2023

Règles de gouvernance en matière de renseignements personnels

COLLÈGE D'ANJOU

11/10/2023

Table des matières

Préambule et Loi 25

En septembre 2021, la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (« 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 que dans la Loi sur la protection des renseignements personnels dans le secteur privé.

Rôles et responsabilités

Responsable de la protection des renseignements personnels
M. Frédéric Desjardins
Directeur général

Rôles

- 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 de la protection des renseignements personnels au sein de l'établissement.

Responsabilités

Dans l'accomplissement de ses responsabilités, le responsable de la protection des renseignements personnels peut déléguer l'entièreté ou une partie des responsabilités tout en conservant l'autorité décisionnelle :

- Conseiller 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.
- En collaboration avec le service informatique, tenir les registres de communications de renseignements personnels, incluant en cas d'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.
- Procéder (seul ou avec les services concernés) à l'inventaire des contrats avec des fournisseurs, prestataires externes et, le cas échéant, les réviser.
- Répondre aux demandes d'accès aux renseignements personnels, de rectification, aux plaintes.
- Prêter assistance au demandeur à comprendre la décision de lui refuser, en tout ou en partie, l'accès ou la rectification d'un renseignement personnel.
- Mettre en place des formations, 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.

Rôles et responsabilités

Service informatique
M. Maxime Leclerc-Valade
Analyste informatique

Rôles du responsable

- Au niveau du système informatique, 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.
- Toujours au niveau des technologies de l'information, promouvoir le droit au respect de la vie privée et de la protection des renseignements personnels au sein de l'établissement.

Responsabilités

- Faire un audit des mesures de sécurité déployées par le Collège, 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.
- S'assurer de la formation des nouveaux employés en matière de sécurité informatique et du maintien de la formation continue.
- Réviser les consentements à l'utilisation et à la communication au moment de l'embauche.

Rôles et responsabilités

Comité Loi 25

Messieurs Frédéric Desjardins et Maxime Leclerc-Valade

Rôles

- 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 (PRP).
- 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 service impliquant 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 lié à l'embauche et à la gestion des ressources humaines.
- Promouvoir le droit au respect de la vie privée et de la protection des renseignements personnels au sein de l'établissement.

Responsabilités

- Effectuer toute vérification relative à la confidentialité des renseignements personnels confiés à un tiers.
- Mettre en place des formations, des mécanismes de sensibilisation à la protection des renseignements personnels au sein de l'établissement.
- Mettre en place des formations et des activités de sensibilisation sur la sécurité des renseignements personnels et l'utilisation des ressources informatiques.
- Dresser un inventaire des renseignements personnels détenus par chacun des services.
- Approuver des règles de gouvernance du Collège d'Anjou.
- Être consulté, dès le début d'un projet impliquant des renseignements personnels et aux fins de l'évaluation des facteurs relatifs à la vie privée, pour tous les projets d'acquisition, de développement et de refonte d'un système d'information ou d'une prestation électronique de services impliquant des renseignements personnels. Le comité peut également suggérer, à toutes les étapes du projet :
    - La nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels.
    - Des mesures de protection des renseignements personnels dans les documents relatifs au projet, comme un cahier des charges ou un contrat.
    - Une description des responsabilités des participants au projet en matière de protection des renseignements personnels.

    - La tenue d'activités de formation sur la protection des renseignements personnels pour les participants.
- 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 les services 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 le Collège d'Anjou quant à la collecte, l'utilisation, la communication, la conservation et la sécurité.
- S'assurer que les employés attestent annuellement avoir pris connaissance des différentes politiques et procédures applicables en matière de protection des renseignements personnels.
- En collaboration avec les directeurs réviser les contrats avec les fournisseurs de services et organismes à qui des renseignements personnels sont transmis.
- En collaboration avec le responsable de la protection des renseignements personnels, tenir les registres de communications de renseignements personnels, incluant en cas d'incident de confidentialité.
- Effectuer toute vérification relative à la confidentialité des renseignements personnels confiés à un tiers.

