

MISE EN PLACE DE LA LOI 25 SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (ANCIENNEMENT PROJET DE LOI NO 64)

Foire aux questions

Mai 2022

Dernière mise à jour : 2023-03-30

Note au lecteur : vous retracerez les ajouts ou modifications de **septembre 2022**, ceux-ci sont **surlignées en jaune** dans le présent document.

Les ajouts ou modifications de **mars 2023** sont **surlignées en turquoise** dans le présent document.

Veuillez noter que l'ordre des questions peut avoir changé d'une version à l'autre compte tenu de la bonification du contenu du document

Document produit en collaboration avec la firme Langlois, avocats.

TABLE DE MATIÈRES

TABLE DE MATIÈRES	3
OBJET DE LA FOIRE AUX QUESTIONS	5
RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET COMITÉ SUR L'ACCÈS À L'INFORMATION ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	5
1. Qu'entend-t-on par principe de responsabilité ?	5
2. Qui est responsable de la protection des renseignements personnels au sein d'un établissement d'enseignement privé ?	5
3. La fonction de responsable de la protection des renseignements personnels peut-elle être déléguée ? ..	5
4. De quelle façon se fait la délégation ?	5
5. Quel est le rôle du responsable de la protection des renseignements personnels ?	5
6. La Commission d'accès à l'information doit-t-elle être avisée de qui est responsable de la protection des renseignements personnels au sein de l'établissement ?	6
7. Un établissement doit-il constituer un comité sur l'accès à l'information et la protection des renseignements personnels ?	6
8. Quel est le rôle du comité sur l'accès à l'information et la protection des renseignements personnels ? ..	6
9. Quelle est la composition du comité sur l'accès à l'information et la protection des renseignements personnels ?	7
10. De qui relève le comité sur l'accès à l'information et sur la protection des renseignements personnels ? ..	7
INCIDENT DE CONFIDENTIALITÉ	7
11. Qu'est-ce qu'un incident de confidentialité ?	7
12. Un incident de confidentialité doit-il être déclaré à la Commission d'accès à l'information ?	7
13. Un incident de confidentialité doit-il être déclaré aux personnes concernées ?	8
14. Comment déterminer si un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé ?	8
15. Le responsable de la protection des renseignements personnels doit-il être consulté en cas d'incident de confidentialité ?	8
16. Quelle procédure suivre en cas d'incident de confidentialité ?	8
17. En plus des mesures à prendre en cas d'incident de confidentialité, que doit faire un établissement pour se préparer ?	9
18. Un registre doit-il être tenu en cas d'incident de confidentialité ?	9
RÈGLES ENCADRANT LA GOUVERNANCE	9
19. Quelle est la date d'entrée en vigueur de cette obligation ?	9
20. En quoi consiste les règles de gouvernance qu'un établissement doit publier sur son site Internet ?	9
21. Quel est le but d'adopter des règles encadrant la gouvernance des renseignements personnels ?	10
22. Comment mettre en place ces règles de gouvernance ?	11

23. Qui doit approuver les règles encadrant la gouvernance à l’égard des renseignements personnels?.....	11
POLITIQUE DE CONFIDENTIALITÉ.....	11
24. Quel est l’objectif d’une politique de confidentialité ?	11
25. Dois-je adopter une politique de confidentialité ?	11
26. Que doit contenir une politique de confidentialité ?.....	11
CONSENTEMENT	12
27. Dois-je obtenir un consentement avant de collecter, utiliser ou communiquer des renseignements personnels ?.....	12
28. Un élève de moins de 14 ans peut-il consentir par lui-même ?	13
29. Un élève de 14 ans et plus peut-il consentir par lui-même ?.....	13
30. Existe-t-il des exceptions au consentement quant à l’utilisation de renseignements personnels?	13
31. Existe-t-il des exceptions au consentement quant à la communication de renseignements personnels ?.....	13
RENSEIGNEMENT PERSONNEL	14
32. Qu’est-ce qu’un renseignement personnel ?	14
33. Qu’est-ce qu’un renseignement personnel sensible ?	14
34. Qu’est-ce qu’un renseignement dépersonnalisé ?.....	14
35. Qu’est-ce qu’un renseignement anonymisé ?.....	15
ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE	15
36. Qu’est-ce qu’une évaluation des facteurs relatifs à la vie privée ?	15
37. Dans quel cas doit-on réaliser une EFVP ?.....	15
38. Quels sont les éléments à prendre en considération dans le cadre d’une EFVP ?.....	16
39. À quel moment doit être réalisée une EFVP ?.....	16
40. Le responsable de la protection des renseignements personnels ou, le cas échéant, le comité sur l’accès et sur la protection des renseignements personnels doivent-ils être consultés ?	16
41. Quelles questions poser à un prestataire de service avant de lui communiquer des renseignements personnels – qu’il soit ou non à l’extérieur du Québec.	16
BIOMÉTRIE.....	17
TYPE DE BIOMÉTRIE.....	17
AUTRES EXIGENCES DONT UN ÉTABLISSEMENT VA DEVOIR TENIR COMPTE	17

