

DIRECTIVE 2600-094

TITRE :	Directive relative à la protection des renseignements personnels		
ADOPTION :	Comité de direction de l'Université	Résolution :	CD-2023-09-18-07
ENTRÉE EN VIGUEUR :	2023-09-18		
MODIFICATION :	Comité de direction de l'Université	Résolution :	

TABLE DES MATIÈRES

PRÉAMBULE	3
1. OBJECTIF	3
2. CADRE LÉGAL ET NORMATIF	3
3. CHAMP D'APPLICATION	4
4. DÉFINITIONS	4
5. MESURES APPLICABLES À TOUTES LES ÉTAPES DU CYCLE DE VIE DES RENSEIGNEMENTS PERSONNELS	7
5.1. CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS.....	7
5.2. CONSENTEMENT DES PERSONNES CONCERNÉES.....	7
5.2.1. <i>Consentement obligatoire</i>	7
5.2.2. <i>Critères de validité du consentement</i>	7
5.2.3. <i>Consentement de la personne mineure</i>	7
5.3. NÉCESSITÉ D'UN RENSEIGNEMENT PERSONNEL.....	8
5.4. INCIDENT DE CONFIDENTIALITÉ	8
5.4.1. <i>Obligations en cas d'incident de confidentialité</i>	8
5.4.2. <i>Rôles et responsabilités</i>	8
5.4.3. <i>Registre des incidents de confidentialité</i>	10
6. MESURES APPLICABLES AUX CINQ ÉTAPES DU CYCLE DE VIE DES RENSEIGNEMENTS PERSONNELS	10
6.1. COLLECTE DES RENSEIGNEMENTS PERSONNELS.....	10
6.1.1. <i>Mesures liées à la collecte</i>	10
6.1.2. <i>Mesures liées à la biométrie</i>	11
6.1.3. <i>Mesures liées aux sondages</i>	12
6.1.4. <i>Mesures liées à la collecte pour le compte d'un partenaire</i>	12
6.2. UTILISATION DES RENSEIGNEMENTS PERSONNELS.....	13
6.2.1. <i>Mesures lors d'une utilisation sans le consentement de la personne concernée</i>	13
6.2.2. <i>Mesures liées aux décisions fondées sur un traitement automatisé</i>	14
6.3. COMMUNICATION DES RENSEIGNEMENTS PERSONNELS.....	14
6.3.1. <i>Mesures de communication sans le consentement de la personne concernée</i>	14
6.3.2. <i>Mesures de communication de renseignements personnels à l'extérieur du Québec</i>	19
6.4. CONSERVATION DES RENSEIGNEMENTS PERSONNELS	20

6.5. DESTRUCTION ET ANONYMISATION DES RENSEIGNEMENTS PERSONNELS	20
7. MESURES PARTICULIÈRES LORS D'UN PROJET DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES	20
8. MODALITÉS D'EXERCICE DES DROITS DES PERSONNES CONCERNÉES	21
8.1. EXERCICE DES DROITS D'ACCÈS ET DE RECTIFICATION.....	21
8.2. EXIGENCES PARTICULIÈRES LORS D'UNE DEMANDE DE RENSEIGNEMENT PERSONNEL OU DE RECTIFICATION D'UNE CONJOINTE OU D'UN CONJOINT OU D'UN PROCHE PARENT DE LA PERSONNE CONCERNÉE DANS SON PROCESSUS DE DEUIL.....	22
8.3. EXIGENCE PARTICULIÈRE LORS D'UNE DEMANDE DE RENSEIGNEMENT PERSONNEL OU DE RECTIFICATION DU LIQUIDATEUR DE LA SUCCESSION, DU BÉNÉFICIAIRE D'UNE ASSURANCE VIE OU D'UNE INDEMNITÉ DE DÉCÈS OU D'UN HÉRITIER OU D'UN SUCCESSIBLE DE LA PERSONNE CONCERNÉE	22
8.4. TRAITEMENT DES PLAINTES	23
9. RESPONSABILITÉ	23
10. ENTRÉE EN VIGUEUR	23
ANNEXE	24

PRÉAMBULE

L'Université de Sherbrooke est responsable des renseignements personnels qu'elle détient dans l'exercice de ses fonctions. À ce titre, l'Université prend les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, l'Université de Sherbrooke a adopté les *Règles de gouvernance à l'égard des renseignements personnels* (Politique 2500-051). Ces règles prévoient qu'elles sont complétées par une directive visant à préciser les droits et obligations des personnes concernées et des membres de la communauté universitaire, de sorte à faciliter leur application et l'instauration de bonnes pratiques en matière de protection des renseignements personnels.

La présente *Directive relative à la protection des renseignements personnels* (la « Directive ») établit donc les principales mesures applicables aux cinq étapes du cycle de vie d'un renseignement personnel, soit :

- sa collecte, qu'il soit recueilli, créé ou inféré;
- son utilisation au sein de l'Université;
- sa communication à un tiers, lorsque permis;
- sa conservation, qu'il soit activement utilisé ou non;
- sa destruction lorsque ses fins sont accomplies, sous réserve des règles concernant les archives de l'Université.

La Directive précise de plus les modalités particulières à l'exercice des droits des personnes concernées par un renseignement personnel.

1. OBJECTIF

La Directive encadre la gestion des renseignements personnels détenus par l'Université dans l'exercice de ses fonctions et de ce fait, elle participe à la mise en œuvre des *Règles de gouvernance à l'égard des renseignements personnels* (Politique 2500-051) à chacune des étapes du cycle de vie d'un renseignement personnel.

La Directive poursuit donc les objectifs suivants :

- favoriser la protection des renseignements personnels de façon cohérente au sein de l'Université;
- limiter les incidents de confidentialité et le cas échéant, leur conséquence;
- préciser les droits et obligations des membres de la communauté universitaire et des personnes concernées relativement aux renseignements personnels.