Rôles et responsabilités

L'ensemble des membres du personnel du Collège d'Anjou

Rôles

- 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 de la protection des renseignements personnels au sein de l'établissement.

Responsabilités

- S'assurer de recevoir uniquement les renseignements personnels et données sensibles nécessaires à leur fonction.
- Respecter le cycle de vie des renseignements personnels jusqu'à leur destruction.
- Informer les responsables s'ils font ou subissent une erreur en matière de renseignements personnels et données sensibles.
- Participer activement à la prévention de la protection des renseignements personnels.
- Se faire discret quant à la collecte, l'utilisation et la transmission des renseignements personnels.
- Informer les responsables de tous nouveaux fournisseurs externes qui doivent transiger avec des renseignements personnels et s'assurer que ceux-ci consentent à respecter la Loi 25.
- Permettre, aux parents et élèves, tous consentements éclairés dans le cas d'un partage nécessaire ou d'une relatif à un renseignement personnel.

Traitement des plaintes

Au Collège d'Anjou, un élève, un titulaire de l'autorité parentale ou un employé peut déposer une plainte à l'égard de la gestion de ses renseignements personnels ou demande à avoir accès à ses renseignements personnels. La personne responsable de la protection des renseignements personnels s'occupe également du traitement des plaintes.

Voici la procédure à suivre lors d'un traitement des plaintes :

1- La plainte doit être envoyée par courriel au responsable de la protection des renseignements personnels (dg@collegedanjou.com). Dans le cas où une autre personne de l'organisation reçoive une plainte, celle-ci devra être acheminée dans les plus brefs délais au responsable.
2- Le responsable en accusera réception et répondra par la suite, dans les 20 jours (un délai de 10 jours supplémentaires pourrait s'appliquer selon le cas). Lors de cette période, il prendra connaissance de son contenu, mènera son enquête sur les circonstances et répondra par écrit au plaignant. Le cas échéant, il peut formuler des recommandations permettant d'améliorer la protection des renseignements personnels.
3- S'il s'agit d'un incident, enregistrer l'incident au registre.

Demandes d'accès

Pour toute demande d'accès à l'information, voici les étapes à suivre :

1- La demande doit être envoyée par courriel au responsable de l'accès et de la protection des renseignements personnels (dg@collegedanjou.com). Dans le cas où une autre personne de l'organisation reçoive la demande, celle-ci devra être acheminée dans les plus brefs délais au responsable.

2- Le responsable en accusera réception et répondra par la suite, dans les 20 jours (pour les établissements assujettis à la Loi sur le secteur privé, le délai possible est de 30 jours). Si la demande est refusée, les motifs ou restrictions vous seront annoncés brièvement. Au moindre doute, il convient de communiquer avec le demandeur afin qu'il précise sa demande ou identifie les documents susceptibles de contenir les renseignements recherchés. Une demande d'accès vague et imprécise ne peut constituer un motif pour refuser de la traiter. Si la demande est acceptée, les étapes suivantes seront mises de l'avant :

   - L'analyse de la demande
   - La réponse au demandeur
   - Le repérage des documents
   - La conservation des démarches effectuées
   - L'analyse des documents

3- La demande sera enregistrée au registre des demandes d'accès.

Sondage et cybersécurité

SONDAGE

Le Collège d'Anjou s'engage à respecter les règles suivantes lors de la mise en place de différents sondages :

- Prendre toutes mesures de protection à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage, incluant le fait d'obtenir le consentement des personnes concernées si le sondage requiert la collecte de renseignements personnels.
- Évaluer la nécessité de recourir au sondage.
- Tenter d'anonymiser le sondage, lorsque possible.
- Évaluer 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 fournisseur externe (ou un prestataire de services), un contrat sera conclu afin de préciser les obligations de chacune des parties en ce qui concerne les renseignements personnels qui seront recueillis et utilisés dans le cadre du sondage.

