Mise en place de la Loi 25 sur la protection des renseignements personnels

Gouvernance des renseignements personnels
Liste de contrôle et Modèles | MAI 2023

CHX
AVOCAT·LAWYER

PRODUIT PAR :
M^e^ Cynthia Chassigneux, CHX Avocat inc.

Fédération des établissements d'enseignement privés
Savoir réussir

Table des matières

Contexte

En septembre 2021, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[1] (« Loi 25 ») a été adoptée par l'Assemblée nationale du Québec. Cette loi vient ajouter et modifier plusieurs dispositions au cadre juridique applicable aux établissements d'enseignement privés en ce qui concerne la collecte, l'utilisation, la communication à des tiers, la conservation et la sécurité des renseignements personnels.

Ces exigences s'appliquent aussi bien à l'égard des renseignements personnels des élèves et de leurs parents (titulaires de l'autorité parentale, tuteurs, tutrices) que de ceux des employés ou des différents partenaires des établissements d'enseignement privés.

Parmi ces exigences, il est prévu que les établissements d'enseignement privés fassent preuve de transparence et adoptent des règles dites de gouvernance quant à la gestion des renseignements personnels qu'ils détiennent, et ce, même si celle-ci est confiée à un tiers.

Cette exigence entre en vigueur le 22 septembre 2023. Elle est intégrée aussi bien dans la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels*[2] que dans la *Loi sur la protection des renseignements personnels dans le secteur privé*[3].

> *Les règles de gouvernance doivent « permettre aux membres du personnel [des établissements d'enseignement privés] de connaître et de comprendre les exigences légales et les principes de protection des renseignements personnels qui sont inhérents à l'exercice de leurs fonctions ».*
>
> SOURCE
> *GOUVERNEMENT DU QUÉBEC*
> Règles encadrant la gouvernance des renseignements personnels

1 LQ 2021, c. 25.
2 RLRQ, c. A-2.1, la « Loi sur l'accès ».
3 RLRQ, c. P-39.1, la « Loi sur le secteur privé ».

Loi sur l'accès

63.3 Un organisme public doit **publier** sur son site Internet des **règles encadrant sa gouvernance** à l'égard des renseignements personnels. Ces règles doivent être **approuvées par** son comité sur l'accès à l'information et la protection des renseignements personnels.

Elles peuvent prendre la forme d'une politique, d'une directive ou d'un guide et doivent notamment prévoir les **rôles et les responsabilités des membres de son personnel** tout au long du cycle de vie de ces renseignements ainsi qu'un processus de traitement des plaintes relatives à la protection de ceux-ci. Elles incluent une **description des activités de formation et de sensibilisation** que l'organisme offre à son personnel en matière de protection des renseignements personnels.

Ces règles incluent également les **mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage**, dont une évaluation de :

1° la nécessité de recourir au sondage ;

2° l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

Un règlement du gouvernement peut déterminer le contenu et les modalités de ces règles.

Loi sur le secteur privé

3.2 Toute personne qui exploite une entreprise doit **établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance** à l'égard des renseignements personnels et propres à assurer la protection de ces renseignements. Celles-ci doivent notamment prévoir **l'encadrement applicable à la conservation et à la destruction** de ces renseignements, prévoir les **rôles et les responsabilités des membres de son personnel** tout au long du cycle de vie de ces renseignements et un **processus de traitement des plaintes** relatives à la protection de ceux-ci. Elles doivent également être proportionnées à la nature et à l'importance des activités de l'entreprise et être **approuvées par** le responsable de la protection des renseignements personnels.

Des informations détaillées au sujet de ces politiques et de ces pratiques, notamment en ce qui concerne le contenu exigé au premier alinéa, sont, en termes simples et clairs, **publiées** sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendues accessibles par tout autre moyen approprié.

Pour ce faire, les établissements d'enseignement privés doivent :

- Dresser l'inventaire des renseignements personnels qu'ils détiennent, des supports sur lesquels ils se trouvent et des personnes qui y ont accès, tant à l'interne qu'à l'externe.
- Dresser l'inventaire des consentements demandés, des contrats avec les fournisseurs de services, mais aussi des politiques, procédures et directives relatives à la protection des renseignements personnels en vigueur au sein de l'établissement.

Ces inventaires permettent aux établissements d'enseignement privés d'avoir une vue d'ensemble sur leurs pratiques en matière de protection des renseignements personnels.

Ils permettent aussi de voir quelles sont les règles à réviser ou, le cas échéant, à adopter pour répondre aux exigences découlant de la Loi 25 et intégrées à la Loi sur l'accès et à la Loi sur le secteur privé. Ils permettent aussi de savoir quelles sont les mesures qui doivent être prises pour sensibiliser les membres du personnel à la protection des renseignements personnels.