2. CADRE LÉGAL ET NORMATIF

La Directive est adoptée en prenant en considération, notamment :

- la *Charte des droits et libertés de la personne*, RLRQ, c. C-12;
- le *Code civil du Québec*, RLRQ c. CCQ-1991;
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 (LADPRP) ainsi que les règlements qui en découlent;

- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ c. G-1.03;
- la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c. C-1.1;
- la *Loi sur les archives*, RLRQ, c. A-21.1;
- les *Règles de gouvernance à l'égard des renseignements personnels* (Politique 2500-051);
- la *Politique de sécurité de l'information* (Politique 2500-036);
- la *Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels* (Directive 2600-063);
- la *Politique relative à la gestion intégrée des documents administratifs et des archives historiques institutionnelles* (Politique 2500-050).

3. CHAMP D'APPLICATION

La Directive s'applique à tout renseignement personnel détenu par l'Université de Sherbrooke dans l'exercice de ses fonctions, que sa conservation soit assurée par l'Université ou par un tiers et quel que soit le support, de sa collecte à sa destruction.

Elle s'applique à toute personne liée ou ayant pu être liée à l'Université en tant que membre de la communauté universitaire et s'étend également à tout tiers de l'Université ayant accès à un renseignement personnel détenu par l'Université. Toutefois, cette Directive ne s'applique pas aux renseignements détenus par un membre de la communauté universitaire à des fins personnelles, même s'ils sont conservés sur une plateforme technologique de l'Université.

4. DÉFINITIONS

« **Anonymiser** » : action d'utiliser un ensemble de méthodes techniques et de processus organisationnels visant à transformer un renseignement personnel en un renseignement anonymisé.

« **Collecte** » : toute opération par laquelle un renseignement personnel est obtenu, incluant sa création.

« **Comité sur l'accès à l'information et la protection des renseignements personnels** » : comité formé en vertu des *Règles de gouvernance à l'égard des renseignements personnels* et chargé de soutenir l'Université et la personne responsable PRP dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la LADPRP (aussi appelé « CAIPRP »).

« **Communauté universitaire** » : ensemble des étudiantes et étudiants, des membres du personnel, des professeures associées ou professeurs associés, des membres d'une instance décrite dans les Statuts de l'Université de Sherbrooke, ainsi que toute personne accueillie en vertu d'une convention de travail, d'études ou de stage.

« **Communication** » : action de transférer, transmettre ou envoyer des renseignements à un tiers ou de donner accès à ceux-ci.

« **Confidentiel** » : propriété d'un renseignement de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulgué qu'à celles-ci.

« **Cycle de vie** » : ensemble des étapes que franchit un renseignement personnel, soit sa collecte, son utilisation, sa communication, sa conservation et sa destruction ou anonymisation.

« **Dépersonnaliser** » : action d'utiliser un ensemble de méthodes techniques et de processus organisationnels visant à transformer un renseignement personnel en un renseignement dépersonnalisé.

« **Données biométriques** » : toute caractéristique physique, biologique ou comportementale permettant d'identifier une personne physique. Cela inclut également tout renseignement produit à partir d'une telle caractéristique (par exemple : un code chiffré représentant le gabarit facial d'une personne).

« **Évaluation des facteurs relatifs à la vie privée** » ou « **EFVP** » : démarche qui consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées. La réalisation d'une EFVP doit être proportionnée à la sensibilité des renseignements personnels concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. Une EFVP est concluante lorsque a) il existe un lien rationnel entre les objectifs et la solution proposée (c'est-à-dire qu'il s'agit d'un moyen efficace d'atteindre l'objectif visé, cette efficacité étant basée sur des données concrètes et probantes), b) l'atteinte à la vie privée est minimale ou il n'y a pas d'autres solutions efficaces moins intrusives, c) les avantages concrets surpassent les conséquences ou les préjudices pour les personnes concernées.

« **Incident de confidentialité** » : accès, utilisation, communication d'un renseignement personnel non autorisé par la LADPRP, de même que sa perte ou toute autre forme d'atteinte à sa protection. En voici quelques exemples :

- un membre du personnel consulte des renseignements personnels non nécessaires à l'exercice de ses fonctions;
- un pirate informatique s'infiltré dans un système;
- une personne utilise des renseignements personnels d'une base de données à laquelle il a accès dans le cadre de ses fonctions dans le but d'usurper l'identité d'une personne;
- une communication est effectuée par erreur à la mauvaise personne;
- une personne perd ou se fait voler des documents contenant des renseignements personnels;
- une personne s'immisce dans une banque de données contenant des renseignements personnels afin de les altérer.

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

« **Organisme public** » : les organismes publics du Québec, notamment : le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères, les organismes gouvernementaux, les organismes municipaux, les organismes scolaires, dont les universités et les établissements de santé et de services sociaux.

« **Partenaire** » : un organisme public avec lequel l'Université collabore à l'occasion d'une collecte ou d'une communication nécessaire à l'exercice des attributions de l'organisme ou la mise en œuvre d'un programme pour la prestation de services ou la réalisation d'une mission commune.

« **Personnes concernées** » : personnes physiques concernées par un ou plusieurs renseignements personnels.

« **Prestataire** » : prestataire de service recevant des renseignements personnels de la part de l'Université dans le cadre de l'exécution d'un contrat de service ou d'un mandat, incluant les services à l'occasion d'un projet T.I.

« **Profilage** » : toute collecte ou utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la réussite académique, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.

« **Projet en T.I.** » : tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

« **Receveur** » : tiers recevant les renseignements personnels dans le cadre d'une communication.

« **Renseignement anonymisé** » : renseignement concernant une personne physique dont il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement la personne concernée. Un renseignement anonymisé n'est plus considéré être renseignement personnel.