OBJET DE LA FOIRE AUX QUESTIONS

La présente Foire aux questions (« FAQ ») a pour but d'accompagner les établissements d'enseignement privés dans la mise en place des mesures prévues par la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (« Loi 25 » anciennement « PL64 ») qui entrent en vigueur au cours des prochaines années.

Cette FAQ complète le Calendrier de réalisation proposé.

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET COMITÉ SUR L'ACCÈS À L'INFORMATION ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

1. *Qu'entend-t-on par principe de responsabilité ?*

Le principe de responsabilité introduit par la Loi 25 vise à responsabiliser les établissements à adopter de bonnes pratiques en matière de protection des renseignements personnels, notamment par la mise en place de documents encadrant la collecte, l'utilisation, la communication et la conservation des renseignements personnels.

En ce sens, les établissements devront adopter et/ou réviser leurs règles de gouvernance à ce sujet.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Principe de responsabilité d'un organisme public](#)

2. *Qui est responsable de la protection des renseignements personnels au sein d'un établissement d'enseignement privé ?*

La personne ayant la plus haute autorité au sein de l'établissement.

3. *La fonction de responsable de la protection des renseignements personnels peut-elle être déléguée ?*

Oui, la fonction peut être déléguée, par écrit, en tout ou en partie, soit :

- À un membre de l'établissement ou de son conseil d'administration, ou le cas échéant :
- À un membre du personnel de direction.

4. *De quelle façon se fait la délégation ?*

La délégation peut se faire de la même façon que pour le responsable de l'accès aux documents qui est déjà nommé au sein des établissements. Cette personne peut aussi assumer la fonction de responsable de la protection des renseignements personnels.

5. *Quel est le rôle du responsable de la protection des renseignements personnels ?*

Le responsable de la protection des renseignements personnels a pour fonction de :

- Veiller à assurer le respect et la mise en œuvre de la Loi ;
- Tenir les registres de communications de renseignements personnels sans le consentement de la personne concernée, incluant en cas d'incident de confidentialité ;
- Être consulté lors de l'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité ;
- Être avisé en cas d'incident de confidentialité survenu chez un mandataire ou l'exécutant d'un contrat de service ou d'entreprise ;
- Répondre aux demandes de communication ou de rectification.

6. La Commission d'accès à l'information doit-t-elle être avisée de qui est responsable de la protection des renseignements personnels au sein de l'établissement ?

Oui, la Commission doit être avisée, dès que possible, par écrit, du titre, des coordonnées et de la date d'entrée en fonction de la personne qui exerce les fonctions de responsable de la protection des renseignements personnels.

Un [formulaire](#) est disponible sur le site de la Commission d'accès à l'information à cet effet.

7. Un établissement doit-il constituer un comité sur l'accès à l'information et la protection des renseignements personnels ?

Oui, un tel comité doit être constitué à partir du 22 septembre 2022 au sein des établissements agréés à des fins de subventions en vertu de la *Loi sur l'enseignement privé et les personnes qui les tiennent*.

Établissements agréés à des fins de subventions en vertu de la *Loi sur l'enseignement privé et les personnes qui les tiennent*.

En vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, ces établissements sont considérés comme des organismes publics en ce qui concerne les documents détenus dans l'exercice de leurs fonctions relatives aux services éducatifs faisant l'objet de l'agrément et à la gestion des ressources qui y sont affectées.

À titre d'organisme public, ces établissements doivent se doter d'un comité sur l'accès à l'information et sur la protection des renseignements personnels.

Note : Un [projet de règlement](#) visant à exclure certains organismes publics de l'obligation de former un tel comité a été publié le 21 décembre 2022 à la Gazette officielle du Québec. Cette exclusion vise notamment les organismes publics qui emploient 50 employés ou moins.

Il convient de préciser que si ce projet de règlement est adopté, les fonctions confiées au comité sont assumées par le responsable de la protection des renseignements personnels.