Objectif

Afin d'accompagner les établissements d'enseignement privés dans l'application des exigences relatives à la gouvernance des renseignements personnels qu'ils détiennent, la Fédération des établissements d'enseignement privés a produit le présent document qui contient des listes de contrôles et des modèles à l'égard des éléments suivants :

- Rôles et responsabilités des membres du personnel tout au long du cycle de vie des renseignement personnels
- Processus de traitement des plaintes
- Activités de formation et de sensibilisation
- Mesures prises à l'égard des sondages
- Encadrement applicable à la conservation et à la destruction

Par ailleurs, le présent document présente aussi des éléments en lien avec :

- Le traitement des demandes d'accès
- La gestion des incidents de confidentialité
- Les évaluations des facteurs relatifs à la vie privée – notamment pour les projets de système d'information ou de prestation électronique de services impliquant des renseignements personnels, pour les communications de renseignements personnels (que celles-ci aient lieu ou non à l'extérieur du Québec) ou encore pour la collecte des renseignements personnels nécessaires à l'exercice des attributions ou à la mise en œuvre d'un programme
- Et toute autre situation impliquant des renseignements personnels, comme la cueillette de tels renseignements par un moyen technologique qui nécessite d'avoir une politique de confidentialité

Il convient de préciser que le contenu de ces règles « doit demeurer suffisamment général, de manière à ne pas divulguer de renseignements confidentiels ni stratégiques. Ainsi, le contenu

ne doit pas détailler les mesures de sécurité qu'utilise un [établissement d'enseignement privé] pour protéger ses systèmes informatiques ».[4]

Enfin, ces règles doivent être approuvées par le comité sur l'accès à l'information et la protection des renseignements personnels ou, selon le cas, par le responsable de la protection des renseignements personnels.

[4] GOUVERNEMENT DU QUÉBEC, « Règles encadrant la gouvernance des renseignements personnels »

Rôles et responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels

Au sein d'un établissement d'enseignement privé, plusieurs personnes peuvent avoir accès aux renseignements personnels des élèves, des titulaires de l'autorité parentale ou encore des membres du personnel.

Pour éviter qu'une personne ait accès à de tels renseignements en dehors de ses fonctions, de son mandat ou de son contrat[5], il revient aux établissements d'enseignement privés de :

- Faire une cartographie du cycle de vie des renseignements personnels pour déterminer qui a (doit avoir) accès aux renseignements à chacune des étapes du cycle :
  - Documenter le rôle de la personne ou du corps de métier
  - Réviser la description du poste (rôle et responsabilité)
  - Revoir les permissions d'accès et les révoquer le cas échéant
  - Faire signer des engagements ou des accords de confidentialité

Parmi les postes visés par cet exercice, pensons notamment :

- Au responsable de la protection des renseignements personnels (modèle ci-après)
- Aux membres du secteur des ressources informatiques (modèle ci-après)
- Aux membres des ressources humaines (modèle ci-après)
- Aux membres de l'administration
- Aux enseignants
- Aux membres de la vie scolaire (bibliothèque, cafétéria, service de santé, service de garde, etc.)
- Aux fournisseurs de services et consultants externes, etc.

[5] Loi sur l'accès, art. 62; Loi sur le secteur privé, art. 20.

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

FICHE DESCRITPTIVE

Rôle du responsable de la protection des renseignements personnels

- Voir au respect de la protection des renseignements personnels au sein de l'établissement, mais aussi à l'égard de ceux confiés à un tiers.
- Promouvoir le droit au respect de la vie privée et à la protection des renseignements personnels au sein de l'établissement.

Responsabilités du responsable de la protection des renseignements personnels

- Conseiller la direction de l'établissement en matière de protection des renseignements personnels.
- Siéger au Comité sur l'accès à l'information et sur la protection des renseignements personnels.
- Établir et mettre en œuvre les politiques et pratiques encadrant la gouvernance de l'établissement à l'égard des renseignements personnels et veiller à sa révision périodique.
- Participer à l'établissement de la position organisationnelle en matière de protection des renseignements personnels.
- Intervenir à toute étape d'une évaluation des facteurs relatifs à la vie privée d'un projet visant un système d'exploitation ou de prestation électronique de services impliquant des renseignements personnels.
- 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.
- Tenir les registres de communication de renseignements personnels, incluant en cas d'incident de confidentialité.
- Être avisé en cas d'incident de confidentialité survenu chez un mandataire ou chez l'exécutant d'un contrat de service ou d'entreprise. Procéder (seul ou avec les services concernés) à l'inventaire des contrats avec des fournisseurs, prestataires externes et, le cas échéant, les réviser.
- Effectuer toute vérification relative à la confidentialité des renseignements personnels confiés à un tiers.
- Répondre aux plaintes ainsi qu'aux demandes d'accès aux renseignements personnels et de rectification.
- Prêter assistance au demandeur pour comprendre la décision de lui refuser – en tout ou en partie – l'accès à un renseignement personnel ou la rectification de celui-ci.
- Mettre en place des formations et des mécanismes de sensibilisation à la protection des renseignements personnels au sein de l'établissement.
- Répondre aux demandes de la Commission d'accès à l'information.