« **Renseignement professionnel** » : renseignement personnel qui concerne l'exercice par la personne concernée d'une fonction au sein d'une entreprise tel que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail.

« **Renseignement dépersonnalisé** » : renseignement personnel qui ne permet plus d'identifier directement la personne concernée. La dépersonnalisation d'un renseignement personnel est réversible, contrairement à l'anonymisation qui est irréversible.

« **Renseignement personnel** » : tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier. Le nom d'une personne, pris isolément, n'est pas un renseignement personnel. Cependant, lorsque ce nom est associé ou jumelé à un autre renseignement visant cette même personne, il devient alors un renseignement personnel. Sont des exemples de renseignement personnel :

- le nom d'une personne et sa date de naissance;
- matricule étudiant et/ou code permanent;
- numéro d'assurance sociale;
- numéro de carte de crédit;
- numéro d'assurance maladie;
- renseignement de nature médicale ou financière;
- le nom d'une personne et son numéro de téléphone personnel;
- le nom d'une personne et son adresse de domicile;
- le nom d'une personne et ses résultats scolaires.

« **Renseignement sensible** » : renseignement personnel qui, par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, suscite un haut degré d'attente raisonnable en matière de vie privée. Il peut s'agir, par exemple, de renseignements médicaux, biométriques, génétiques ou financiers, ou de renseignements sur l'origine ethnique, les convictions politiques, l'orientation sexuelle, les convictions religieuses.

« **Responsable de la protection des renseignements personnels** » : les personnes assumant les rôles de secrétaire général et de secrétaire général adjoint (aussi appelé « personne responsable PRP »), ou tout autre membre du personnel de direction désigné par la rectrice ou le recteur.

« **Sécurité** » : le respect du niveau de confidentialité de l'information, tant sur le format numérique que papier, le maintien de son intégrité et de sa disponibilité tout au long de son cycle de vie.

« **Sous-traitant** » : toute personne, organisme ou autre entité recevant d'un prestataire, d'un receveur ou d'un partenaire des renseignements personnels qui lui ont été préalablement communiqués par l'Université.

« **Tiers** » : toute personne ou organisme ayant une personnalité juridique distincte de l'Université, incluant les fournisseurs, les sous-traitants, les prestataires de services ou d'autres partenaires de l'Université telle que La Fondation de l'Université de Sherbrooke, les associations étudiantes, les syndicats et les milieux de formation affiliés.

« **Utilisation** » : acte d'utiliser un renseignement personnel à l'interne de l'Université (par opposition à un tiers, à qui on communique un renseignement personnel).

5. MESURES APPLICABLES À TOUTES LES ÉTAPES DU CYCLE DE VIE DES RENSEIGNEMENTS PERSONNELS

5.1. Confidentialité des renseignements personnels

Un renseignement personnel détenu par l'Université est confidentiel, sauf dans les cas suivants :

- la personne concernée par ce renseignement consent à sa divulgation;
- il revêt un caractère public en vertu de la LADPRP, tel que précisé au paragraphe suivant.

À moins que leur divulgation ne soit de nature à nuire ou à entraver le travail d'une personne ou d'un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime, ou que la personne responsable des renseignements personnels ait des motifs raisonnables de croire que ces renseignements seront utilisés à des fins illégitimes, les renseignements personnels suivants ont un caractère public :

- le nom, le titre, la fonction, la classification, le traitement le cas échéant, l'adresse de courrier électronique et l'adresse et le numéro de téléphone du lieu de travail d'un membre du personnel de l'Université, et si applicable d'un membre de l'assemblée de l'Université ou de son conseil d'administration. Les règles particulières concernant le caractère public ou non du traitement de ces personnes sont prévues à la LADPRP ;
- un renseignement concernant une personne en sa qualité de partie à un contrat de service conclu avec l'Université, ainsi que les conditions de ce contrat.

5.2. Consentement des personnes concernées

5.2.1. Consentement obligatoire

La collecte, l'utilisation et la communication d'un renseignement personnel par l'Université est subordonné à l'obtention du consentement de la personne concernée, sauf lorsqu'expressément permis à la présente Directive.

Le consentement est obtenu au moment de la collecte. Il peut être complété, modifié ou retiré à tout moment par la suite, étant entendu qu'une telle modification ne vaut que pour l'avenir. Le refus de donner ou maintenir un consentement requis peut notamment entraîner la cessation du traitement d'un dossier, par exemple un dossier étudiant, celui relié à l'emploi ou celui relatif à une prestation de services.

5.2.2. Critères de validité du consentement

Tout consentement requis d'une personne concernée doit être manifeste, libre, éclairé et donné à des fins spécifiques. Le consentement lié à des renseignements sensibles doit être manifesté de manière expresse.

Le consentement ne vaut que pour la période nécessaire à la réalisation des fins auxquelles il a été demandé.

5.2.3. Consentement de la personne mineure

Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par le tuteur. Le consentement du mineur de 14 ans et plus est donné par le mineur, par le titulaire de l'autorité parentale ou par le tuteur.

5.3. Nécessité d'un renseignement personnel

Un renseignement personnel est collecté, utilisé, communiqué ou conservé par l'Université uniquement si cela est nécessaire à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont elle a la gestion. Un renseignement qui est nécessaire est obligatoirement utilisé par l'Université en temps pertinent. Un renseignement personnel qui n'est pas ou n'est plus nécessaire est détruit, sous réserve de l'application du calendrier de conservation de l'Université prévu à la *Loi sur les archives* ou du *Code des professions*.