Établissements non agréés à des fins de subventions en vertu de la *Loi sur l'enseignement privé*

Les établissements non agréés à des fins de subventions sont assujettis à la *Loi sur la protection des renseignements personnels* dans le secteur privé. Ces établissements n'ont pas à constituer un comité sur l'accès à l'information et sur la protection des renseignements personnels.

Toutefois, il peut être opportun de constituer un comité ayant pour mission la sécurité et la protection des renseignements personnels pour gérer notamment les incidents de confidentialité ou encore pour envisager les règles de gouvernance devant être adoptées (ou révisées) au sein de l'établissement.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels](#)

8. Quel est le rôle du comité sur l'accès à l'information et la protection des renseignements personnels ?

Le comité sur l'accès à l'information et la protection des renseignements personnels a pour fonction de :

- Soutenir l'établissement dans l'exercice de ses responsabilités et dans l'exécution de ses obligations à l'égard de la protection des renseignements personnels ;
- Approuver les règles de gouvernance à l'égard des renseignements personnels ;

- Être consulté lors des évaluations de facteurs relatifs à la vie privée pour tout projet d'acquisition, de développement et de refonte d'un système d'information ou d'une prestation électronique de services impliquant des renseignements personnels.

Infographie : Rôle / composition / actions clés

9. Quelle est la composition du comité sur l'accès à l'information et la protection des renseignements personnels ?

Le comité sur l'accès à l'information et la protection des renseignements personnels est composé du :

- Responsable de l'accès aux documents ;
- Responsable de la protection des renseignements personnels ;
- Toute autre personne dont l'expertise est requise, incluant, le cas échéant, le responsable de la sécurité de l'information et le responsable de la gestion documentaire.

10. De qui relève le comité sur l'accès à l'information et sur la protection des renseignements personnels ?

De la personne ayant la plus haute autorité au sein de l'établissement.

INCIDENT DE CONFIDENTIALITÉ

11. Qu'est-ce qu'un incident de confidentialité ?

On parle d'incident de confidentialité dans les cas suivants :

- Accès non autorisé par la loi à un renseignement personnel ;
- Utilisation non autorisée par la loi d'un renseignement personnel ;
- Communication non autorisée par la loi d'un renseignement personnel ;
- Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

12. Un incident de confidentialité doit-il être déclaré à la Commission d'accès à l'information ?

Depuis le 22 septembre 2022, les établissements d'enseignements privés – agréés aux fins de subventions ou non agréés – doivent aviser la Commission d'accès à l'information (« CAI ») mais aussi les personnes dont les renseignements personnels sont visés par un incident de confidentialité présentant un risque de préjudice sérieux. Ils doivent également tenir un registre des incidents de confidentialité.

Un [Règlement sur les incidents de confidentialité](#) a été publié à la Gazette officielle du Québec. Ce règlement prévoit les éléments que doivent contenir l'avis à la CAI, l'avis aux personnes concernées et le registre.

OUTIL

- Commission d'accès à l'information : Voir l'[Avis concernant un incident de confidentialité impliquant des renseignements personnels et qui présente un risque de préjudice sérieux](#) disponible sur le site de la CAI
- La FEEP vous propose une [Grille d'analyse – Évaluation des risques de préjudice](#) pour vous permettre d'évaluer les risques devant être déclarés à la CAI disponible sur son site internet.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Incident de confidentialité](#)

13. Un incident de confidentialité doit-il être déclaré aux personnes concernées ?

Oui, à partir du 22 septembre 2022, un établissement doit aviser les personnes concernées d'un incident de confidentialité.

Toutefois, si le fait de les aviser est susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé(e) de prévenir, détecter ou réprimer le crime ou les infractions aux lois, un établissement peut ne pas les aviser tout de suite.

- Personnes concernées : Voir le [Modèle de lettre](#) publié par le Gouvernement du Québec

14. Comment déterminer si un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé ?

Pour déterminer si un risque qu'un préjudice sérieux soit causé, l'établissement doit considérer :

- La sensibilité du renseignement concerné,
 - Exemple : numéro d'assurance sociale, dossier médical ou renseignement de nature médicale, renseignement financier
- Les conséquences appréhendées de son utilisation,
 - Exemple : vol d'identité, fraude financière, atteinte à la réputation
- La probabilité qu'il soit utilisé à des fins préjudiciables.

OUTIL : [Modèles de grille d'analyse d'un incident de confidentialité](#)

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Incident de confidentialité](#)

15. Le responsable de la protection des renseignements personnels doit-il être consulté en cas d'incident de confidentialité ?

