



Directive sur la protection des renseignements personnels

Responsabilité de gestion :	Direction des ressources humaines et des affaires corporatives		
Date d'approbation :	2025-09-02		
☐ C.A.	☐ C.E.	☒ Direction générale	
Date d'entrée en vigueur :	2025-09-02	Référence :	DIR-
Date de révision :			

Table des matières

1	PRÉAMBULE.....	3
2	DÉFINITIONS.....	3
3	CADRE JURIDIQUE ET CHAMP D'APPLICATION	5
4	RÔLES ET RESPONSABILITÉS.....	5
5	COLLECTE DES RENSEIGNEMENTS PERSONNELS	7
6	GESTION DU CONSENTEMENT	8
7	OBSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS	10
8	DEMANDE D'ACCÈS OU DE RECTIFICATION À DES RENSEIGNEMENTS PERSONNELS.....	10
9	GESTION DES INCIDENTS DE CONFIDENTIALITÉ.....	12
10	TRAITEMENT DES INCIDENTS DE CONFIDENTIALITÉ.....	12
11	PROCESSUS DE TRAITEMENT DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	13
12	VIDÉOSURVEILLANCE	13
13	PROJETS DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS.....	14
14	ACTIVITÉS DE FORMATION ET DE SENSIBILISATION À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS OFFERTES PAR LE CÉGEP À SON PERSONNEL.....	14

15	SANCTIONS APPLICABLES EN CAS DE NON-RESPECT DE LA DIRECTIVE	14
16	ENTRÉE EN VIGUEUR	15
	ANNEXE 1 – PROPOSITION DE FORMULAIRE D'ENGAGEMENT DE CONFIDENTIALITÉ	16
	ANNEXE 2 – PROPOSITION DE FORMULAIRE DE CONSENTEMENT PRÉALABLE À LA DIVULGATION DES RENSEIGNEMENTS PERSONNELS.....	17
	ANNEXE 3 – PROPOSITION DE FORMULAIRE DE PLAINTÉ - PROTECTION DES RENSEIGNEMENTS PERSONNELS .	18
	ANNEXE 4 - LIGNES DIRECTRICES POUR LA MISE EN ŒUVRE DU PROCESSUS D'ANONYMISATION DES RENSEIGNEMENTS PERSONNELS.....	19
	ANNEXE 5 – PROCÉDURE DE TRAITEMENT DES DEMANDES D'ACCÈS A DES RENSEIGNEMENTS PERSONNELS INFORMATISÉS - PORTABILITÉ.....	21
	ANNEXE 6 - MODÈLE DE REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ	23

La Directive doit être lue en concomitance avec la *Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*.

1 PRÉAMBULE

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*¹ (ci-après la « Loi 25 »), promulguée le 22 septembre 2022, actualise l'encadrement applicable à la protection des renseignements personnels, dont la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*² (ci-après la « Loi sur l'accès »).

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* octroie aux personnes le droit à la protection de leurs renseignements personnels détenus par les organismes publics, ainsi ces derniers ont plusieurs obligations et responsabilités.

La présente Directive³ vise à encadrer les règles de gouvernance à l'égard de la protection des renseignements personnels que le Cégep détient, en complément de la [Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques](#).

2 DÉFINITIONS

Cette directive utilise plusieurs termes juridiques. Pour en faciliter la lecture et la compréhension, une brève définition de ces termes est fournie ci-dessous. Toutefois, ces définitions ne remplacent pas les définitions légales officielles. En cas de doute, il convient de se référer à la loi. Dans la présente Directive, les expressions suivantes signifient :

Actifs informationnels :	L'actif informationnel peut inclure une banque d'information électronique, un système d'information, une technologie de l'information ou une installation, ou encore un ensemble de ces éléments acquis ou constitués par une entreprise ou une organisation.
Anonymisation :	Les renseignements personnels (RP) peuvent être anonymisés lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies. Un renseignement personnel (RP) est anonymisé lorsqu'il ne permet plus d'identifier directement ou indirectement cette personne, en tout temps et dans toute circonstance. Le processus d'anonymisation doit être irréversible.
Collecte des renseignements :	Action de recueillir des renseignements personnels auprès de la personne concernée ou auprès d'un tiers, ou de générer ou d'inférer, par différents moyens, de tels renseignements à partir d'autres renseignements concernant cette personne.
Communication des renseignements :	La communication d'un renseignement personnel inclut toute divulgation de celui-ci à une personne, qu'il s'agisse de la communication d'un

¹ *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, L.Q. 2021, c. 25

² *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1

³ La Directive doit être lue en concomitance avec la Politique.

document contenant le renseignement personnel, de l'accès qui est accordé ou de sa divulgation totale.

Comité sur l'accès à l'information et la protection des renseignements personnels :

Afin de soutenir la personne responsable de l'accès à l'information et la protection des renseignements personnels, un comité sur l'accès à l'information et la protection des renseignements personnels est institué au sein du Cégep. La direction générale doit en nommer les membres conformément à la Loi sur l'accès.

Évaluation des facteurs relatifs à la vie privée (EFVP) :

Démarche préventive qui vise à mieux protéger les renseignements personnels et à respecter davantage la vie privée des personnes physiques en effectuant une analyse des risques d'atteinte à la vie privée⁴. Cette démarche doit se faire pour tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels; et avant de communiquer un renseignement personnel à l'extérieur du Québec ou avant de communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques.

Incident de confidentialité :

Un accès, une utilisation ou une communication non autorisée par la Loi sur l'accès d'un renseignement personnel, la perte d'un tel renseignement ou toute autre atteinte à la protection d'un tel renseignement.

Portabilité :

La portabilité réfère à la possibilité pour toute personne, d'obtenir la communication, dans un format technologique structuré et couramment utilisé, des renseignements personnels informatisés qu'elle a fournis à un organisme public, par exemple lors d'une prestation électronique de services.⁵

Proche parent :

Cette expression inclut les ascendants et les descendants directs, mais peut également inclure les frères et les sœurs, les cousins et les cousines, les tantes et les oncles, etc.