5.4. Incident de confidentialité

5.4.1. Obligations en cas d'incident de confidentialité

Tout membre de la communauté universitaire ou tiers auxquels l'Université communique des renseignements personnels doit effectuer un signalement lorsqu'il a un motif raisonnable de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par l'Université. Pour ce faire, ce signalement doit être effectué sans délai au Centre d'aide et de soutien informatisé de l'Université (Casius) via la déclaration disponible sur le Site Web à l'adresse suivante : <https://www.usherbrooke.ca/securite-info/incidents-a-signaler/>.

En cas de panne du système Casius le signalement doit être fait suivant les modalités prévues sur le site Internet des mesures d'urgence, à l'adresse suivante : <https://www.usherbrooke.ca/urgence/>.

Le membre du personnel de l'Université qui a un motif raisonnable de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par l'Université doit aussi aviser son supérieur hiérarchique sans délai.

Tout membre de la communauté universitaire ou tiers auxquels l'Université communique des renseignements personnels doivent collaborer à l'analyse de l'incident.

5.4.2. Rôle et responsabilités

La gestion d'un incident de confidentialité à l'Université est attribuée aux personnes suivantes en raison des fonctions qu'elles exercent. La gestion d'un tel incident peut être complétée par les plans de mesures d'urgence suivant le niveau de criticité.

5.4.2.1. Secrétaire générale ou secrétaire général

Lors d'un incident de confidentialité impliquant des renseignements personnels sensibles, la secrétaire générale ou le secrétaire général en saisit, sans délai, le membre du comité de direction responsable de la gestion des mesures d'urgence afin de déterminer le niveau de criticité et de gérer les risques à court et moyen terme de cet événement, dont déclencher les plans de mesures d'urgence, le cas échéant.

En cas d'incident de confidentialité, la secrétaire générale ou le secrétaire général prend en charge le traitement de l'incident et s'associe avec la personne chef de la sécurité de l'information organisationnelle ainsi que toute autre personne utile selon la nature de l'incident, incluant une conseillère ou un conseiller juridique.

À ce titre, la secrétaire générale ou le secrétaire général :

- évalue le risque qu'un préjudice soit causé et en détermine le degré de sévérité. Lors de cette évaluation, sont considérées notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables;
- avise, avec diligence, la personne dont un renseignement personnel est concerné par l'incident, lorsqu'il présente un risque qu'un préjudice sérieux soit causé, sauf lorsque cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois. Cet avis doit contenir les renseignements suivants :
 - une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
 - une brève description des circonstances de l'incident;
 - la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
 - une brève description des mesures que l'organisation a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;
 - les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;
 - les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

L'avis est transmis à la personne concernée par l'incident de confidentialité. Toutefois, l'avis est donné au moyen d'un avis public dans l'une ou l'autre des circonstances suivantes :

- lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;
- lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'Université;
- lorsque l'Université n'a pas les coordonnées de la personne concernée.

Par ailleurs, afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou afin d'atténuer un tel préjudice, l'avis à la personne concernée peut également être donné au moyen d'un avis public. Dans ce cas, l'Université demeure toutefois tenue de transmettre, avec diligence, un avis à la personne concernée, à moins que l'une des circonstances énoncées précédemment ne s'applique à sa situation.

Un avis public peut être fait par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée;

- avise, le cas échéant, toute personne ou tout organisme susceptible de diminuer le risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin, sans le consentement de la personne concernée. Cette communication est enregistrée;
- prend les mesures visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que des nouveaux incidents de même nature ne se produisent;
- avise, avec diligence et par écrit, la Commission d'accès à l'information de l'incident de confidentialité lorsqu'il présente un risque qu'un préjudice sérieux soit causé. Le formulaire d'avis de la Commission d'accès à l'information précise les informations à fournir;
- avise, avec diligence, la personne responsable des contacts avec les assureurs, le cas échéant;
- inscrit l'incident de confidentialité dans un registre prévu à cet effet;
- sur demande de la Commission d'accès à l'information, transmet une copie de ce registre.

5.4.2.2. Chef de la sécurité de l'information organisationnelle

Le chef de la sécurité de l'information organisationnelle soutient la secrétaire générale ou le secrétaire général en contribuant notamment à la mise en place des processus de sécurité de l'information et à la mise en œuvre des mesures d'atténuation des risques.

5.4.2.3. Conseillère ou conseiller sectoriel en gestion des incidents

La conseillère ou le conseiller sectoriel en gestion des incidents est impliqué dans la gestion d'un incident de sécurité de l'information. Dans le cadre d'un incident de confidentialité, son rôle est notamment de :

- contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information;
- tenir à jour le registre des incidents de sécurité de l'information ayant pu mettre en péril la sécurité de l'information, de documenter ces incidents et d'en tenir informé la directrice ou le directeur de la sécurité de l'information ainsi que la secrétaire générale ou le secrétaire général;
- contribuer aux analyses de risques de sécurité de l'information afin d'identifier les menaces et les situations de vulnérabilité et de mettre en place les solutions appropriées.

5.4.3. Registre des incidents de confidentialité

L'Université tient un registre des incidents de confidentialité.

Les renseignements contenus au registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle l'Université a pris connaissance de l'incident.

6. MESURES APPLICABLES AUX CINQ ÉTAPES DU CYCLE DE VIE DES RENSEIGNEMENTS PERSONNELS

6.1. COLLECTE des renseignements personnels

L'Université, ou quiconque en son nom, peut recueillir un renseignement personnel que si cela est nécessaire à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont elle a la gestion. L'Université peut également recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme d'un autre organisme public.

L'Université limite la collecte des renseignements personnels à ce qui est nécessaire pour accomplir les fins spécifiques et déterminées préalablement à cette collecte, et procède à la collecte par l'intermédiaire de moyens qui sont portés à la connaissance des personnes concernées.