Oui, l'établissement doit consulter le responsable de la protection des renseignements personnels lors de l'évaluation du préjudice.

De plus, ce dernier doit enregistrer toute communication qui serait faite à une personne ou à un organisme susceptible de diminuer le risque de préjudice.

16. Quelle procédure suivre en cas d'incident de confidentialité ?

En cas d'incident de confidentialité, il convient notamment :

- De déterminer les circonstances de l'incident
- De déterminer les renseignements personnels visés par l'incident
- De diminuer les risques en prenant les mesures nécessaires afin de :
 - Circonscrire l'incident ;
 - Apporter les correctifs requis ;
- D'identifier la nature du préjudice et, s'il présente un risque qu'un préjudice sérieux soit causé, en aviser la Commission d'accès à l'information et les personnes dont les renseignements personnels sont visés par l'incident
- D'inscrire l'incident dans le registre des incidents et ce, que le préjudice soit ou non sérieux.

Pour aller plus loin : Voir la [procédure](#) décrite à la section « Incident de confidentialité » du Gouvernement du Québec ou encore [l'infographie](#) relative à cette procédure.

17. En plus des mesures à prendre en cas d'incident de confidentialité, que doit faire un établissement pour se préparer ?

Pour pouvoir répondre rapidement à un incident de confidentialité, il est recommandé de mettre en place un plan de gestion des incidents de confidentialité.

- Savoir qui contacter en cas d'incident - idée d'avoir une cellule de crise – tant à l'interne qu'à l'externe
 - Exemple : Direction, Conseil d'administration, Responsable de la protection des renseignements personnels, Service technique / informatique, Service juridique, Assureur, Fournisseur de services, Direction, Service de communication.
- Savoir qui fait quoi

Par ailleurs, il est recommandé d'avoir une vue d'ensemble des mesures de sécurité en place, du type de renseignements personnels détenus par et pour le compte d'un établissement ou encore du type de support des renseignements. Cela permet, le cas échéant, de réviser les mesures de sécurité ou encore les contrats avec les fournisseurs de service ou d'assurance. Cela s'inscrit dans les règles de gouvernance qu'un établissement doit mettre en place pour septembre 2023.

18. Un registre doit-il être tenu en cas d'incident de confidentialité ?

Oui, l'établissement doit tenir un registre de tous les incidents de confidentialité que ceux-ci soient considérés ou non comme présentant un risque de préjudice sérieux.

Ce registre doit être transmis à la Commission d'accès à l'information sur demande.

OUTIL : [Modèle de registre des incidents de confidentialité](#)

- **Registre des incidents de confidentialité** : Voir le [Modèle de registre](#) publié par le Gouvernement du Québec.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Incident de confidentialité](#)

RÈGLES ENCADRANT LA GOUVERNANCE

19. Quelle est la date d'entrée en vigueur de cette obligation ?

Cette obligation entre en vigueur le 22 septembre 2023.

20. En quoi consiste les règles de gouvernance qu'un établissement doit publier sur son site Internet ?

Un établissement doit respecter plusieurs exigences issues de différentes lois, incluant celles relatives à la protection des renseignements personnels. Pour permettre à ses employés de comprendre les mesures prises en ce domaine, un établissement doit établir des politiques, directives ou guides à ce sujet. Cette documentation doit pouvoir aussi être disponibles pour les élèves et les titulaires de l'autorité parentale et tuteurs.

Ces règles doivent notamment prévoir :

- Les rôles et responsabilités des membres de l'établissement tout au long du cycle de vie des renseignements personnels, c'est-à-dire, de leur collecte à leur destruction ;
- Le processus de traitement des plaintes relatives à la protection des renseignements personnels, mais aussi celui relatif aux demandes d'accès ;
- La gestion des incidents de confidentialité ;

- Les projets de systèmes d'information ou de prestations électroniques de services impliquant des renseignements personnels ou encore, le fait de recourir à des fonctions d'identification, de localisation ou de profilage des employés ou des élèves ;
- La communication de renseignements personnels lors d'un mandat ou d'un contrat de service ou d'entreprise ;
- Les activités de formation et de sensibilisation proposées par l'établissement ;
- Les mesures de protection prises lors de la mise en place de sondage impliquant la collecte de renseignements personnels.
- Les mesures applicables à la conservation et à la destruction des renseignements personnels

■ **Attention** : Cette dernière mesure ne vise que les établissements d'enseignements privés non agréés aux fins de subventions ... mais il convient de préciser que les autres établissements doivent déjà avoir un calendrier de conservation des renseignements personnels;