CYBERSÉCURITÉ

Le Collège d'Anjou s'engage à mettre toutes les mesures en place afin de protéger les renseignements personnels des personnes utilisant notre communauté informatique.

Il veillera notamment à :

- Surveiller l'infrastructure informatique.
- Protéger les données de l'entreprise.
- Assurer la sécurité du réseau et des terminaux.
- Optimiser la prévention en matière de cyberpiraterie.
- Collaborer avec les différents fournisseurs pour la gestion sécuritaire de nos outils informatiques.

Les renseignements personnels sont accessibles seulement aux membres du personnel qui doivent y avoir accès dans le cadre de leurs fonctions.

Conservation et destruction

En ce qui concerne la conservation et la destruction d'un renseignement personnel, la Loi sur l'accès et 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.

À ce sujet, le Collège d'Anjou se réfère au Guide de gestion des archives à l'intention des établissements d'enseignement privés du Québec préparé par la Fédération des établissements d'enseignement privés et transmis à Bibliothèques et Archives nationales (février 2016) ainsi qu'à la Commission d'accès à l'information.

Gestion des incidents

En cas d'incident de confidentialité, le Collège d'Anjou, conformément aux lois s'y rattachant, s'engage à :

- Inscrire l'incident au registre prévu à cet effet.
- Évaluer les facteurs de risque en matière de vie privée et/ou vol d'identité.
- Informer la Commission d'accès à l'information et les personnes concernées, en cas d'incident présentant un risque de préjudice sérieux.
- Corriger les lacunes afin que l'incident ne se répète pas.

Un plan d'intervention en matière de sécurité, incluant les incidents de confidentialité, a été mis en place. Celui-ci comprend l'introduction de l'incident, l'équipe de réponse en cas d'incident et les différentes étapes et démarches à effectuer pour la gestion de l'incident.

Si vous êtes victime d'un incident de sécurité et/ou de confidentialité, vous devez d'abord communiquer par écrit avec le responsable, M. Frédéric Desjardins, à l'adresse suivante : dg@collegedanjou.com

L'équipe de réponse, en cas d'incident, est composée des personnes suivantes :

Rôle	Nom	Titre	Courriel
Responsable de la protection des renseignements personnels	Frédéric Desjardins	Directeur général	dg@collegedanjou.com
Responsable de la gestion des incidents	Frédéric Desjardins	Directeur général	dg@collegedanjou.com
Responsable TI/sécurité	Maxime Leclerc-Valade	Analyste informatique	mleclerc@collegedanjou.com

Avec diligence, confidentialité, et en cas de besoin, le Collège d'Anjou se réserve le droit de discuter d'un incident avec les membres du Comité Loi 25 ou de prendre un avis juridique auprès d'une firme d'avocats / conseils ou auprès de la Commission d'accès.

Évaluation des facteurs relatifs à la vie privée

Selon la Commission d'accès à l'information, une évaluation de facteurs relatifs à la vie privée (EFVP) se définit comme suit :

« 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.). »

Le Collège d'Anjou s'engage à réaliser, au préalable, des évaluations de facteurs relatifs à la vie privée (EFVP) lors des situations suivantes :

- 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. ***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. Si nécessaire, la EFVP sera suivie d'une entente pour conclure toute communication à l'extérieur du Québec, concernant des renseignements personnels.
- 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.
- Lors de la communication de renseignements personnels sans le consentement des personnes concernées, conformément à **l'article 68 de la Loi sur l'accès**. Dans le cas d'une étude, d'un projet de recherche ou de production de statistiques, une entente devra être conclue et transmise à la Commission d'accès à l'information.

Lorsque le Collège doit effectuer une EFVP, celle-ci peut être proportionnée, mais doit tenir compte de :

- 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.