6.1.1. Mesures liées à la collecte

Lors de la collecte, l'Université ou quiconque collectant des renseignements en son nom doit :

- demander le consentement des personnes concernées avant de recueillir leurs renseignements personnels en appliquant les obligations prévues au paragraphe 5.2, à moins que la LADPRP ou une autre loi applicable ne permette de les recueillir sans un tel consentement;

- transmettre aux personnes concernées les informations suivantes :
 - (a) le nom de la personne pour le compte duquel la collecte est faite si ce n'est pas l'Université;
 - (b) les fins auxquelles ces renseignements sont recueillis;
 - (c) les moyens par lesquels les renseignements sont recueillis;
 - (d) le caractère obligatoire ou facultatif de la demande;
 - (e) les conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande ou, le cas échéant, d'un retrait de son consentement à la communication ou à l'utilisation des renseignements recueillis suivant une demande facultative;
 - (f) les droits d'accès et de rectification prévus par la LADPRP et la présente directive. Lorsqu'applicable, la personne concernée est aussi informée de :
 - (g) l'identité du tiers qui recueille les renseignements au nom de l'Université;
 - (h) du nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer les renseignements aux fins visées au sous-paragraphe (b);
 - (i) de la possibilité que les renseignements soient communiqués à l'extérieur du Québec.

Dans l'éventualité où l'Université recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie, tels les témoins de connexion, comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage, elle doit, au préalable, l'informer du recours à une telle technologie et des moyens offerts pour activer ou désactiver de telles fonctions.

Lorsque l'Université recueille des renseignements personnels en offrant au public un produit ou un service technologique disposant de paramètres de confidentialité autres que ceux d'un témoin de connexion, elle voit à ce que, par défaut, ces paramètres assurent le plus haut niveau de confidentialité sans intervention de la personne concernée.

Une politique de confidentialité concernant la collecte de renseignements personnels recueillis par un moyen technologique est publiée sur le site internet de l'Université et diffusée par des moyens propres à atteindre les personnes concernées. Cette politique vise notamment à informer les utilisateurs des échanges de renseignements lors de l'accès à une plateforme électronique de l'Université, des tiers qui ont accès à ces renseignements et des mesures de confidentialité et de sécurité prises par l'Université à leur égard.

L'Université prend les moyens raisonnables pour diminuer les inexactitudes dans les renseignements personnels recueillis.

6.1.2. Mesures liées à la biométrie

Dans l'éventualité où l'Université procède à la vérification ou à la confirmation de l'identité d'une personne au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques, elle s'assure :

- d'avoir obtenu le consentement exprès de la personne concernée;
- d'avoir préalablement divulgué l'existence de ce procédé à la Commission d'accès à l'information;
- que cette vérification ou confirmation d'identité soit réalisée en faisant appel au minimum de caractéristiques ou de mesures biométriques permettant de relier la personne concernée à l'action qu'elle pose;
- que ces caractéristiques ou mesures biométriques ainsi que toute note les concernant soient détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus;

- que tout autre renseignement concernant la personne concernée qui pourrait être découvert à partir des caractéristiques ou mesures biométriques saisies ne puisse servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit.

Dans l'éventualité où l'Université procède à la création d'une banque de caractéristiques ou de mesures biométriques, elle s'assure que la création de cette banque soit divulguée à la Commission d'accès à l'information au moins 60 jours avant sa mise en service.

6.1.3. Mesures liées aux sondages

Avant de recueillir des renseignements personnels dans le cadre d'un sondage, l'Université doit :

- procéder à une évaluation de la nécessité d'y recourir; et
- procéder à une évaluation de l'aspect éthique du sondage par un comité d'éthique s'il s'agit d'un sondage lié à un projet de recherche ou, à défaut, par la personne responsable des renseignements personnels en tenant compte notamment de la nature du sondage, des personnes visées, de la sensibilité des renseignements personnels recueillis et de la finalité de l'utilisation de ceux-ci.

L'Université s'assure que les tiers agissant pour son compte prennent des mesures de sécurité adéquates à l'égard des renseignements personnels recueillis, notamment en prévoyant les dispositions requises à la section 6.3.1.3 dans le contrat de service conclut préalablement à la réalisation du sondage prévu.

6.1.4. Mesures liées à la collecte pour le compte d'un partenaire

L'Université peut recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme d'un partenaire ou, inversement, un partenaire peut recueillir un renseignement personnel pour l'Université si cela est nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme de l'Université.

Avant de ce faire, le membre de la communauté universitaire voulant collecter un renseignement personnel ou déléguer cette tâche à un partenaire à cette fin doit contacter la personne responsable PRP à l'adresse rprp@usherbrooke.ca.

La personne responsable PRP analysera ensuite si cette collecte est conforme en procédant à une évaluation des facteurs relatifs à la vie privée.

La personne responsable PRP rend sa décision par écrit et informe la personne ou le partenaire ayant fait la demande; cette décision ne dispense pas le partenaire d'obtenir les autorisations requises de son organisme, ainsi que de suivre les autres procédures qui lui sont applicables.

Si la personne responsable PRP autorise la collecte des renseignements personnels suivant son EFVP, une entente écrite comprenant minimalement les clauses suivantes doit être conclue entre l'Université et le partenaire :

- les fins pour lesquelles le renseignement est recueilli;
- la nature ou le type du renseignement recueilli;
- les moyens par lesquels le renseignement est recueilli;
- les mesures propres à assurer la protection du renseignement personnel;
- la périodicité de la collecte; et
- la durée de l'entente.

Une fois signée par les deux parties, la personne responsable PRP transmet l'entente autorisant la collecte par l'Université à la Commission d'accès à l'information. Cette entente entre en vigueur trente (30) jours après sa réception par la Commission d'accès à l'information.

L'Université ou un membre de la communauté universitaire peut débiter la collecte de renseignements personnels uniquement à l'expiration du délai de trente (30) jours, à moins que la Commission d'accès à l'information n'ait formulé une objection dans ce délai.