Par ailleurs, il est recommandé également d'adopter ou à tout le moins de réviser les règles énonçant :

- Les mesures visant à assurer la sécurité des renseignements personnels, incluant le plan de gestion des incidents de confidentialité;
- L'utilisation et la communication des renseignements personnels afin notamment de préciser dans quels cas il convient de procéder à une évaluation des facteurs relatifs à la vie privée;
- Le processus de traitement des demandes d'accès et de rectification aux renseignements personnels;

Cette exigence de la Loi 25, qui entre en vigueur le 23 septembre 2023, fait écho au principe de responsabilité.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Règles encadrant la gouvernance](#)

21. Quel est le but d'adopter des règles encadrant la gouvernance des renseignements personnels ?

En plus de préciser qu'un établissement est responsable des renseignements personnels qu'il détient, la Loi 25 prévoit que celui-ci doit adopter des règles encadrant la gouvernance à l'égard de ces renseignements.

L'adoption des règles vise à encadrer les pratiques d'un établissement en matière de protection des renseignements personnels. Il est donc recommandé de faire répertorier l'ensemble des documents en lien avec la protection des renseignements personnels en vigueur au sein de l'établissement afin de les réviser et, le cas échéant, d'en adopter de nouveau pour répondre aux exigences de la Loi 25.

Ces règles sont le plus souvent énoncées dans des guides, politiques, procédures ou directives et sont diffusées auprès de l'ensemble des membres d'un établissement.

Cette diffusion a pour but de les informer mais aussi de leur permettre de comprendre et d'appliquer les exigences en matière de protection des renseignements personnels. En effet, la protection est l'affaire de tous.

22. Comment mettre en place ces règles de gouvernance ?

En vue de réviser ou d'adopter de nouvelles règles encadrant la gouvernance des renseignements personnels, un établissement doit dresser un inventaire :

- Des politiques, directives, pratiques et procédures en matière de protection des renseignements personnels en vigueur et ce, pour l'ensemble de ses services et activités opérationnelles.

Par exemple :

- Ressources humaines et paie
- Recrutement et inscription
- Services aux élèves (ex : service de garde, bibliothèque, sport, transport, parascolaire, etc.)
- Systèmes informatiques, applications, infonuagiques, serveurs, logiciels
- Fournisseurs de services et/ou sous-contractants
- Des renseignements personnels qu'il détient ou qu'un tiers collecte, utilise, communique ou conserve pour son compte

Cet inventaire doit se faire quel que soit le support nécessitant la collecte, l'utilisation, la communication ou la conservation des renseignements personnels (papier ou électronique).

23. Qui doit approuver les règles encadrant la gouvernance à l'égard des renseignements personnels ?

Pour les établissements qui ont l'obligation de constituer un comité sur l'accès à l'information et sur la protection des renseignements personnels, les règles doivent être approuvées par ce dernier.

Pour les autres, les règles doivent être approuvées par le responsable de la protection des renseignements personnels.

POLITIQUE DE CONFIDENTIALITÉ

24. Quel est l'objectif d'une politique de confidentialité ?

Une politique de confidentialité vise à informer les personnes qui visitent un site Internet, entre autres, à des fins pour lesquelles leurs renseignements personnels sont collectés, des catégories de personnes qui y auront accès tant à l'interne qu'à l'externe, de l'endroit où ils seront conservés et de la manière dont ils peuvent faire valoir leurs droits.

25. Dois-je adopter une politique de confidentialité ?

Oui, la Loi 25 précise qu'à partir du 22 septembre 2023, les établissements d'enseignements privés – agréés aux fins de subventions ou non agréés – qui recueillent par un moyen technologique des renseignements personnels doivent publier sur leur site Internet, le cas échéant, et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs.

26. Que doit contenir une politique de confidentialité ?

Une politique de confidentialité doit contenir au minimum les informations suivantes :

- Une description des renseignements personnels qui seront recueillis, notamment par le biais du site Internet de l'établissement;
- Les fins pour lesquelles les renseignements sont recueillis, notamment la prestation du service éducatif;

- Les moyens par lesquels les renseignements sont recueillis, notamment si ceux-ci sont recueillis directement ou indirectement auprès des élèves / des parents ou encore par le biais d'une technologie permettant de les identifier, de les localiser ou de les profiler;
- Les catégories de personnes qui y auront accès tant à l'intérieur qu'à l'extérieur de l'établissement;
- Le lieu de conservation ou de détention des renseignements personnels, notamment si ceux-ci sont communiqués à l'extérieur du Québec;
- La durée de conservation des renseignements personnels;
- Les droits (accès, rectification, retrait, désindexation) accordés, comment les exercer et auprès de qui.