Pour télécharger une version éditable de ce texte, cliquez ici

RESPONSABLE SECTEUR RESSOURCES INFORMATIQUES

FICHE DESCRITPTIVE

Rôle du responsable du secteur des ressources informatiques

- [Décrire son rôle en termes généraux]

Rôle des membres du secteur des ressources informatiques

- [Décrire son rôle en termes généraux]

Responsabilités du responsable et des membres du secteur des ressources informatiques

- Faire un audit des mesures de sécurité déployées par l'établissement, et ce, quel que soit le support des renseignements personnels.
- Élaborer, avec le Comité sur l'accès à l'information et la protection des renseignements personnels, un plan d'intervention en cas d'incident de confidentialité.
- Établir les modalités des permissions d'accès et les gérer en collaboration avec les services concernés.
- Participer à la réalisation de l'inventaire des politiques, procédures, directives en lien avec la sécurité des renseignements personnels et, le cas échéant, les réviser ou en adopter de nouvelles.
- Dresser un inventaire des technologies utilisées pour collecter, communiquer et conserver les renseignements personnels.
- Établir les procédures quant à la destruction, l'anonymisation et la dépersonnalisation des renseignements personnels.
- Mettre en place des formations et des activités de sensibilisation sur la sécurité des renseignements personnels et l'utilisation des ressources informatiques.

Pour télécharger une version éditable de ce texte, cliquez ici

RESPONSABLE SECTEUR RESSOURCES HUMAINES

FICHE DESCRITPTIVE

Rôle du secteur des ressources humaines

- [Décrire le rôle en termes généraux : embauche et collecte des renseignements bancaires des membres du personnel, gestion de la paie, vérification des antécédents judiciaires, convention collective, assurance].

Responsabilités du secteur des ressources humaines

- Dresser un inventaire des renseignements personnels détenus par chacun des services liés aux ressources humaines, et ce, quel que soit le support et la répartition ou la circulation de ceux-ci.
- Dresser un inventaire de la documentation transmise aux employés quant à la collecte, l'utilisation, la communication et la conservation des renseignements personnels et, le cas échéant, la réviser à la lumière des exigences de la Loi 25.
- Déterminer (revoir), de concert avec le secteur des ressources informatiques, les accès attribués à un employé, et ce, en fonction de son rôle au sein du secteur des ressources humaines.
  Mettre en œuvre les différentes politiques, procédures et directives déployées par [indiquer le nom de l'établissement] quant à la collecte, l'utilisation, la communication, la conservation et la sécurité.
- S'assurer que les employés attestent [indiquer la fréquence : annuellement, semestriellement] avoir pris connaissance des différentes politiques et procédures applicables en matière de protection des renseignements personnels.
- Mettre en œuvre les différentes politiques, procédures et directives déployées par [indiquer le nom de l'établissement] quant à la collecte, l'utilisation, la communication, la conservation et la sécurité.
- S'assurer de la formation des nouveaux employés en matière de sécurité informatique.
- S'assurer du maintien de de la formation continue en matière de sécurité informatique avec les employés.
- Réviser les consentements à l'utilisation et à la communication au moment de l'embauche.
- Réviser les contrats avec les fournisseurs de services et organismes à qui des renseignements personnels sont transmis.

Pour télécharger une version éditable de ce texte, cliquez ici

Processus de traitement des plaintes et des demandes d'accès

Au cours du parcours scolaire ou professionnel, il peut arriver qu'un élève, un titulaire de l'autorité parentale ou un employé dépose une plainte à l'égard de la gestion de ses renseignements personnels ou demande à avoir accès à ses renseignements personnels.

Les établissements d'enseignement privés doivent :

- Adopter ou réviser un processus de traitement des plaintes.
  - Déterminer et diffuser auprès de qui et comment les plaintes sont adressées à l'établissement.
    - Prévoir la procédure dans les cas où la plainte n'est pas adressée « au responsable des plaintes » afin qu'elle lui soit transmise.
  - Déterminer le délai de traitement d'une plainte.
  - Description des différentes étapes du traitement :
    - Réception et accusé de réception.
    - Évaluation de la plainte - prise de connaissance des documents et de la version des faits de chacune des parties.
    - Donner une réponse au plaignant : entente, mesures de redressement, fermeture du dossier.
  - Registre des plaintes / Rapport à la direction.
    - Comportant notamment l'identité et les coordonnées du plaignant et un descriptif de la plainte, des faits et de la solution apportée.

Note : Exemple de clause pouvant être inclus dans la politique de confidentialité du site Internet ou dans les procédures internes de l'établissement relatives à la protection des renseignements personnels :

Exemple de clause de processus de traitement des plaintes

La personne responsable de la protection des renseignements personnels reçoit les plaintes relatives à la protection de ceux-ci. Lorsqu'une telle plainte est déposée, la personne responsable de la protection des renseignements personnels en accuse

réception auprès de la personne concernée, prend connaissance de son contenu, enquête sur les circonstances et répond par écrit de manière diligente. Le cas échéant, elle peut formuler des recommandations permettant d'améliorer la protection des renseignements personnels.

Pour télécharger une version éditable de ce texte, cliquez ici

- Adopter ou réviser un processus de traitement des demandes d'accès
  - Diffuser auprès de qui et comment les demandes d'accès sont transmises à l'établissement.
    - Prévoir la procédure dans les cas où la demande n'est pas adressée « au responsable de la protection des renseignements personnels », afin qu'elle lui soit transmise.
  - Description des différentes étapes du traitement :
    - Réception.
    - Accusé de réception et réponse dans les 20 jours (+ possibilité de prolonger de 10 jours)[6].
      - Durant ce délai : examen de la demande et détermination des motifs de restriction ou de refus.
  - Registre des demandes d'accès.

Note : COMMISSION D'ACCÈS À L'INFORMATION
Demande de révision ou d'examen de mésentente – Repérage complet et sérieux des documents visés par une demande d'accès.