Lorsqu'un membre de la communauté universitaire collecte des renseignements personnels aux fins mentionnées ci-dessus, il doit s'assurer que la personne responsable PRP ait les informations nécessaires pour que cette dernière puisse inscrire cette collecte au registre approprié, en lui précisant :

- le nom de l'organisme pour lequel les renseignements sont recueillis;
- l'identification du programme ou de l'attribution pour lequel les renseignements sont nécessaires;
- la nature ou le type de la prestation de service ou de la mission;
- la nature ou le type de renseignements recueillis;
- la fin pour laquelle ces renseignements sont recueillis;
- la catégorie de personnes, au sein de l'organisme qui recueille les renseignements et au sein de l'organisme recevoir, qui a accès aux renseignements.

6.2. UTILISATION des renseignements personnels

Un renseignement personnel ne peut être utilisé au sein de l'Université qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée ou lorsque la loi le permet.

Chaque membre du personnel de l'Université n'utilise que les renseignements personnels nécessaires à l'exercice de ses fonctions. De plus, chaque membre du personnel de l'Université qui utilise des renseignements personnels est tenu à la confidentialité de ceux-ci.

6.2.1. Mesures lors d'une utilisation sans le consentement de la personne concernée

L'Université peut utiliser un renseignement à une autre fin que celle pour laquelle il a été collecté, sans le consentement de la personne concernée, dans les seuls cas suivants :

- lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli, c'est-à-dire, qu'il doit y avoir un lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli;
- lorsque son utilisation est manifestement au bénéfice de la personne concernée;
- lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi;
- lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques pour l'Université et qu'il est dépersonnalisé.

Lorsqu'un membre de la communauté universitaire utilise un renseignement personnel au nom de l'Université aux trois premières fins mentionnées ci-dessus, il doit écrire à la personne responsable PRP à l'adresse rpr@usherbrooke.ca afin d'inscrire cette utilisation dans le registre approprié, en l'informant des points suivants :

- la fin pour laquelle ce renseignement est utilisé (qui doit faire partie des exceptions énumérées);
- la catégorie de personnes qui a accès au renseignement aux fins de l'utilisation indiquée.

6.2.2. Mesures liées aux décisions fondées sur un traitement automatisé

Dans l'éventualité où l'Université utilise des renseignements personnels pour rendre une décision fondée exclusivement sur un traitement automatisé de ceux-ci, elle doit en informer la personne concernée au plus tard au moment où elle l'informe de cette décision.

Une fois la décision rendue et sur demande, la personne concernée est informée (a) des renseignements personnels utilisés pour rendre la décision ; (b) des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision ; et (c) de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.

L'Université doit donner à toute personne visée par une décision fondée exclusivement sur un traitement automatisé, l'occasion de présenter ses observations écrites à un membre de son personnel en mesure de réviser la décision.

6.3. COMMUNICATION des renseignements personnels

Une communication de renseignements personnels peut être effectuée par l'Université avec le consentement de la personne concernée ou lorsque la loi l'exige ou le permet.

Toute communication de renseignements personnels par l'Université ne doit contenir que les renseignements personnels nécessaires à l'atteinte de fins spécifiques et déterminées préalablement à cette communication. L'Université prend des moyens raisonnables pour vérifier que les tiers receveurs de renseignements personnels respectent des mesures permettant de maintenir la confidentialité, l'intégrité et la disponibilité des renseignements communiqués.

6.3.1. Mesures de communication sans le consentement de la personne concernée

Une communication de renseignements personnels peut être effectuée par l'Université sans le consentement de la personne concernée, lorsque la LADPRP l'exige ou le permet. Dans ce cas, des exigences supplémentaires sont requises et plus amplement décrites dans la présente section.

6.3.1.1. Communication sans le consentement de la personne concernée à des fins juridiques ou d'identification

L'Université peut communiquer des renseignements personnels, sans le consentement des personnes concernées, mais après avoir consulté la personne responsable PRP sauf en cas d'urgence, lors des circonstances suivantes :

- au procureur de l'Université, au directeur des poursuites criminelles et pénales, à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, uniquement si les renseignements personnels sont nécessaires aux fins, selon le cas, d'une poursuite pour infraction à une loi applicable au Québec ou pour d'une procédure judiciaire;
- à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police ou par une personne ou un organisme agissant en application d'une loi qui exige un rapport de même nature, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement;

- à toute personne ou organisme si cette communication est nécessaire à l'application d'une loi au Québec, ou à l'application d'une convention collective, d'un décret, d'un arrêté, d'une directive ou d'un règlement qui établissent des conditions de travail;
- communiquer un renseignement sur l'identité d'une personne afin de recueillir des renseignements personnels déjà colligés par un tiers, uniquement si la personne responsable PRP a informé la Commission d'accès à l'information au préalable.

Lorsqu'un membre de la communauté universitaire communique un renseignement personnel pour l'Université aux fins mentionnées ci-dessus, il doit écrire à la personne responsable PRP à l'adresse rprp@usherbrooke.ca afin d'inscrire cette communication dans le registre approprié, en l'informant des points suivants :

- la nature ou le type de renseignement communiqué;
- la personne ou l'organisme qui reçoit la communication;
- la fin pour laquelle ce renseignement est communiqué et préciser si ces renseignements personnels ont été communiqués à l'extérieur du Québec.

6.3.1.2. Communication sans le consentement de la personne concernée en vue d'assurer la protection des personnes lors d'une situation d'urgence

L'Université peut communiquer des renseignements personnels, sans le consentement des personnes concernées, en vue d'assurer la protection des personnes, dans les deux cas et aux conditions qui suivent :

- 1- à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée, uniquement lorsque l'Université s'est assurée du caractère urgent et dangereux de la situation;
- 2- à une personne exposée à un danger, son représentant ou toute autre personne susceptible de pouvoir leur porter secours, en vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence. On entend par « blessures graves » toute blessure physique ou psychologique qui nuit d'une manière importante à l'intégrité physique, à la santé ou au bien-être d'une personne ou d'un groupe de personnes identifiable.