CONSENTEMENT

27. *Dois-je obtenir un consentement avant de collecter, utiliser ou communiquer des renseignements personnels ?*

Oui, et le consentement doit être manifeste, libre, éclairé. Il doit être donné à des fins spécifiques et, il ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Dans la section « [Validité du consentement](#) » du Gouvernement du Québec, les cinq caractéristiques du consentement sont définies de la façon suivante :

Manifeste :

Cela signifie que le consentement doit être évident, certain et indiscutable et qu'il ne doit laisser aucun doute quant à la volonté qui y est exprimée.

Libre

Le consentement doit être donné sans contrainte. Ce critère ne serait pas satisfait si, par exemple, le consentement résultait d'une pression exercée sur la personne concernée.

Éclairé

S'entend d'une demande précise et rigoureuse, qui permet à la personne concernée de donner son consentement en toute connaissance de cause.

Donné à des fins spécifiques

Cela signifie que le consentement doit être demandé à des fins précises et qu'il ne peut donc pas être général. La personne concernée doit être en mesure de comprendre à quelles fins elle donne son consentement.

Durée nécessaire à la réalisation des fins auxquelles il est demandé

Le consentement ne doit être donné que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé. Cette durée peut être un nombre de jours, de mois ou d'années, ou alors faire référence à un événement déterminé ou à une situation précise.

Par ailleurs, il est prévu que lorsque le consentement est demandé par écrit, il doit être présenté distinctement de toute autre information communiquée aux personnes concernées (c.-à-d. employé, élève, parent d'élève (titulaire de l'autorité parentale ou tuteur)).

Attention, en ce qui concerne les renseignements personnels sensibles, le consentement doit être manifesté de façon expresse.

28. Un élève de moins de 14 ans peut-il consentir par lui-même ?

Non, il est prévu qu'un mineur de moins de 14 ans ne peut consentir par lui-même. Le consentement doit être donné par le titulaire de l'autorité parentale ou le tuteur du mineur.

Par contre, un établissement peut collecter des renseignements personnels auprès d'un mineur de moins de 14 ans lorsque la collecte est manifestement au bénéfice du mineur.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Personnes mineures, titulaires de l'autorité parentale ainsi que tutrices ou tuteurs](#)

29. Un élève de 14 ans et plus peut-il consentir par lui-même ?

Oui, le consentement d'un mineur de 14 ans et plus peut être donné par le mineur, par le titulaire de l'autorité parentale ou par le tuteur.

30. Existe-t-il des exceptions au consentement quant à l'utilisation de renseignements personnels?

En principe, un renseignement personnel ne peut être utilisé au sein d'un établissement qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée.

Toutefois, un établissement en fonction peut utiliser les renseignements personnels collectés à une autre fin sans le consentement des personnes concernées notamment :

- Lorsque son utilisation est à des **fins compatibles** avec celles pour lesquelles il a été recueilli ;
- Lorsque son utilisation est **manifestement au bénéfice de la personne concernée** ;
- Lorsque son utilisation est nécessaire à des **fins d'étude, de recherche ou de production de statistiques** et qu'il est **dépersonnalisé** ;
- Lorsque son utilisation est **nécessaire à l'application d'une loi au Québec**, que cette utilisation soit ou non prévue expressément par la loi.

31. Existe-t-il des exceptions au consentement quant à la communication de renseignements personnels ?

En principe, un établissement ne peut communiquer un renseignement personnel sans le consentement de la personne concernée.

Toutefois, un établissement peut communiquer les renseignements personnels collectés, sans le consentement des personnes concernées, dans les cas suivants :

- Au procureur de l'établissement, si le renseignement est **nécessaire aux fins d'une poursuite pour infraction à une loi que l'établissement est chargé d'appliquer**, ou au Directeur des poursuites criminelles et pénales, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec ;
- À une personne ou à un organisme qui, en vertu de la loi, est chargé(e) de **prévenir, détecter ou réprimer le crime ou les infractions aux lois**, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec ;
- À une personne à qui cette communication doit être faite en raison d'une **situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée** ;
- En vue de **prévenir un acte de violence**, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence ;

- À toute personne ou organisme, si cette communication est **nécessaire à l'application d'une loi au Québec**, que cette communication soit ou non prévue expressément par la loi ;
- À toute personne ou organisme, si cette communication est nécessaire **à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise** confié par l'établissement à cette personne ou à cet organisme ;
- À une personne ou à un organisme qui souhaite utiliser ces renseignements **à des fins d'étude, de recherche ou de production de statistiques**. Cette communication devra faire l'objet d'une évaluation des facteurs relatifs à la vie privée et d'une entente soumise à la Commission d'accès à l'information.