Renseignement personnel :

Tout renseignement concernant une personne physique et qui permet directement ou indirectement de l'identifier, tel que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la photographie, le code permanent, le numéro de demande d'admission (DA) et les coordonnées bancaires. En principe, ils sont confidentiels et doivent être protégés⁶.

⁴ Gouvernement du Québec. (2024, août). *Définitions de mots en lien avec la protection des renseignements personnels*. <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/lexique>

⁵ Gouvernement du Québec. (2024, août). *Droit à la portabilité*. <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/acces-aux-renseignements-personnels/droit-portabilite>

⁶ Gouvernement du Québec. (2023, sept.). *Présentation des concepts clés liés aux renseignements personnels*. <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/concepts>

Système d'information :

Un système d'information est constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation.

Par exemple : bases de données, logiciels d'application, procédures, documentation, etc. Il faut différencier le système d'information du système informatique. Ce dernier ne constitue que la partie informatique du système d'information, notamment l'unité centrale de traitement, les périphériques, le système d'exploitation, etc.⁷

3 CADRE JURIDIQUE ET CHAMP D'APPLICATION

En tant qu'organisme public, le Cégep recueille des renseignements personnels, notamment ceux de sa population étudiante, des membres du personnel et de ses fournisseurs. Il est donc assujéti aux dispositions de la *Loi sur l'accès*, du *Code civil du Québec*⁸ et de la *Charte des droits et libertés de la personne*⁹. En cas de divergence entre la *Loi sur l'accès* et la présente Directive, la *Loi sur l'accès* prévaut.

Le Cégep de Rosemont s'est également doté, en 2023, de sa *Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*. Cette Politique traite des engagements du Cégep par rapport au respect de la *Loi sur l'accès* et la protection des renseignements personnels recueillis par des moyens technologiques.

4 RÔLES ET RESPONSABILITÉS

4.1 Comité de direction

- Adopte la Directive sur la protection des renseignements personnels ainsi que toute modification à celle-ci.
- Sur recommandation du comité sur l'accès à l'information et la protection des renseignements personnels, il adopte les procédures visant à soutenir l'application de la Directive et des obligations légales du Cégep en matière de protection des renseignements personnels.

4.2 Direction générale

- Assure la conformité de la Directive avec la *Loi sur l'accès*.
- Nomme et délègue les responsabilités de la protection des renseignements personnels à la personne responsable de la protection des renseignements personnels. Préside et supervise les travaux du comité sur l'accès à l'information et la protection des renseignements personnels.

⁷ Gouvernement du Québec. (2024, août). *Définitions de mots en lien avec la protection des renseignements personnels*. <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/lexique>

⁸ *Code civil du Québec*, c. CCQ-1991

⁹ *Charte des droits et libertés de la personne*, RLRQ, c. C-12

- S'assure que les mesures sont prises pour diminuer les risques qu'un préjudice soit causé et éviter que, le cas échéant, de nouveaux incidents de même nature ne se reproduisent.
- Assure la diffusion et la mise à jour de la Directive sur le site Web.

4.3 Responsable de la protection des renseignements personnels

La responsabilité de la protection des renseignements personnels est déléguée à la personne occupant la fonction de secrétaire général.

- Veille à l'application de la Directive sur la protection des renseignements personnels et la Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques.
- Prend, en cas d'incident de confidentialité, les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se reproduisent.
- Est responsable de la réception et du traitement des plaintes.
- Est responsable de l'inscription des incidents dans le registre des incidents de confidentialité.

4.4 Comité sur l'accès à l'information et la protection des renseignements personnels

Il se compose de la personne responsable de l'accès aux documents, de celle responsable de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise. Le comité relève de la direction générale.

- Détermine les procédures qui précisent et soutiennent l'application de la Directive.
- Recommande des règles encadrant la gouvernance à l'égard des renseignements personnels.
- Soutient la personne responsable de la protection des renseignements personnels dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la *Loi sur l'accès*.
- Est responsable de l'évaluation des facteurs relatifs à la vie privée (EFVP) pour tout projet d'acquisition, de développement ou de refonte d'un système d'information ou d'une prestation électronique de services qui impliquerait la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

4.5 Direction des ressources humaines et des affaires corporatives

- S'assure que tout membre du personnel ayant accès à des renseignements personnels dans le cadre de leurs fonctions signe le formulaire d'engagement de confidentialité (voir en annexe 1).
- Assure la tenue d'activités de formation et de sensibilisation sur la protection des renseignements personnels.
- Détermine les sanctions applicables en cas de non-respect de la présente Directive, en respect des conventions collectives.

4.6 Direction des ressources informationnelles

- S'assure de la prise en charge des exigences de protection des renseignements personnels dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels elle intervient ;
- Participe à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre, et à l'anticipation des menaces en matière de protection des renseignements personnels faisant appel aux technologies de l'information ;

- Applique les mesures appropriées à toute menace ou à tout incident de confidentialité ;
- Participe aux enquêtes informatiques relatives à des contraventions réelles ou apparentes à la présente Directive et autorisées par la Direction générale ;
- Participe, en collaboration avec la Direction des ressources matérielles, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

4.7 Membres du personnel

La responsabilité de la protection des renseignements personnels incombe à toute personne qui utilise des actifs informationnels du Cégep. Quiconque collecte, accède ou conserve un renseignement personnel, le consulte ou le traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger sa confidentialité. À cette fin, le personnel qui a accès à des renseignements personnels dans le cadre de ses fonctions doit :

- Se conformer à la présente Directive en matière de protection des renseignements personnels ;
- Accéder et utiliser les renseignements personnels qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés ;
- Participer aux activités de formation et de sensibilisation offertes par le Cégep ;
- Signaler à la personne responsable de la protection des renseignements personnels du Cégep tout incident de confidentialité susceptible de constituer une contravention à la présente Directive.

