte à la vie privée subsistent même après avoir éliminé ou minimisé la plupart d'entre eux.</p> <p>Revoir la proportionnalité du projet : Après avoir terminé l'exercice de gestion des risques, refaire l'exercice d'évaluer la proportionnalité du projet par rapport aux risques qu'il fait toujours courir aux personnes concernées.</p> <p>À la lumière de l'ensemble de l'EFVP, est-ce que la solution proposée pour atteindre nos objectifs paraît toujours proportionnelle, compte tenu des risques résiduels ?</p> <p>En cas de plainte par une personne concernée ou de vérification par un organisme de contrôle, serons-nous prêts à répondre aux questions de la Commission sur le fait que notre solution est proportionnelle ?</p>
<p>18- Faire le suivi de l'Évaluation</p>	<p>Établir le plan d'action : Planifier la mise en œuvre des stratégies et des moyens retenus.</p> <p>Identifier les responsables de la gestion des risques résiduels : Identifier les personnes responsables de surveiller l'évolution des risques résiduels.</p> <p>Informers les autorités : Pour accepter les conclusions de l'analyse et cautionner les risques qui subsistent malgré les moyens déployés pour les atténuer.</p>
<p>19- Rendre compte de l'Évaluation</p>	<p>Un rapport d'EFVP sert à documenter et à consolider les résultats de l'évaluation.</p> <p>Il permet d'attester des démarches et de la réflexion dans le cas d'une vérification, d'une inspection ou d'une enquête menée par une autorité réglementaire.</p> <p>De plus, lorsque la loi prévoit une obligation de transmettre une EFVP à la Commission, le rapport est un moyen approprié.</p>

Directive relative à la gestion des incidents de confidentialité impliquant des renseignements personnels

1. Procédure de déclaration des incidents de confidentialité

- 1.1. L'employé qui a des motifs de croire qu'un incident de confidentialité est survenu doit, sans délai, le déclarer à sa direction d'établissement ou de service et au Responsable.
- 1.2. La déclaration doit être faite à l'adresse courriel suivante : secgen@cssps.gouv.qc.ca.
- 1.3. Dans la mesure du possible, le déclarant consigne les informations suivantes relativement à l'incident de confidentialité qu'il croit être survenu :
 - Le contexte et les circonstances entourant l'événement (dates, description des faits, etc.) ;
 - La nature des renseignements personnels en cause (ex. : noms, adresse, courriel, code permanent, etc.) ;
 - Les mesures de protection qui étaient en place au moment des faits ;
 - Le nombre de personnes concernées par l'incident de confidentialité et leurs coordonnées ;
 - L'identité et le nombre de personnes qui ont reçu les renseignements personnels sans autorisation le cas échéant ;
 - Les mesures immédiates prises le cas échéant ;
 - Toute autre information pertinente.
- 1.4. Dans les meilleurs délais, le déclarant doit informer la direction de son établissement ou de son service de l'Incident.
- 1.5. Le Responsable analyse sommairement la situation déclarée et détermine s'il s'agit d'un incident de confidentialité concernant des renseignements personnels.
- 1.6. S'il détermine qu'il ne s'agit pas d'un incident de confidentialité, mais qu'il juge qu'une intervention est tout de même nécessaire auprès des personnes impliquées, il communique avec la direction d'établissement ou la direction du service visé afin qu'elle pose, le cas échéant, les actions requises.

2. Mise en application de mesures d'atténuation immédiates

2.1. Lorsque les circonstances le permettent, le Responsable met en application des mesures d'atténuation immédiates pour éviter qu'un préjudice ne soit causé aux personnes concernées ou qu'un incident de confidentialité de même nature ne survienne. Pour ce faire, le Responsable peut faire appel à tout employé dont l'aide ou l'expertise est requise, dont notamment le Chef de la sécurité de l'information organisationnelle.

2.1.1. Les mesures d'atténuation immédiates peuvent comprendre :

- La fermeture de tout serveur ou logiciel informatique ;
- Rappeler des courriels ;
- Révoquer ou modifier des mots de passe ou des codes d'accès ;
- Etc.

2.2. Le cas échéant, le Responsable, en collaboration avec la direction d'établissement ou de la direction du service, veille à obtenir des personnes à qui ont été illégalement communiqués des renseignements personnels, une confirmation de destruction ou un engagement de non-divulgateion de ces renseignements.

2.3. Selon le cas, le Responsable veille à informer les principaux intervenants concernés par l'incident de confidentialité : direction générale, direction du service des affaires publiques, des communications et du secrétariat général, service de police (si les circonstances portent à croire qu'un crime a été commis), assureurs, ministère de l'Éducation (ex. : en cas de cyberattaque), etc.

3. Évaluation du risque de préjudice sérieux

3.1. Le Responsable coordonne l'évaluation du risque de préjudice sérieux de l'incident de confidentialité en considérant notamment la sensibilité du renseignement, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

4. Mesures à prendre lorsque l'incident de confidentialité présente un risque de préjudice sérieux

4.1. Si l'incident de confidentialité présente un risque de préjudice sérieux, le Responsable doit veiller à ce que :

- La Commission d'accès à l'information du Québec soit avisée de l'incident de confidentialité avec diligence, de la manière et en fournissant les informations requises ;
- Toute personne dont les renseignements personnels sont en cause par l'incident de confidentialité soit informée et en lui fournissant les

informations requises ;

- Tout organisme susceptible de diminuer le risque de préjudice sérieux soit informé (ex. : ministère, police, spécialiste en gestion de crise, etc.) en ne communiquant que les renseignements personnels nécessaires à cette fin.

4.2. Aucun avis aux personnes visées n'est nécessaire si un tel avis avait pour effet d'entraver une enquête faite par une personne ou par un organisme qui en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

5. Registre des Incidents de confidentialité

5.1. Le Responsable inscrit l'incident de confidentialité impliquant des renseignements personnels au registre des Incidents de confidentialité dans tous les cas.

6. Mesures à prendre pour éviter qu'un Incident de confidentialité de même nature se reproduise

6.1. Une fois les mesures immédiates mises en place, le Responsable détermine si d'autres mesures doivent être appliquées pour éviter que des incidents de confidentialité de même nature ne se reproduisent. Ces mesures peuvent comprendre : la modification des accès informatiques, des rappels des bonnes pratiques, la révision de processus internes, etc. ;

6.2. Afin de mettre en place les mesures correctrices identifiées, le Responsable peut faire appel à toute personne dont l'aide lui est nécessaire, dont notamment la direction d'un établissement ou d'un service.