RENSEIGNEMENT PERSONNEL

32. Qu'est-ce qu'un renseignement personnel ?

Un renseignement personnel est un renseignement qui concerne une personne physique (c.-à-d. employé, élève, parent d'élève (titulaire de l'autorité parentale ou tuteur)) et permet, directement ou indirectement, de l'identifier.

Cette définition vise entre autres :

- Nom, prénom, adresse (résidence principale et/ou secondaire), téléphone (maison, cellulaire), code postal
- Adresse courriel
- Date de naissance, âge
- État civil
- Nationalité
- Antécédents médicaux, scolaires, professionnels, financiers – voir la définition de renseignements sensibles
- Empreinte digitale, voix, forme de la main / du visage, ADN, etc. – voir la définition de renseignements sensibles
- Numéro d'assurance sociale, d'assurance maladie, de permis de conduire
- etc.

33. Qu'est-ce qu'un renseignement personnel sensible ?

À partir du 22 septembre 2023, seront considérés comme sensibles les renseignements personnels qui, par leur nature, notamment médicale, biométrique ou autrement intime, ou en raison du contexte de leur utilisation et communication, suscitent un haut degré d'attente raisonnable en matière de vie privée.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Définition](#)

34. Qu'est-ce qu'un renseignement dépersonnalisé ?

À partir du 22 septembre 2023, un renseignement sera considéré comme dépersonnalisé lorsqu'il ne permet plus d'identifier directement la personne concernée.

« La dépersonnalisation consiste à retirer tous les renseignements qui permettent l'identification directe de la personne concernée, notamment les renseignements identificatoires. Il s'agit, par exemple, du nom, de l'adresse du domicile ou d'un numéro

associé à une personne, comme celui de l'assurance sociale ou de l'assurance maladie. Habituellement, ces renseignements sont remplacés par un code.

Les renseignements dépersonalisés demeurent des renseignements personnels, car l'identification indirecte de la personne concernée est toujours possible. Cela peut se faire, par exemple, en combinant différents renseignements sur une personne, tels son sexe, son âge ou son code postal. »

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Définition](#)

35. Qu'est-ce qu'un renseignement anonymisé ?

À partir du 22 septembre 2023, un renseignement sera considéré comme anonymisé lorsqu'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.

« Le terme « irréversible » implique qu'il ne doit pas être possible, au moment de l'anonymisation et en tout temps, et ce, en considérant un futur prévisible, d'identifier de nouveau la personne concernée directement ou indirectement.

L'évaluation du caractère irréversible de l'anonymisation doit notamment tenir compte :

- des avancées technologiques raisonnablement prévisibles ;
- du nombre et de la nature des renseignements visés ;
- des liens qui peuvent être effectués entre ces renseignements et d'autres informations qui sont détenues par l'organisme ou publiquement accessibles, ou qu'il est raisonnable de prévoir qu'elles le seront. »

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, [Destruction ou anonymisation, Définition](#)

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

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

Une évaluation des facteurs relatifs à la vie privée (« EFVP ») permet d'anticiper les risques d'atteinte à la vie privée des personnes concernées et de prendre les mesures pour les atténuer et, ainsi se conformer aux exigences légales en matière de protection des renseignements personnels.

Pour aller plus loin :

- GOUVERNEMENT DU QUÉBEC, [Évaluation des facteurs relatifs à la vie privée](#)
- COMMISSION D'ACCÈS À L'INFOMATION, [Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée, 2021 \(en révision\)](#).

37. Dans quel cas doit-on réaliser une EFVP ?

La Loi 25 prévoit plusieurs cas dans lesquels un établissement doit réaliser une EFVP :

- Depuis le 22 septembre 2022, une EFVP doit être réalisée avant de communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques;
- À compter du 22 septembre 2023, une EFVP devra être réalisée :
 - Pour tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, Projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services;

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

Pour aller plus loin : GOUVERNEMENT DU QUÉBEC, Communication à l'extérieur du Québec;

- Avant de recueillir des renseignements personnels nécessaires à l'exercice des attributions d'un organisme public ou à la mise en œuvre d'un programme - **Attention** : ne vise que les établissements d'enseignements privés agréés aux fins de subventions
- Avant de communiquer des renseignements personnels dans les cas prévus par l'article 68 de la Loi sur l'accès - **Attention** : ne vise que les établissements d'enseignements privés agréés aux fins de subventions

38. Quels sont les éléments à prendre en considération dans le cadre d'une EFVP ?

Chacun des cas dans lequel une EFVP doit être réalisée prévoit des éléments spécifiques. Néanmoins, il est permis de considérer que doivent être pris en considération :

- La sensibilité des renseignements personnels;
- La finalité de leur utilisation;
- Leur quantité, leur répartition et leur support.