5 COLLECTE DES RENSEIGNEMENTS PERSONNELS

5.1 Renseignements personnels pouvant être collectés

Le Cégep recueille uniquement les renseignements personnels nécessaires à la réalisation de sa mission et son offre de services. Le Cégep prend des mesures pour s'assurer que les renseignements personnels qu'il recueille sont adéquats, pertinents, non excessifs et utilisés à des fins spécifiques et limitées :

- a) Sa collecte est liée aux objectifs établis ;
- b) L'atteinte du droit à la vie privée est réduite au minimum ;

Lorsqu'il recueille des renseignements personnels, le Cégep s'assure d'informer la personne concernée, au plus tard au moment de la collecte :

1. Du nom de l'organisme public au nom duquel la collecte est faite ;
2. Des fins auxquelles ces renseignements sont recueillis ;
3. Des moyens par lesquels les renseignements sont recueillis ;
4. Du caractère obligatoire ou facultatif de la demande ;
5. Des conséquences d'un refus de répondre ou de consentir à la demande ;
6. Des droits d'accès et de rectification prévus par la *Loi sur l'accès* ;
7. De la possibilité que les renseignements personnels soient communiqués à l'extérieur du Québec, le cas échéant.

En conformité avec la *Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*, le Cégep ne fait pas usage des renseignements personnels à d'autres fins que celles précisées lors de la collecte, à moins qu'une personne n'y consente expressément ou que la *Loi sur l'accès* l'exige.

5.2 Moyens de collecte

En cohérence avec la *Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*, les renseignements personnels conservés par le Cégep sont recueillis seulement après que la personne concernée par une collecte fut avisée des fins de celle-ci et qu'elle ait soumis volontairement lesdits renseignements, soit par l'entremise d'un formulaire ou par leur transmission par courriel.

Sur demande, la personne concernée est informée des renseignements personnels recueillis auprès d'elle, des catégories de personnes qui y ont accès au Cégep, de la durée de conservation de ces renseignements ainsi que des coordonnées de la personne responsable de la protection des renseignements personnels.

6 GESTION DU CONSENTEMENT

L'obtention du consentement est nécessaire lorsque des renseignements personnels sont communiqués, c'est-à-dire divulgués à l'externe ou à des membres du personnel au Cégep qui ne peuvent pas y avoir accès. De plus, l'article 65.1 de la *Loi sur l'accès* précise qu'un « organisme public peut [...] utiliser un renseignement personnel à une autre fin sans le consentement de la personne concernée [...] lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli »¹⁰. Par exemple, lors de sondages destinés à la population étudiante.

6.1 Obtention du consentement préalable à la communication

Toute direction ou tout service devant effectuer la communication de renseignements personnels doit transmettre le formulaire de consentement préalable à la communication des renseignements personnels prévu à cette fin en annexe 2 aux personnes concernées afin qu'elles le complètent. Lorsque rempli, la direction ou le service concerné doit le conserver selon le processus en place.

Pour être valable, le consentement devra être manifeste, libre, éclairé, donné à des fins spécifiques, en termes simples et clairs ainsi que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé¹¹. Si la personne concernée est une personne mineure de 14 ans et plus, le consentement peut être donné par elle-même, par son ou ses parents détenant l'autorité parentale ou par le tuteur ou la tutrice¹². Le cas échéant, le Cégep doit accompagner toute personne qui en fait la demande afin de lui expliquer clairement la portée et les conséquences du consentement demandé¹³.

¹⁰ ¹⁰ *Loi sur l'accès*, RLRQ, c. 3, Art. 65.1

¹¹ *Loi sur l'accès*, RLRQ, c. 3, Art. 53.1

¹² Id.

¹³ Id.

6.2 Retrait du consentement

Une personne peut, en tout temps, retirer son consentement à la communication de ses renseignements personnels. Pour ce faire, elle doit communiquer avec le secrétariat général en suivant les modalités indiquées dans le formulaire de consentement.

Dans certains cas, le retrait du consentement peut faire en sorte que le Cégep ne puisse pas fournir un service prévu dans sa mission. Pour aider à la prise de décision, le Cégep doit expliquer l'impact possible du retrait du consentement.

Le décès de la personne révoque automatiquement le consentement, à moins qu'il ne soit clairement établi que ce consentement demeure valide après le décès.

6.3 Communication sans le consentement préalable lors de circonstances exceptionnelles

En complément à l'article 6 de la *Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*, les membres du personnel du Cégep sont autorisés à divulguer des renseignements personnels sans le consentement lors de circonstances exceptionnelles, dans une situation comportant un risque important pour la santé ou la sécurité des personnes. Pour ce faire, les conditions suivantes doivent être respectées :

- La situation doit avoir un caractère urgent et dangereux.¹⁴
- La divulgation de renseignements personnels est nécessaire pour protéger la vie, la santé ou la sécurité d'une personne.¹⁵
- Il doit être évident que la divulgation des renseignements personnels bénéficiera à la personne concernée.¹⁶
- La décision doit être fondée sur des faits tangibles, et non seulement sur des soupçons ou une inquiétude. Toute personne raisonnable placée dans la même situation doit être en mesure de conclure à un risque sérieux.¹⁷

Modalité de mise en œuvre

Lorsque les conditions ci-dessus sont respectées, seuls les renseignements personnels nécessaires peuvent être communiqués¹⁸, et ce, uniquement aux personnes en mesure de leur porter secours, soit des personnes touchées directement par la situation, comme un professionnel ou une professionnelle de la santé, un intervenant ou une intervenante d'urgence ou une ou un membre des services de sécurité du Cégep.¹⁹

Tout membre du personnel qui communique des renseignements personnels détenus dans le cadre de leur fonction en application de cette exception doit en informer le responsable de la protection des renseignements personnels qui l'inscrira au registre prévu à cet effet.