[6] Pour les établissements ou les activités assujetties à la Loi sur le secteur privé, le délai est de 30 jours.

Entête de l'établissement
[Ville, Date]

[Nom et coordonnées du destinataire]

INDIQUER LE MODE DE TRANSMISSION(Courriel, Lettre avec AR)

Objet : Demande d'accès

[Nom du destinataire],

Par la présente, nous vous informons que [nom de l'établissement] a reçu le [date] la demande d'accès de [nom du demandeur] (la « **Demande** ») visant à obtenir [préciser la nature des renseignements personnels demandés].

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, la « **Loi sur l'accès** »), prévoit que [nom de l'établissement] doit effectuer le traitement de la Demande dans un délai de vingt (20) jours suivant sa réception. Nous vous informons que des démarches ont été entreprises afin de retracer les documents visés par la Demande.

Dans l'éventualité où ce délai n'est pas respecté, vous avez le droit d'exercer, devant la Commission d'accès à l'information, le recours en révision prévu à la section III du chapitre IV de la Loi sur l'accès. Vous trouverez ci-joint les informations relatives à l'exercice de ce recours.

Veuillez agréer, [nom de destinataire], l'expression de mes sentiments distingués.

[Nom et titre du signataire]

p.j. Annexe – Avis de recours en révision

Pour télécharger une version éditable de ce texte, cliquez ici

RECOURS

L'article 135 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « **Loi sur l'accès** ») prévoit qu'une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit ; elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137 Loi sur l'accès).

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 de la Loi sur l'accès.

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135 Loi sur l'accès).

Les coordonnées de la Commission d'accès à l'information sont les suivantes :

Québec

Commission d'accès à l'information
Bureau 2.36
525, boul. René-Lévesque Est
Québec (Québec) G1R 5S9

Tél : (418) 528-7741
Téléc : (418) 529-3102

Montréal

Commission d'accès à l'information
Bureau 900
2045, rue Stanley
Montréal (Québec) H3A 2V4

Tél : (514) 873-4196
Téléc : (514) 844-6170

Sans frais : 1 888 528-7741
Courriel : cai.communications@cai.gouv.qc.ca

Pour télécharger une version éditable de ce texte, cliquez ici

Activités de formation et de sensibilisation

Compte tenu des modifications apportées à la Loi sur l'accès et à la Loi sur le secteur privé par la Loi 25, il revient aux établissements d'enseignement privés de former et de sensibiliser, notamment, les membres du personnel des exigences en matière de protection des renseignements personnels.

Il est prévu que les établissements mettent en place un document décrivant les activités de formation et de sensibilisation. Pour le moment, aucune précision n'est donnée quant aux éléments devant figurer dans ce document, toutefois celui-ci devrait notamment comprendre les éléments suivants :

- Date
- Titre de la formation ou de l'activité de sensibilisation
- Description de la formation ou de l'activité
- Public cible
- Formateur ou support utilisé

Pour télécharger une version éditable de ce tableau, cliquez ici

Sondage

Les établissements d'enseignement privés qui mettent en place des sondages doivent adopter des règles en la matière[7]. Ces règles doivent inclure :

- Les mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre du sondage, incluant le fait d'obtenir le consentement des personnes concernées si le sondage requiert la collecte de renseignements personnels.
- Une évaluation de la nécessité de recourir au sondage.
- Une évaluation de l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

Si le sondage est réalisé par un prestataire de services, un contrat doit être conclu pour préciser les obligations de chacune des parties en ce qui concerne les renseignements personnels qui seront recueillis et utilisés dans le cadre du sondage[8].

---

7 Cette exigence vise les établissements agréés aux fins de subvention en vertu de la Loi sur l'enseignement privé et les personnes qui les tiennent, à l'égard des 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. Toutefois, cela constitue une bonne pratique à adopter pour les établissements non agréés.

8 Loi sur l'accès, art. 67.2; Loi sur le secteur privé, art. 18.3.

Conservation et destruction

Tant la Loi sur l'accès que la Loi sur le secteur privé prévoient que lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, celui-ci doit être détruit ou anonymisé, sous réserve du délai de conservation prévu par une loi.

> Note : Voir le *Guide de gestion des archives à l'intention des établissements d'enseignements privés du Québec* préparé par la Fédération des établissements d'enseignement privés et transmis à Bibliothèques et Archives nationales (février 2016).
>
> COMMISSION D'ACCÈS À L'INFORMATION, *Destruction des documents contenant des renseignements personnels* (en cours de révision).

Gestion des incidents de confidentialité

Depuis le 22 septembre 2022, les établissements d'enseignement privés doivent aviser la Commission d'accès à l'information, 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.

> **Note :** Voir les outils mis à la disposition des établissements par la Fédération des établissements d'enseignement privés dans son document *Mise en place de la Loi 25 sur la protection des renseignements personnels – Foire aux questions* (dernière mise à jour : juin 2023).

De plus, il est recommandé aux établissements d'enseignement privés d'élaborer un plan d'intervention en matière de sécurité, incluant les incidents de confidentialité. Ce plan peut contenir les éléments présentés dans le modèle ci-après.