La secrétaire générale ou le secrétaire général autorise préalablement toute communication de renseignements personnels, à moins qu'une situation grave et immédiate requière une communication sur-le-champ, auquel cas un avis lui en est donné dès que possible.

En l'absence de la secrétaire générale ou du secrétaire général, la vice-rectrice ou le vice-recteur de qui relève les ressources humaines peut agir en son nom.

La secrétaire générale ou le secrétaire général peut consulter toutes personnes dont l'avis ou les informations qu'elles possèdent seraient utiles à la prise de décision, dont la direction du service ou de la faculté concernée le cas échéant.

La secrétaire générale ou le secrétaire général inscrit cette communication dans le registre approprié.

6.3.1.3. Communication sans le consentement de la personne concernée pour l'exercice d'un mandat ou l'exécution d'un contrat de service ou d'entreprise

L'Université peut communiquer des renseignements personnels, sans le consentement des personnes concernées, si cette communication est nécessaire à l'exercice d'un mandat ou à

l'exécution d'un contrat de service ou d'entreprise confié par l'Université à un tiers, à condition que ce mandat ou contrat soit confié par écrit.

Lorsque le tiers receveur n'est pas un organisme public ou un membre d'un ordre professionnel, le mandat ou contrat doit contenir minimalement les éléments suivants :

- les dispositions de la LADPRP qui s'appliquent aux renseignements personnels communiqués;
- les mesures que doit prendre le tiers cocontractant pour assurer le caractère confidentiel des renseignements personnels;
- la confirmation que le tiers cocontractant utilisera les renseignements personnels que dans l'exercice de son mandat ou l'exécution de son contrat et qu'il ne conservera pas ceux-ci après un délai d'expiration préalablement déterminé;
- l'obligation du tiers d'informer l'Université sans délai de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement personnel communiqué et de tout Incident de confidentialité;
- une annexe comprenant un engagement de confidentialité de toutes personnes qui pourraient avoir accès aux renseignements personnels chez le tiers, à moins que la personne responsable PRP estime que cela n'est pas nécessaire.

Lorsqu'un membre de la communauté universitaire communique un renseignement personnel pour l'Université aux fins mentionnées ci-dessus, il doit écrire à la personne responsable PRP à l'adresse rprp@usherbrooke.ca afin d'inscrire cette communication dans le registre approprié en l'informant des points suivants :

- la nature ou le type de renseignement communiqué;
- la personne ou l'organisme qui reçoit la communication;
- la fin pour laquelle ce renseignement est communiqué et préciser si ces renseignements personnels ont été communiqués à l'extérieur du Québec.

Le membre doit également lui envoyer une copie signée du mandat ou du contrat.

6.3.1.4. Communication sans le consentement de la personne concernée pour des fins d'études, de recherches ou de productions de statistiques

Lorsqu'un tiers souhaite obtenir la communication de renseignements personnels pour les utiliser à des fins d'études, de recherches ou de production de statistiques ou lorsque l'Université ou ses membres en son nom veut communiquer à un tiers ces renseignements pour les mêmes fins, le tiers doit faire une demande écrite à l'attention de la personne responsable PRP à l'adresse rprp@usherbrooke.ca en remplissant le formulaire *Demande d'utilisation de renseignements personnels à des fins d'études, de recherches ou de production de statistiques sans le consentement des personnes concernées*.¹

La personne responsable PRP analysera ensuite si ces renseignements peuvent être communiqués tel que demandé en procédant à une évaluation des facteurs relatifs à la vie privée. Avant d'autoriser la communication de renseignements personnels, la personne responsable PRP devra conclure que :

¹ La communication de renseignements personnels contenus dans les fonds d'archives privés de l'Université est régie par des règles particulières dont la gestion est assumée par la section des archives du Service des bibliothèques et archives de l'Université de Sherbrooke.

- l'objectif de l'étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes concernées (si l'objectif de l'étude, la recherche ou la production de statistiques peut être atteint en utilisant des renseignements personnels anonymisés, alors cette forme doit être privilégiée et les renseignements personnels ne doivent pas être communiqués);
- il est déraisonnable d'exiger que la personne ou l'organisme obtienne le consentement des personnes concernées par les renseignements personnels (s'il n'est pas déraisonnable d'obtenir le consentement, alors la personne ou l'organisme devra l'obtenir des personnes concernées);
- l'objectif de l'étude, de la recherche ou de la production de statistiques l'emporte, eu égard à l'intérêt public, sur l'impact de la communication et de l'utilisation des renseignements sur la vie privée des personnes concernées (si ce n'est pas le cas, la communication sera refusée);
- les renseignements personnels sont utilisés de manière à en assurer la confidentialité (si ce n'est pas le cas, la communication sera refusée ou des mesures de protection supplémentaires devront être mises en place pour assurer le maintien du caractère confidentiel des renseignements personnels); et
- seuls les renseignements personnels nécessaires sont communiqués.

La personne responsable PRP rend sa décision par écrit et informe la personne ou l'organisme ayant fait la demande.