¹⁴ Loi sur l'accès, RLRQ, c. 3, art. 60, alinéa 1

¹⁵ Loi sur l'accès, RLRQ, c. 3, art. 59, paragraphe 4°

¹⁶ Loi sur l'accès, RLRQ, c. 3, art. 65.1

¹⁷ Commission d'accès à l'information. (s. d.) *Ministères et organismes publics, Utilisation et communication de renseignements personnels*. <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-ministeres-et-organismes-publics/utilisation-communication-de-renseignements-personnels>

¹⁸ Loi sur l'accès, RLRQ, c. 3, art. 60.1

¹⁹ Loi sur l'accès, RLRQ, c. 3, art. 59.1, alinéa 1

7 OBSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Sauf exception ou exigence particulière, et en cohérence avec la *Politique de gestion documentaire*, lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, le Cégep détruit les renseignements personnels, et ce, conformément à son calendrier de conservation. Lorsque pertinent pour des fins d'intérêt public, le Cégep peut les anonymiser de la manière prescrite dans le Règlement sur l'anonymisation des renseignements personnels du Gouvernement du Québec (voir l'annexe 4).

Lorsque le Cégep procède à la destruction de documents contenant des renseignements personnels, il s'assure de prendre les mesures de protection nécessaires visant à assurer la confidentialité de ceux-ci.

Le choix de la méthode de destruction dépend de plusieurs facteurs, notamment la sensibilité des informations, l'objectif de leur utilisation, leur volume, leur répartition et le support sur lequel elles se trouvent. Les renseignements détenus par le Cégep sont généralement traités et sauvegardés au Québec.

8 DEMANDE D'ACCÈS OU DE RECTIFICATION À DES RENSEIGNEMENTS PERSONNELS

8.1 Demande d'accès à des renseignements personnels

Toute personne qui en fait la demande peut avoir accès aux renseignements personnels la concernant détenus par le Cégep, sous réserve des exceptions prévues par la *Loi sur l'accès*. Ces demandes d'accès ne requièrent pas de format particulier, elle peut s'appliquer tant pour les renseignements personnels informatisés que sur support papier.

Une demande d'accès ne sera considérée que si elle est faite par écrit par une personne physique justifiant son identité à titre de personne concernée, à titre de représentante ou de représentant, d'héritière ou d'héritier ou de successible de cette dernière, à titre de liquidatrice ou de liquidateur de la succession, à titre de bénéficiaire d'assurance vie ou d'indemnité de décès, à titre de titulaire de l'autorité parentale même si l'enfant mineur est décédé, ou à titre de conjointe, de conjoint ou de proche parent d'une personne décédée.

Cette demande doit être adressée à la personne responsable de la protection des renseignements personnels du Cégep par l'intermédiaire du formulaire en ligne ou par courriel à secretariatgeneral@crosemont.qc.ca. La demande doit fournir suffisamment d'indications précises pour permettre au Cégep de la traiter.

Un accusé de réception sera envoyé lors de la réception de la demande et les renseignements personnels demandés seront fournis au plus tard dans les vingt (20) jours (jours civils) qui suivent la date de la réception de la demande. Si le traitement de la demande dans le délai prévu ne semble pas possible sans nuire au déroulement normal des activités du Cégep, la personne responsable peut, avant l'expiration de ce délai, le prolonger d'une période n'excédant pas dix (10) jours, en le signalant à la personne requérante avant l'expiration du délai de vingt (20) jours. L'absence de réponse équivaut à un refus.

Si la personne qui fait la demande n'est pas satisfaite de la réponse du Cégep, elle peut aviser la Commission sur l'accès à l'information de cette décision afin que celle-ci soit révisée. Cette demande de révision doit être faite dans les trente (30) jours qui suivent la date de la décision ou de l'expiration du délai.

8.1.1 Droit à la portabilité

Toute personne peut exercer son droit à la portabilité, c'est-à-dire demander à recevoir ses renseignements personnels informatisés dans un format technologique structuré et couramment utilisé, comme JSON, CSV ou XML. Le détail de la procédure de traitement de ces demandes se trouve en annexe 5.

Elle peut également demander que ses renseignements personnels informatisés soient communiqués à un tiers autorisé à les recueillir en vertu de la Loi sur l'accès.

8.2 Demande de rectification

Toute personne qui reçoit une confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la *Loi sur l'accès*, exiger que le fichier soit rectifié.

Une demande de rectification ne sera considérée que si elle est faite par écrit par une personne physique justifiant son identité à titre de personne concernée, à titre de représentante ou de représentant, d'héritière ou d'héritier ou de successible de cette dernière, à titre de liquidatrice ou de liquidateur de la succession, à titre de bénéficiaire d'assurance vie ou d'indemnité de décès, à titre de titulaire de l'autorité parentale même si l'enfant mineur est décédé ou à titre de conjointe, de conjoint ou de proche parent d'une personne décédée.

Cette demande doit être adressée à la personne responsable de la protection des renseignements personnels du Cégep par courriel à l'adresse suivante secretariatgeneral@crosemont.qc.ca. La demande doit fournir les indications précises permettant au Cégep de la traiter.

La personne responsable doit répondre au plus tard dans les vingt (20) jours qui suivent la date de la réception d'une demande. Si le traitement de la demande dans le délai prévu précédemment ne lui paraît pas possible sans nuire au déroulement normal des activités du Cégep, la personne responsable peut, avant l'expiration de ce délai, le prolonger d'une période n'excédant pas dix (10) jours en donnant un avis à cet effet à la personne requérante.

Lorsque le Cégep reçoit une demande de rectification d'un fichier contenant des renseignements personnels, il est tenu de fournir gratuitement à la personne ayant formulé la demande une copie des renseignements personnels modifiée ou ajoutée, ou une attestation confirmant le retrait des renseignements personnels.

En cas de refus d'accéder à une demande de rectification, le responsable doit préciser la disposition légale applicable et, au besoin, expliquer la décision à la personne requérante. Il doit également conserver le renseignement visé pendant la période nécessaire pour permettre au requérant d'épuiser les recours prévus par la loi.

Si la personne qui fait la demande n'est pas satisfaite de la décision du Cégep, elle peut aviser la Commission sur

l'accès à l'information de cette décision afin que celle-ci soit révisée.