Pour ce qui est des EFVP à réaliser avant de communiquer des renseignements à l'extérieur du Québec, il convient également de considérer les mesures de protection dont le renseignement bénéficierait, ainsi que le régime juridique applicable dans l'État où les renseignements sont communiqués. De plus, une entente doit être conclue entre les parties.

39. À quel moment doit être réalisée une EFVP ?

Une EFVP doit être réalisée avant tout projet d'acquisition, de développement ou de refonte et avant de communiquer les renseignements personnels à l'extérieur du Québec ou à des fins d'étude, de recherche ou de production de statistiques. Une EFVP doit donc être réalisée en amont de ces trois cas de figure.

40. Le responsable de la protection des renseignements personnels ou, le cas échéant, le comité sur l'accès et sur la protection des renseignements personnels doivent-ils être consultés ?

Oui, le responsable ou le comité doivent être consulté dans le cadre d'une EFVP.

41. Quelles questions poser à un prestataire de service avant de lui communiquer des renseignements personnels – qu'il soit ou non à l'extérieur du Québec.

Voici une liste non exhaustive de question à poser :

- Quels sont les moyens mis en place pour garantir la confidentialité, l'intégrité et la disponibilité des renseignements qui vous sont confiés ?
- Disposez-vous de certifications ou d'audits tiers pour évaluer votre conformité en matière de sécurité des renseignements ?

- Comment gérez-vous les incidents de sécurité, mais aussi de confidentialité?
- Avez-vous des plans d'intervention et des procédures pour prévenir, détecter et répondre à de tels incidents?
- Avez-vous une assurance cybersécurité?
- Où sont situés vos serveurs? S'ils sont situés à l'extérieur du Québec, vous êtes-vous assuré du niveau de protection offert?
- Qui est la personne responsable des renseignements personnels?

BIOMÉTRIE

Un nouvel encadrement entre en vigueur le 22 septembre 2022 et qui oblige les organisations qui souhaitent utiliser la biométrie et constituer une banque de caractéristiques ou de mesures biométriques : celles-ci doivent, préalablement à la création d'une telle banque, divulguer cette création à la Commission.

Pour aller plus loin : COMMISSION D'ACCÈS A L'INFORMATION, [Biométrie](#)

TYPE DE BIOMÉTRIE

Il existe trois grandes catégories de biométrie :

- La **biométrie morphologique** est basée sur l'identification de traits physiques particuliers. Elle regroupe notamment, mais pas exclusivement, la reconnaissance des empreintes digitales, de la forme de la main, du visage, de la rétine et de l'iris de l'œil ;
- La **biométrie comportementale** est basée sur l'analyse de certains comportements d'une personne, comme le tracé de sa signature, l'empreinte de sa voix, sa démarche, sa façon de taper sur un clavier, etc.
- La **biométrie biologique** est basée sur l'analyse des traces biologiques d'une personne, comme l'ADN, le sang, la salive, l'urine, les odeurs, etc.

Pour aller plus loin : COMMISSION D'ACCÈS A L'INFORMATION, [La biométrie au travail](#)

AUTRES EXIGENCES DONT UN ÉTABLISSEMENT VA DEVOIR TENIR COMPTE

En plus des exigences énoncées ci-dessus, un établissement va devoir tenir compte d'autres exigences. Pour en tenir compte, les présentes FAQ seront mises à jour prochainement.

Toutefois, un établissement peut déjà réfléchir aux éléments suivants :

- [Informations à communiquer](#) aux personnes concernées en cas de :
 - Recours à de la biométrie ;
 - [Fonctions permettant d'identifier, de localiser ou de profiler une personne physique](#) ;
 - [Décision fondée exclusivement sur un traitement automatisé](#) ;
 - [Paramètre de confidentialité](#) ;
 - Etc.

- Communication pour l'exercice d'un mandat ou pour l'exécution d'un contrat de service ou d'entreprise ;
- Procédure de dépersonnalisation, destruction et anonymisation des renseignements personnels;
- Droit à la portabilité.