Modèle de plan d'action

Introduction

Contexte

Indiquer dans quel contexte le plan s'inscrit (Loi sur l'accès/Loi sur le secteur privé, directive/politique prise par l'établissement, etc.)

Objectif

Indiquer l'objectif du plan.

Proposition : *« Ce plan d'intervention a pour objectif d'identifier les intervenants, les étapes, les démarches et les actions requises en vue de s'assurer que les incidents impliquant les Renseignements personnels détenus par [Nom de l'établissement] soient traités de manière coordonnée, efficiente et rapide, afin d'atténuer les risques susceptibles d'en découler et d'apporter les correctifs nécessaires* ».

Définitions

- Incident de sécurité
  Incident qui affecte la confidentialité, la disponibilité ou l'intégrité des informations d'un système ou la continuité de service de [Nom de l'établissement], incluant ou non des renseignements personnels.
- Incident de confidentialité
  Accès, utilisation et communication non autorisé(e) par la loi d'un renseignement personnel, perte d'un tel renseignement ou toute autre atteinte à la protection de celui-ci.
- Renseignements personnels
  Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Champ d'application

Indiquer qui est visé par le plan.

Responsabilité

Indiquer qui veille au respect du plan : identifier la personne responsable de la mise en œuvre du Plan au sein de l'établissement.

Équipe de réponse en cas d'incident de sécurité et/ou de confidentialité

Préciser qui sont les membres de l'équipe de réponse au sein de l'établissement, le rôle et les responsabilités de chacun et préciser qui contacter, à l'interne et à l'externe, en cas d'incident (par exemple : assureurs).

Idéalement, identifier les ressources externes que l'établissement pourrait mandater pour l'assister en cas d'incident : conseillers juridiques, experts en cybersécurité, cabinet de relations publiques, etc.

Proposition : Présenter l'information sous forme de tableau.

Rôle	Nom	Titre	Téléphone	Courriel
Interne				
Responsable de la gestion des incidents				
Responsable de la protection des renseignements personnels				
Responsable TI / sécurité				
Service juridique (peut être à l'externe)				
Communication (peut être à l'externe)				
Etc.				
Externe				
Assureur				
Expert TI (externe)				
Fournisseur(s) de service				
Commission d'accès à l'information				
Etc.				

Étapes et démarches en cas d'incident de sécurité ou de confidentialité

Indiquer les différentes étapes du plan d'intervention. Les étapes présentées ci-dessous le sont à titre indicatif, chaque établissement d'enseignement privé peut en ajouter notamment celles développées en matière de sécurité.

Identifier, circonscrire, enquêter

Implication immédiate de l'équipe de gestion des incidents
Communiquer avec le coordonnateur de l'équipe de gestion des incidents de sécurité, qui verra à mettre en œuvre le plan d'intervention et à impliquer les membres de l'équipe et toute autre personne susceptible d'aider à diminuer le risque.

Identifier l'incident
Sous la direction de l'équipe de gestion des incidents, l'établissement doit tout d'abord identifier l'incident concerné, dans la mesure du possible. À cette fin, il doit déterminer et documenter :

- La cause et l'origine de l'incident (date, heure, lieu, support, cause interne ou externe, personne responsable, déterminer si l'incident est terminé ou en cours)
- Les renseignements visés (personnels ou non), leur nombre et les personnes concernées.

Circonscrire l'incident
L'établissement doit entreprendre immédiatement des mesures pour contenir les effets de l'incident et prévenir des impacts négatifs additionnels pour lui ou des tiers. Les mesures entreprises devraient être documentées. La nature de ces mesures dépendra du type d'incident en cause. Ainsi, on ne réagira pas de la même manière à une cyber-attaque qu'à un courriel transmis par erreur à un mauvais destinataire.

À cette étape, l'établissement pourra notamment considérer les éléments suivants :

- Contenir la menace par le confinement ou l'isolement des composants affectés
- Modifier (révoquer) les accès et mots de passe si requis
- Identifier, localiser et préserver les renseignements visés par l'incident
- Protéger la confidentialité des renseignements personnels visés
- Récupérer les renseignements personnels ou les supports – obtenir une confirmation de destruction ou de non-diffusion du responsable de l'incident
- Empêcher la diffusion ou la divulgation des renseignements – chiffrement, blocage des accès
- Conserver tous les documents en place au moment de l'incident sans les modifier, notamment pour préserver la preuve

Enquêter sur l'incident
Une fois que l'établissement a identifié et contenu l'incident, une enquête plus approfondie doit être effectuée pour déterminer et documenter, aussi précisément que possible :

- La cause et l'origine de l'incident ;
- Les renseignements visés (personnels ou non) ainsi que leur nombre ;
- Les personnes visées, le cas échéant, et leur emplacement géographique ;
- Le risque de préjudice pour les personnes concernées selon la grille d'analyse du préjudice.

Communiquer

L'établissement doit mettre en place un protocole, tant à l'interne qu'à l'externe, pour communiquer sur l'incident de confidentialité.

Plan de communication interne

- Aviser le personnel
  - Insister sur le fait que l'incident n'a pas encore été révélé à l'externe
  - Indiquer jusqu'à quelle date il y a un embargo
  - Etc.

Plan de communication externe

- Avis aux autorités (Commission d'accès à l'information ou autres autorités réglementaires pertinentes, service de police, etc.)
- Avis aux personnes concernées
  - Si l'établissement décide de ne pas le faire, documenter les raisons ayant conduit à cette décision.
- Avis aux médias ou communiqué de presse
- Etc.