Cette demande de révision doit être faite dans les trente (30) jours qui suivent la date de la décision ou de l'expiration du délai prévu à la *Loi sur l'accès* pour répondre à la demande.

9 GESTION DES INCIDENTS DE CONFIDENTIALITÉ

9.1 Définition

Selon la Loi sur l'accès, un incident de confidentialité se définit comme :

- Tout accès à un renseignement personnel non autorisé par la Loi ;
- Toute utilisation ou toute communication non autorisée d'un renseignement personnel ;
- La perte d'un renseignement personnel ou toute autre atteinte à sa protection²⁰.

Par exemple, un incident de confidentialité pourrait se produire :

- Lorsqu'un membre du personnel consulte un renseignement personnel sans autorisation ;
- Lorsqu'un membre du personnel communique des renseignements personnels au mauvais destinataire ;
- Lorsque l'entreprise est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

10 TRAITEMENT DES INCIDENTS DE CONFIDENTIALITÉ

Lorsque le Cégep a des motifs de croire qu'il s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, il doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent, ce qui peut inclure la sanction des individus en cause.

Si l'incident de confidentialité présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, en aviser la Commission sur l'accès à l'information. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident.

10.1 Registre des incidents de confidentialité

Le Cégep tient un registre des incidents de confidentialité dont un modèle est joint en annexe 6 à la présente Directive. Celui-ci contient, notamment :

1. Une description des renseignements personnels visés par l'incident ;
2. Les circonstances de l'incident ;
3. La date où l'incident a eu lieu ;
4. La date où la personne responsable de la protection des renseignements personnels a eu connaissance

²⁰ Loi sur l'accès, RLRQ, c. 3, art. 63.9

- de l'incident ;
5. Le nombre de personnes visées ;
 6. L'évaluation de la gravité du risque de préjudice ;
 7. S'il existe un risque de préjudice sérieux pour la personne concernée, les dates de transmission des avis ;
 8. Les mesures prises en réaction à l'incident.

11 PROCESSUS DE TRAITEMENT DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

11.1 Dépôt d'une plainte relative à la protection des renseignements personnels

Toute personne ayant des raisons de penser qu'une violation de la confidentialité s'est produite et que le Cégep n'a pas assuré la protection des renseignements personnels qu'il détient peut déposer une plainte à l'aide du formulaire prévu à cette fin afin de demander la correction de la situation. Un formulaire de plainte est en annexe 3 de la Directive.

La plainte doit être déposée par écrit et comporter une description de l'incident, la date ou la période où l'incident s'est produit, la nature des renseignements personnels visés par l'incident et le nombre de personnes concernées. La plainte doit être adressée à la personne responsable de la protection des renseignements personnels. Elle doit être faite par courriel à l'adresse suivante secretariatgeneral@crosemont.qc.ca.

Dans le cas où la plainte mettrait en cause la conduite de la personne responsable de la protection des renseignements personnels, celle-ci doit être adressée par courriel à la Direction générale du Cégep à l'adresse dirgen@crosemont.qc.ca.

11.2 Traitement de la plainte

La personne responsable de la protection des renseignements personnels a la responsabilité de recevoir et de traiter la plainte dans un délai de 20 jours ouvrables. Dans le cas où celle-ci s'avèrerait fondée, le Cégep prend les mesures requises pour corriger la situation dans les meilleurs délais conformément au paragraphe 10 de la présente Directive et procède à l'inscription de l'incident au registre des incidents de confidentialité, comme indiqué au paragraphe 10.1.

12 VIDÉOSURVEILLANCE

Le recours à la vidéosurveillance s'effectue en respect des obligations prévues notamment par le Code civil du Québec, par la Charte des droits et libertés de la personne ainsi que par la *Loi sur l'accès*.

À moins d'indication contraire, les règles énoncées dans la présente Directive concernant la collecte, l'utilisation, la communication ou la conservation des renseignements personnels s'appliquent aux renseignements

personnels enregistrés par vidéosurveillance, en cohérence avec la *Directive administrative concernant l'utilisation de la vidéosurveillance avec enregistrement*.

13 PROJETS DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS

Le Cégep procède à une évaluation des facteurs relatifs à la vie privée (EFVP) pour tout projet d'acquisition, de développement ou de refonte d'un système d'information ou d'une prestation électronique de services qui impliquerait la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Lors de l'EFVP, le Cégep s'assure que le système d'information ou de prestation de services électroniques permet qu'un renseignement personnel informatisé soit extrait dans un format technologique structuré et couramment utilisé afin de répondre aux demandes d'accès à des renseignements personnels informatisés exigés dans ce format.

13.1 Procédure d'évaluation des facteurs relatifs à la vie privée (EFVP)

1. La direction ou le service qui projette acquérir, développer ou refondre un système d'information ou de prestation électronique de services impliquant des renseignements personnels doit effectuer une évaluation initiale de son projet à l'aide de la grille d'évaluation (voir la [Grille d'évaluation des facteurs relatifs à la vie privée](#)). Une EFVP doit également être effectuée si une direction ou un service projette de communiquer des renseignements personnels que ce soit à l'extérieur du Québec, à un autre organisme public ou dans d'autres contextes.
2. La direction ou le service doit informer la Direction des ressources informationnelles et collaborer avec elle, au besoin, pour compléter l'évaluation.
3. La direction ou le service transmet l'évaluation au comité sur l'accès à l'information et la protection des renseignements personnels qui procède à sa validation et son approbation.
4. Dans le cas d'un processus d'acquisition, l'évaluation complétée et approuvée doit être transmise au service de l'approvisionnement.
5. L'EFVP doit faire l'objet d'une révision périodique lors du renouvellement de l'acquisition ou si le fournisseur du logiciel est acquis par un tiers ou si ce fournisseur modifie ses règles.

14 ACTIVITÉS DE FORMATION ET DE SENSIBILISATION À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS OFFERTES PAR LE CÉGEP À SON PERSONNEL

Les activités de formation et de sensibilisation sont publiées sur le portail du Cégep. Le calendrier de formations et d'activités de sensibilisation sera mis à jour régulièrement dans l'année. Le cas échéant, le caractère obligatoire de la participation aux formations et activités apparaîtra au calendrier.

15 SANCTIONS APPLICABLES EN CAS DE NON-RESPECT DE LA DIRECTIVE

Le non-respect de la Directive par le personnel pourrait entraîner des mesures administratives ou disciplinaires pouvant aller jusqu'au congédiement, en conformité avec les conventions collectives de travail. La nature, la gravité et le caractère répétitif des actes reprochés doivent être considérés au moment de déterminer une sanction.

Le non-respect de la Directive par des personnes embauchées de manière contractuelle peut entraîner des sanctions proportionnelles à la gravité de la faute commise, pouvant aller jusqu'à la résiliation du contrat sans préavis, en conformité avec le contrat et sous réserve des dispositions en matière de droit du travail.

En complément à l'article 3 de la *Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*, les personnes embauchées de manière contractuelle qui pourraient, dans le cadre de leur contrat, avoir accès à des renseignements personnels doivent s'engager, par le moyen du formulaire d'engagement de confidentialité en annexe 1, à respecter la confidentialité des renseignements personnels et de toute autre information confidentielle à laquelle elle pourrait avoir accès.

16 ENTRÉE EN VIGUEUR

La nouvelle *Directive* entre en vigueur au moment de son approbation par le comité de direction et est révisée au besoin. Elle doit être lue en concomitance avec la [*Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*](#).

Approuvée par le comité de direction, le 2 septembre 2025.

ANNEXE 1 – PROPOSITION DE FORMULAIRE D'ENGAGEMENT DE CONFIDENTIALITÉ

Le Cégep de Rosemont est tenu, en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, d'assurer la confidentialité des renseignements personnels qu'il détient. On entend par renseignement personnel toute information concernant une personne physique et permettant directement ou indirectement de l'identifier.

Afin de réaliser adéquatement sa mission et fournir les services prévus, le Cégep recueille et détient des informations confidentielles, incluant des renseignements personnels, dont il doit assurer la confidentialité en tout temps.

Considérant ce qui précède, et le fait que je peux avoir accès à de tels renseignements et à de telles informations dans le cadre de mes fonctions, je soussigné(e), **[prénom, nom]**, occupant le poste de **[titre du poste]**, m'engage à respecter la confidentialité des renseignements personnels et de toute autre information confidentielle auxquels je pourrais avoir accès dans l'exercice de mes fonctions.

Je m'engage également à accéder, collecter, utiliser uniquement les renseignements personnels et les informations confidentielles nécessaires à l'exécution de mes tâches ainsi qu'à les communiquer, conserver ou détruire conformément aux exigences de mes fonctions. Je m'engage à ne divulguer aucune information pouvant permettre d'identifier une personne.

Finalement, je reconnais avoir pris connaissance de la ***Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*** ainsi que de la ***Directive sur la protection des renseignements personnels*** et m'engage à en respecter les termes et le contenu.

Signature de l'employé-e

Date

Nom en lettres moulées

ANNEXE 2 – PROPOSITION DE FORMULAIRE DE CONSENTEMENT PRÉALABLE À LA DIVULGATION DES RENSEIGNEMENTS PERSONNELS

En vue de **[indiquer la fin spécifique]**, j'autorise le Cégep à divulguer les renseignements personnels suivants me concernant **[indiquer de manière précise quels renseignements sont visés]** à **[indiquer de manière précise les personnes à qui la transmission sera faite]** de manière **[indiquer si s'agit d'une communication verbale ou écrite, lorsque pertinent]**.

Le consentement est valide pour une durée de

Je comprends que ce consentement peut être modifié ou révoqué en tout temps. Pour ce faire, j'aurai à en informer le responsable de la protection des renseignements personnels à cette adresse : secretariatgeneral@crosemont.qc.ca.

Nom en lettres moulées

Date

Signature de la participante
ou du participant

Nom en lettres moulées

Date

Signature du parent / tuteur légal
(Si la participante ou le participant a moins de 18 ans)

ANNEXE 3 — PROPOSITION DE FORMULAIRE DE PLAINTE — PROTECTION DES RENSEIGNEMENTS PERSONNELS

Veuillez remplir ce formulaire si vous avez des motifs de croire qu'il y a eu une violation de la confidentialité des renseignements personnels détenus par l'organisme public, et que le processus de traitement des plaintes doit être enclenché conformément à l'article 63.3 de la *Loi sur l'accès*.

Informations sur la personne plaignante :

Nom complet : _____

Adresse : _____

Numéro de téléphone : _____

Adresse électronique : _____

Description de la plainte :

Date de la plainte : _____

Décrivez brièvement les circonstances de la violation présumée de la confidentialité des renseignements personnels : _____

Étapes du processus de traitement de la plainte :

- **Réception de la plainte :**

Date de réception : _____

Personne responsable : _____

- **Consultation des intervenants concernés :**

Liste des intervenants consultés : _____

Ressources nécessaires : _____

- **Traitement de la plainte :**

Mesures prises : _____

Date de résolution prévue : _____

- **Suivi auprès de la personne plaignante :**

Méthode de suivi préférée (téléphone, courriel, rencontre, etc.) : _____

- **Ajustements nécessaires :**

Décisions prises pour faire suite à la plainte : _____

Date de mise en œuvre des ajustements : _____

Reddition de comptes :

L'organisme public déterminera les modalités de reddition de comptes. Veuillez indiquer vos préférences ou suggestions quant à la présentation des résultats du traitement de la plainte (ex. : rencontre, rapport, autre) : _____

Signature de la personne plaignante :

Je soussigné(e), déclare que les informations fournies dans ce formulaire sont exactes et complètes à ma connaissance.