Rencontrer les répondants du centre d'appels

Etc.

Continuité des activités et Suivi (sur une base régulière)

L'établissement doit préciser les éléments qui seront pris en considération pour continuer les activités mais aussi afin pour faire un suivi (post-mortem) sur l'incident pour éviter que pareille situation ne se reproduise.

Plan de continuité des activités

- Effectuer un post-mortem pour identifier et examiner les leçons tirées de l'incident ainsi que les domaines à améliorer

Plan de surveillance

- Faire un suivi interne des mesures de sécurité, des politiques et procédures adoptées ou révisées à la suite de l'incident
- Possibilité de faire appel à un audit externe pour évaluer les mesures de sécurité ; politiques et procédures adoptées ou révisées à la suite de l'incident
- Considérer la mise en place d'un service de surveillance de crédit (Équifax, TransUnion, par ex.)

Plan juridique

- Prévoir la stratégie pour réduire le risque de poursuite judiciaire et la stratégie de défense en cas de poursuite judiciaire
- Enregistrer l'incident dans le registre des incidents de confidentialité
- Revoir la couverture d'assurance

Plan de gestion de la réputation et de la communication

- Formation, sensibilisation
- Communication pour reconstruire la confiance tant à l'interne qu'à l'externe

Pour télécharger une version éditable de ce texte, cliquez ici

Évaluation des facteurs relatifs à la vie privée

Depuis le 22 septembre 2022, mais surtout à partir du 22 septembre 2023, les établissements d'enseignement privés doivent ou devront réaliser des évaluations de facteurs relatifs à la vie privée (« EFVP ») dans les situations suivantes :

- *Septembre 2022*
  - Lors de la communication de 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**[9].
- *Septembre 2023*
  - Lors d'un **projet d'acquisition, de développement ou de refonte** d'un système d'information ou de prestation électronique de services impliquant des renseignements personnels[10].

    Note : La mise à jour d'un système d'information ou de prestation électronique n'est pas visée par cette exigence, sauf si la mise à jour à une incidence importante sur la protection des renseignements personnels.
  - Lors de la **communication à l'extérieur du Québec** de renseignements personnels ou lorsque la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte de tels renseignements est confiée à une personne ou à un organisme à l'extérieur du Québec[11].
  - Lors de la **collecte** de renseignements personnels nécessaires à l'**exercice des attributions ou à la mise en œuvre d'un programme** d'un organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune[12].
  - Lors de la communication de renseignements personnels sans le consentement des personnes concernées, conformément à l'**article 68 de la Loi sur l'accès**.

Une EFVP, c'est quoi ?

Selon la Commission d'accès à l'information, une EFVP:

---

9 Loi sur l'accès, art. 67.2.1 et suiv.; Loi sur le secteur privé, art. 21 et suiv.

10 Loi sur l'accès, art. 63.5; Loi sur le secteur privé, art. 3.3. Voir GOUVERNEMENT DU QUÉBEC, *Outil de réflexion : Conception d'un système d'information ou de prestation électronique de services*.

11 Loi sur l'accès, art. 70.1 tel que modifié par la Loi 25; LPRPSP, art. 17 tel que modifié par la Loi 25.

12 Loi sur l'accès, art. 64 tel que modifié par la Loi 25.

> « est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées. […] Ce processus vise d'abord à protéger les personnes physiques concernées par ces renseignements. Il vise aussi la mise en place de mesures adéquates pour respecter [les] obligations en matière de protection des renseignements personnels. Ainsi, l'EFVP permet d'éviter les problèmes que causerait une gestion inadéquate (plaintes, incidents de sécurité, poursuites judiciaires, atteinte à l'image, etc.). »[13]

Une EFVP, quand la réaliser ?

Quelle que soit la situation pour laquelle un établissement d'enseignement privé doit procéder à une EFVP, celle-ci doit être **réalisée avant** la communication, la collecte ou encore la réalisation du projet de d'acquisition, de développement ou de refonte.

Une EFVP, quels sont les éléments à considérer ?

Même si chacune des situations dans laquelle une EFVP doit être réalisée requiert une EFVP spécifique, il est néanmoins permis de considérer qu'**une EFVP doit être proportionnée** et tenir compte :

- De la **sensibilité** des renseignements personnels ou encore de leur nature ou de leur type
- De la **finalité** de leur utilisation
- De leur **quantité**, leur **répartition** et leur **support**
- Des **mesures de protection** en place incluant, dans le cas des communications à l'extérieur du Québec, l'analyse du régime juridique applicable dans l'État où les renseignements personnels seront communiqués

En plus de réaliser une EFVP, un établissement d'enseignement privé doit, dans certains cas :

- Consulter **le comité sur l'accès à l'information et la protection des renseignements personnels ou le responsable de la protection des renseignements personnels**. Il en va ainsi pour tout projet d'acquisition, de développement ou de refonte[14];
- Conclure **une entente** pour toute :
  - Communication à l'extérieur du Québec ou collecte de renseignements personnels nécessaires à l'exercice des attributions ou à la mise en œuvre d'un programme;
  - Communication de renseignements personnels à des fins d'étude, de recherche, de production de statistiques ou encore dans les cas de l'article 68 de la Loi sur l'accès. Dans ces cas, l'entente devra être transmise à la Commission d'accès à l'information.