Signature : _____ Date : _____

Veuillez soumettre ce formulaire complété à l'adresse suivante : secretariatgeneral@crosemont.qc.ca

ANNEXE 4 - LIGNES DIRECTRICES POUR LA MISE EN ŒUVRE DU PROCESSUS D'ANONYMISATION DES RENSEIGNEMENTS PERSONNELS

Dans le cadre de la Loi sur l'accès, l'anonymisation est règlementée par une procédure qui se retrouve dans le Règlement sur l'anonymisation des renseignements personnels²¹ associé à la Loi sur l'accès.

À titre de personne responsable de la protection des renseignements personnels, le ou la secrétaire général·e est responsable de la mise en œuvre de ces lignes directrices.

L'importance de recourir au Comité

En raison de la complexité et de la nécessité de recourir à des compétences spécialisées, avant d'amorcer un processus d'anonymisation, il est recommandé qu'une personne ou un comité avec les compétences spécialisées nécessaires en fasse la démonstration de la nécessité au comité sur l'accès à l'information et la protection des renseignements personnels.

Lignes directrices

Le Comité ou la personne déléguée s'assure de mettre en œuvre les lignes directrices suivantes.

En conformité avec le Règlement sur l'anonymisation des renseignements personnels, le Cégep doit s'assurer d'établir les fins pour lesquelles elle entend utiliser les renseignements anonymisés.

Étape 1 : Identifier les renseignements personnels (RP) arrivés à la fin de leur cycle de vie, selon le calendrier de conservation et déterminer s'il est utile de les anonymiser ou s'il est préférable de les détruire. Si l'on juge que l'anonymisation est souhaitable, il faut alors en justifier la raison.

Étape 2 : Identifier la ou les méthodes d'anonymisation appropriées en fonction des caractéristiques des RP, en collaboration avec des spécialistes. Il est possible de regrouper les RP dans un ensemble de données (*data set*, en anglais) qui auront chacune une manière différente d'être anonymisées en fonction de leurs caractéristiques et les besoins liés à leur utilisation. À titre d'exemple, un ensemble de données au Cégep de Rosemont serait les RP du personnel ou encore ceux de la population étudiante. Ces ensembles pourraient également être sous-divisés en sous-ensembles de données.

Étape 3 : Appliquer la ou les méthodes d'anonymisation sélectionnées afin de retirer tous les renseignements personnels qui permettent d'identifier directement ou indirectement la ou les personnes concernées.

Étape 4 : Effectuer une analyse préliminaire des risques de réidentification.

Étape 5 : Au regard des risques de réidentification identifiés à l'étape précédente, établir les techniques d'anonymisation à utiliser raisonnables pour diminuer les risques de réidentification, lesquelles doivent être conformes aux meilleures pratiques généralement reconnues.

Étape 6 : effectuer une analyse des risques de réidentification.

- Note : il n'est pas nécessaire de démontrer un risque nul, mais il faut démontrer que le processus d'anonymisation permet, de façon irréversible, de ne pas identifier directement ou indirectement une personne.

²¹ Règlement sur l'anonymisation des renseignements personnels. RLRQ A-2.1, r. 0.1. <https://www.legisquebec.gouv.qc.ca/fr/document/rc/A-2.1.%20r.%200.1%20/>

Étape 7 : consigner dans un registre les renseignements suivants :

- 1° une description des renseignements personnels qui ont été anonymisés ;
- 2° les fins pour lesquelles elle entend utiliser ces renseignements anonymisés ;
- 3° les techniques d'anonymisation utilisées et les mesures de protection et de sécurité établies ;
- 4° la date à laquelle l'analyse des risques de réidentification a été complétée et, le cas échéant, la date à laquelle la mise à jour de l'analyse.

Finalement, le Cégep doit mettre à jour la dernière analyse des risques de réidentification qu'elle a effectuée de manière périodique. Cette mise à jour doit notamment considérer les avancées technologiques qui peuvent contribuer à réidentifier une personne.

ANNEXE 5 — PROCÉDURE DE TRAITEMENT DES DEMANDES D'ACCÈS À DES RENSEIGNEMENTS PERSONNELS INFORMATISÉS — DROIT À LA PORTABILITÉ

Lorsqu'une personne demande l'accès à ses renseignements personnels informatisés dans un format technologique structuré et couramment utilisé, la procédure suivante doit être mise en œuvre, en complément de l'article 8.1 *Demande d'accès à des renseignements personnels*. La procédure suivante doit être mise en œuvre uniquement dans un contexte de portabilité.

Les renseignements personnels (RP) concernés par le droit à la portabilité sont les renseignements informatisés qui ont été recueillis directement ou indirectement auprès de la personne par le Cégep de Rosemont. Sont exclus les renseignements créés ou inférés comme les notes personnelles portant sur la personne concernée.

- Exemples de RP recueillis directement : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la photographie, le numéro de demande d'admission (DA), les coordonnées bancaires, la plaque d'immatriculation, etc.
- Exemples de RP recueillis indirectement : l'historique de paiement au registrariat, l'historique d'emprunt à la bibliothèque, etc.

Étape 1 : Dépôt de la demande de portabilité des renseignements personnels

La personne qui en fait la demande doit envoyer une demande écrite au responsable de la protection des renseignements personnels par l'entremise du formulaire en ligne sur le site Internet du Cégep. Ce formulaire est envoyé directement à l'adresse courriel secretariatgeneral@crosemont.qc.ca. Un avis de réception de la demande est émis automatiquement dès la réception de la demande.

Étape 2 : Analyse de la demande

L'analyse de la demande est faite par la technicienne juridique au secrétariat général. L'analyse doit permettre de répondre aux questions suivantes :

- La demande concerne-t-elle des RP informatisés recueillis auprès de la personne concernée ?
 - Si non, la demande ne peut être traitée. Un courriel est envoyé à la personne qui a formulé la demande afin de lui expliquer que la demande ne peut être traitée.
- La demande est-elle suffisamment précise ?
 - Si non, il faut prêter assistance. Il faut prendre contact rapidement avec la personne qui a formulé la demande pour la préciser.
- La demande entraîne-t-elle des « difficultés pratiques sérieuses » ?
 - Si oui, la demande peut être refusée. Un courriel expliquant la raison du refus doit être envoyé à la personne qui a formulé la demande.