---

13 COMMISSION D'ACCÈS À L'INFORMATION, *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privée*, mars 2021 (en révision).

14 Loi sur l'accès, art. 63.5 et 63.6; Loi sur le secteur privé, art. 3.3.

Enfin, les résultats de l'EFVP doivent faire l'objet d'un rapport qui pourra contenir les éléments suivants :

Éléments évalués	
Quel est le projet ? Quelle est sa finalité ? ► Étude, recherche, production de statistiques ► Acquisition, développement, refonte ► Communication hors Québec ► Exercice des attributions/mise en œuvre ► Communication en vertu de la Loi sur l'accès	
Quels sont les renseignements personnels nécessaires pour réaliser le projet ? ► Nom, Prénom ► Adresse (postale, courriel, IP, …) ► Numéro de téléphone ► NAS ► Renseignements démographiques ► Etc	
Quel est le niveau de sensibilité des renseignements personnels ? ► *Si renseignement sensible* – un consentement manifesté de manière expresse a-t-il été obtenu ?	
Comment les renseignements personnels sont-ils recueillis ?	
Quelles sont les personnes qui auront accès aux renseignements personnels ? ► Au sein de l'établissement ► À l'extérieur de l'établissement	
Sur quel(s) support(s) les renseignements personnels sont conservés ? hébergés ?	
Les renseignements sont-ils communiqués ou confiés à l'extérieur du Québec ?	

► *Si oui*- Quels sont les éléments pris en considération pour évaluer l'adéquation du pays destinataire des renseignements personnels ?	
Un contrat a-t-il été conclu avec le fournisseur de service externe ? ► *Si oui*, une clause doit être prévue à l'égard des sous-traitants, des obligations de chacune des parties, des obligations en matière d'assurance et d'audit notamment	
Quelles sont les mesures de sécurité mises en place pour assurer la protection des renseignements personnels ?	
Quels sont les risques identifiés ? et quelles sont les probabilités qu'ils se réalisent ?	
Quelles sont les mesures prises pour minimiser les risques pour les personnes concernées ?	
Quels sont les moyens et les stratégies mis en place pour assurer le respect des obligations et des principes de protection des renseignements personnels ?	
Quelles sont les mesures prises en lien avec la conservation et la destruction des renseignements personnels ?	
Est-ce qu'un processus de vérification et de correction des renseignements personnels est prévu ?	
Quel est le suivi prévu ? Par qui ?	

Pour télécharger une version éditable de ce texte, cliquez ici

Politique de confidentialité

À compter du 22 septembre 2023, les établissements d'enseignement privés qui recueillent par un moyen technologique des renseignements personnels devront publier sur leur site Internet et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs[15].

Il est prévu qu'un règlement du gouvernement détermine le contenu et les modalités de cette politique. En attendant un tel règlement, il est permis de considérer que les éléments en lien avec les informations devant être fournies aux personnes concernées lors de la collecte, sur demande ou encore le cas échéant [16] doivent minimalement être dans la politique de confidentialité, soit :

- Une description des renseignements personnels qui seront recueillis, notamment par le biais du site Internet
- Les fins pour lesquelles les renseignements sont recueillis
- Les moyens par lesquels les renseignements sont recueillis
- Les catégories de personnes qui y auront accès tant à l'intérieur qu'à l'extérieur de l'organisation
- 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

[15] Loi sur l'accès, art. 63.4 ; Loi sur le secteur privé, art. 8.2.

[16] Loi sur l'accès, art. 65 et suiv. ; Loi sur le secteur privé, art. 8 et suiv. Voir GOUVERNEMENT DU QUÉBEC, « Politique de confidentialité ».

Il convient de préciser que la politique de confidentialité publiée sur le site Internet des établissements peut différer des politiques et procédures adoptées pour encadrer, à l'interne, le cycle de vie des renseignements personnels.

Politique de confidentialité (Site Internet)

[Nom de l'établissement] reconnaît l'importance de la confidentialité et de la sensibilité des renseignements personnels qu'il recueille par le biais de son site Web ou de toute autre plateforme utilisée pour présenter son offre de service scolaire.

La présente *Politique de confidentialité* explique quels renseignements personnels sont resueillis auprès de vous et à quelle(s) fin(s).

Renseignements personnels recueillis

[Préciser ici l'ensemble des renseignements personnels recueillis. Il y a possibilité de présenter les renseignements en lien avec les moments de la vie scolaire où ils sont collectés (lors de l'inscription nous recueillons : […], lorsque vous naviguez sur notre site Internet, nos plateformes : […] ; lorsque vous utilisez le bouton « contact » : […] ; etc.)]

Finalité de la collecte et moyens

Nous utilisons les renseignements recueillis uniquement pour atteindre les objectifs décrits ci-dessous.

[Préciser les objectifs : identification, inscription, formation, mesurer l'audience, gestion des services scolaires, fourniture ou livraison d'une prestation de service ; communiquer avec vous, etc.]

Utilisation et Communication des renseignements

[Nom de l'établissement] s'assure que les employés mais aussi les tiers avec qui il fait affaire [indiquer les tiers ou les catégories de tiers] protègent la confidentialité des renseignements personnels auxquels ils ont accès, et ce, quel que soit le support sur lequel ils sont accessibles.

Nous ne les utiliserons, ni ne les communiquerons à d'autres fins que celles mentionnés sans votre consentement, sauf si cela est requis ou permis par la loi.

Durée de conservation et mesures de sécurité

Sauf autorisation ou exigence des lois applicables, [Nom de l'établissement] ne conserve vos renseignements personnels que le temps nécessaire pour atteindre les fins pour lesquelles elles ont été collectées, y compris aux fins de satisfaire aux exigences légales, comptables ou en matière d'avis aux instances gouvernementales appropriées.

Lorsque l'utilisation prévue est terminée, vos renseignements personnels sont détruits, supprimés ou anonymisés, sauf si la loi nous oblige à les conserver. Les renseignements anonymisés ne permettent plus de vous identifier.

[Nom de l'établissement] met en place des mécanismes de sécurité rigoureux pour protéger vos renseignements personnels contre la perte ou le vol et contre l'accès, la divulgation, la copie, l'utilisation ou la modification non autorisés.

Les sous-traitants ayant accès aux renseignements personnels dont [Nom de l'établissement] a la garde ou le contrôle seront informés de la présente politique et des autres politiques et processus applicables pour assurer la sécurité et la protection des renseignements personnels. Tous les sous-traitants devront accepter de se conformer aux politiques et aux processus et aux lois avant de commencer leur mandat pour [Nom de l'établissement].

Accès, rectification- Retrait du consentement- Plainte à l'égard de vos renseignements personnels

Vous pouvez consulter les renseignements que nous détenons à votre sujet. Si vous y constatez des erreurs, vous pouvez demander leur correction.

Vous pouvez également retirer votre consentement à l'utilisation et à la communication de vos renseignements personnels ou encore porter plainte quant à la protection de vos renseignements personnels.

Pour exercer vos droits, contactez-nous par courriel ou par la poste aux coordonnées indiquées au bas de cette page.

Nous contacter

Vous pouvez communiquer avec nous au sujet de la présente Politique de confidentialité ou encore pour exercer vos droits en vous adressant à [indiquer le titre et les coordonnées du responsable de la protection des renseignements personnels].

Pour télécharger une version éditable de ce texte, cliquez ici

Modèles supplémentaires

Afin de répondre à certaines préoccupations formulées par plusieurs établissements d'enseignement privés, nous vous proposons de modèles pour ce qui est des éléments suivants :

- Engagement à la confidentialité d'un membre du personnel
- Consentement à la communication de renseignements personnels à la Fondation d'un établissement d'enseignement privé

Engagement à la confidentialité d'un membre du personnel

Dans le cadre de mes fonctions au sein du [indiquer le nom de l'établissement], je peux avoir accès à des renseignements personnels [indiquer à propos de qui: élèves, titulaires de l'autorité parentale, employés, fournisseurs de services]. Ces renseignements doivent être collectés, utilisés, communiqués et conservés conformément aux exigences de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

À ce titre, je, soussigné-e [indiquer le nom du membre du personnel], m'engage à respecter la confidentialité des renseignements personnels auxquels j'aurai accès dans le cadre de mes fonctions.

Je confirme avoir pris connaissance de la documentation qui m'a été remise à mon arrivée [indiquer les différents documents remis à l'employé en lien avec la protection des renseignements personnels et, le cas échéant, les formations qu'il doit suivre- éventuellement prévoir une case à cocher à côté de chacun des documents], et m'engage à respecter les principes et obligations énoncés dans cette documentation.

Plus particulièrement, je m'engage [la liste n'est donnée qu'à titre indicatif]:

- À accéder aux seuls renseignements personnels nécessaires à l'exercice de mes fonctions;
- À utiliser ces renseignements que dans le cadre de mes fonctions;
- À ne révéler aucun renseignement personnel dont j'aurai eu connaissance dans le cadre de mes fonctions, sauf à y être dument autorisé-e et, cet engagement vaut aussi bien pendant mon embauche qu'à la suite de celle-ci;

- À informer sans délai mon supérieur et/ou la personne responsable de la protection des renseignements personnels de toute situation qui pourrait compromettre de quelque façon que ce soit la sécurité, l'intégrité ou la confidentialité des renseignements personnels détenus par [indiquer le nom de l'établissement];

J'ai signé, ce [date]

Nom et matricule de l'employé, Signature

** Une copie de ce document est conservée au dossier de l'employé détenu par la Direction des ressources humaines.*

Pour télécharger une version éditable de ce texte, cliquez ici

Consentement pour la communication de renseignements personnels à la Fondation d'un établissement d'enseignement privé

Pour réaliser sa mission, la [indiquer le nom de la Fondation] doit pouvoir communiquer avec vous. Pour ce faire, elle souhaite avoir accès à vos renseignements personnels [préciser lesquels] afin de pouvoir de pouvoir vous faire parvenir [indiquer les fins : par ex. transmission d'une infolettre, du programme des activités].

► Je consens à ce que [Nom de l'établissement] transmette les renseignements ci-dessus mentionnés à [indiquer le nom de la Fondation].

Pour télécharger une version éditable de ce texte, cliquez ici