Étape 3 : Traitement de la demande

Le secrétariat général est responsable de communiquer avec les directions ou les services susceptibles d'avoir recueilli des renseignements personnels sur la personne concernée. Les informations à ce sujet se retrouvent dans l'Annexe 1 de la *Politique de confidentialité sur la protection des renseignements personnels recueillis par des moyens technologiques*.

- **Pour une ou un membre du personnel** : Le Secrétariat général transmet la demande à la Direction des ressources humaines afin d'extraire les données du ou des logiciels utilisés dans le service en collaboration avec la Direction des ressources informationnelles et le ou les fournisseurs, le cas échéant. La demande pourrait également être transférée à la Direction des ressources matérielles pour toute information complémentaire ainsi qu'à la bibliothèque afin d'extraire l'historique d'emprunt de livres, le cas échéant.
- **Pour une étudiante ou un étudiant à la formation ordinaire ou à la formation continue** : Le Secrétariat général transmet la demande au Registrariat et à la Direction des services aux étudiants qui prendront

connaissance du dossier afin d'extraire les renseignements personnels nécessaires, en collaboration avec la Direction des ressources informationnelles et le ou les fournisseurs, le cas échéant. Si l'étudiante ou l'étudiant est dans un programme incluant un stage, le Registrariat doit communiquer avec la direction adjointe concernée afin d'extraire les données. La demande pourrait également être transférée à la Direction des ressources matérielles pour toute information complémentaire ainsi qu'à la bibliothèque afin d'extraire l'historique d'emprunt de livres, le cas échéant.

- **Pour une étudiante ou un étudiant au Cégep à distance** : Le Secrétariat général transmet la demande au Registrariat du Cégep à distance et à la Direction des services aux étudiants qui prendront connaissance du dossier afin d'extraire les données du ou des logiciels utilisés dans le service en collaboration avec la Direction des ressources informationnelles et le ou les fournisseurs, le cas échéant. La demande pourrait également être transférée à la bibliothèque afin d'extraire l'historique d'emprunt de livres, le cas échéant.
- **Pour une personne embauchée de manière contractuelle** : Le Secrétariat général transmet la demande à la Direction des ressources financières et toute autre direction pertinente qui va extraire les données du ou des logiciels pertinents en collaboration avec la Direction des ressources informationnelles ainsi que le ou les fournisseurs, le cas échéant.

Étape 4 : Réponse à la demande

Lorsque le traitement de la demande est terminé, le Secrétariat général communique avec la personne qui a formulé la demande pour l'informer que la demande a été traitée. L'absence d'une réponse équivaut à un refus. Tout refus doit être justifié. Un refus peut être considéré comme acceptable si la demande entraîne des « difficultés pratiques sérieuses »²².

Pour des raisons de sécurité, de confidentialité et de protection des renseignements personnels, le Cégep priorise la remise des renseignements personnels en personne. Ainsi, l'identité de la personne doit être confirmée avant de lui remettre les renseignements personnels.

- **Remise des renseignements en personne** : les renseignements personnels sont remis sur une clé USB en mains propres. La personne qui a formulé la demande doit s'identifier avec une carte d'identité reconnue par l'organisation pour prendre possession de la clé USB.

Si la personne à l'origine de la demande a des contraintes à se déplacer en personne, elle doit justifier sa situation auprès du secrétariat général. Dans la perspective où la demande est jugée recevable et acceptée, une mesure alternative pourra être proposée.

Les documents contenant les renseignements personnels doivent être dans un format technologique structuré et couramment utilisé, comme CSV.

²² Commission d'accès à l'information. (s. d.) *Ministères et organismes publics, Responsabilités des organismes publics, Qui est responsable de la protection des renseignements personnels dans un organisme public ?* <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-ministeres-et-organismes-publics/responsable-acces-documents-et-protection-renseignements-personnels>

À titre d'exemple, la Commission a déjà conclu que les coûts importants engendrés pour donner suite à une demande ou la complexité que nécessite le transfert dû au choix du demandeur quant à la forme peuvent être considérés comme des « difficultés pratiques sérieuses ». Le manque de personnel n'est pas une difficulté pratique sérieuse.

ANNEXE 6 - MODÈLE DE REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Numéro de l'incident	
Renseignements visés par l'incident	Décrire les renseignements personnels visés par l'incident ou en dresser une liste. Si cette information n'est pas connue, il faut le préciser et expliquer la raison qui justifie l'impossibilité de fournir une telle description.
Circonstances de l'incident	Décrire brièvement les circonstances de l'incident.
Date ou période de l'incident	Mentionner la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation.
Date ou période de la prise de connaissance de l'incident	Mentionner la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident.
Nombre de personnes concernées par l'incident	Mentionner le nombre de personnes concernées par l'incident ou, si ce dernier n'est pas connu, une approximation.
Risque qu'un préjudice sérieux soit causé	Oui Non Décrire les éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées
Transmission des avis	Date(s) de l'avis à la Commission sur l'accès à l'information : S'il y a un risque qu'un préjudice sérieux soit causé, inscrire la ou les dates. Sinon, inscrire « Sans objet ». Date(s) de l'avis aux personnes concernées : S'il y a un risque qu'un préjudice sérieux soit causé, inscrire la ou les dates. Sinon, inscrire « Sans objet ». Date(s) de l'avis aux assureurs : le cas échéant. Sinon, inscrire « Sans objet ». Avis public : Oui / Non Raison : Si un avis public a été diffusé, en expliquer la raison. Dans le cas contraire, inscrire « Sans objet ».
Description des mesures prises par l'organisation	Mécanismes de protection offerts : décrire les mesures de mitigation déployées pour minimiser les effets négatifs de l'incident. Mesures de prévention déployées : décrire brièvement les mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé
Commentaires	Ajouter des commentaires si nécessaire.