Si la personne responsable PRP autorise la communication des renseignements personnels suivant son EFVP, une entente de communication comprenant minimalement les clauses suivantes doit être conclue entre l'Université et le tiers receveur :

- stipulant que les renseignements personnels :
 - ne peuvent être rendus accessibles qu'aux personnes à qui leur connaissance est nécessaire à l'exercice de leurs fonctions et ayant signé un engagement de confidentialité;
 - ne peuvent être utilisés à des fins différentes de celles prévues à la présentation détaillée des activités de recherche;
 - ne peuvent être appariés avec tout autre fichier de renseignements non prévu à la présentation détaillée des activités de recherche;
 - ne peuvent être communiqués, publiés ou autrement diffusés sous une forme permettant d'identifier les personnes concernées.
- prévoyant les informations devant être communiquées aux personnes concernées lorsque les renseignements les concernant sont utilisés pour les rejoindre en vue de leur participation à l'étude ou à la recherche;
- prévoyant des mesures pour assurer la protection des renseignements;
- déterminant un délai de conservation des renseignements;
- prévoyant l'obligation d'aviser l'Université de la destruction des renseignements de façon sécuritaire;
- prévoyant que l'Université et la Commission d'accès à l'information doivent être avisées sans délai :
 - du non-respect de toute condition prévue à l'entente;
 - de tout manquement aux mesures de protection prévues à l'entente;
 - de tout événement susceptible de porter atteinte à la confidentialité des renseignements.

Sur demande, la personne responsable PRP peut transmettre un modèle d'entente comprenant les clauses ci-dessus.

Une fois signée par les deux parties, la personne responsable PRP transmet l'entente à la Commission d'accès à l'information. Cette entente entre en vigueur trente (30) jours après sa réception par la Commission d'accès à l'information.

L'Université ou un membre de la communauté universitaire au nom de l'Université peut communiquer les renseignements personnels demandés uniquement à l'expiration du délai de trente (30) jours, à moins que la Commission d'accès à l'information n'ait formulé une objection dans ce délai.

Lorsqu'un membre de la communauté universitaire communique un renseignement personnel pour l'Université aux fins mentionnées ci-dessus, il doit s'assurer que la personne responsable PRP ait les informations nécessaires pour que cette dernière puisse inscrire cette communication au registre approprié, en lui précisant :

- la nature ou le type de renseignement communiqué;
- la personne ou l'organisme qui reçoit cette communication;
- la fin pour laquelle ce renseignement est communiqué (ici, pour fin d'études, de recherches ou de production de statistiques) et préciser si ces renseignements personnels ont été communiqués à l'extérieur du Québec; et
- la raison justifiant cette communication.

6.3.1.5. Communication sans le consentement de la personne concernée à un organisme public ou un organisme d'un autre gouvernement pour l'exercice des attributions de cet organisme, la mise en œuvre d'un programme ou la prestation d'un service

L'Université peut communiquer des renseignements personnels sans le consentement de la personne concernée à certains tiers pour les raisons suivantes :

- à un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en œuvre d'un programme dont cet organisme a la gestion ou lorsque la communication est manifestement au bénéfice de la personne concernée;
- à un tiers lorsque des circonstances exceptionnelles le justifient;
- à un tiers si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne.

Lorsqu'un membre de la communauté universitaire communique un renseignement personnel pour l'Université aux fins mentionnées ci-dessus, il doit écrire à la personne responsable PRP à l'adresse rprp@usherbrooke.ca afin que cette dernière détermine si ces renseignements peuvent être communiqués tel que demandé, en procédant à une évaluation des facteurs relatifs à la vie privée.

Avant d'autoriser la communication de renseignements personnels, la personne responsable PRP devra conclure que :

- l'objectif visé ne peut être atteint que si les renseignements personnels sont communiqués sous une forme permettant d'identifier la personne concernée;
- il est déraisonnable d'exiger l'obtention du consentement de la personne concernée;
- l'objectif pour lequel la communication est requise l'emporte, eu égard à l'intérêt public, sur l'impact de la communication et de l'utilisation du renseignement sur la vie privée de la personne concernée; et
- les renseignements personnels sont utilisés de manière à en assurer la confidentialité.

La personne responsable PRP rend sa décision par écrit.

Si la personne responsable PRP autorise la communication des renseignements personnels suivant son EFVP, une entente de communication comprenant minimalement les clauses suivantes doit être conclue entre l'Université et le tiers receveur :

- identification du tiers à qui sont communiqués les renseignements personnels;
- les fins pour lesquelles les renseignements personnels sont communiqués;
- la nature du renseignement communiqué;
- le mode de communication utilisé;
- les mesures de sécurité propres à assurer la protection du renseignement personnel;
- la périodicité de la communication, si applicable;
- la durée de l'entente.

Sur demande, la personne responsable PRP peut transmettre un modèle d'entente comprenant les clauses ci-dessus.

Une fois signée par les deux parties, la personne responsable PRP transmet l'entente à la Commission d'accès à l'information. Cette entente entre en vigueur trente (30) jours après sa réception par la Commission d'accès à l'information.

L'Université ou un membre de la communauté universitaire agissant en son nom peut communiquer les renseignements personnels demandés uniquement à l'expiration du délai de trente (30) jours, à moins que la Commission d'accès à l'information n'ait formulé une objection dans ce délai.

Lorsqu'un membre de la communauté universitaire communique un renseignement personnel pour l'Université aux fins mentionnées ci-dessus, il doit s'assurer que la personne responsable PRP ait les informations nécessaires pour que cette dernière puisse inscrire cette communication au registre approprié, en lui précisant :

- la nature ou le type de renseignement communiqué;
- la personne ou l'organisme qui reçoit cette communication;
- la fin pour laquelle ce renseignement est communiqué et préciser si ces renseignements personnels ont été communiqués à l'extérieur du Québec; et
- la raison justifiant cette communication.

6.3.2. Mesures de communication de renseignements personnels à l'extérieur du Québec

Lorsqu'un membre de la communauté universitaire communique un renseignement personnel à l'extérieur du Québec pour l'Université, avec ou sans le consentement de la personne concernée, il doit écrire à la personne responsable PRP à l'adresse rprp@usherbrooke.ca afin que cette dernière détermine si ces renseignements peuvent être communiqués tel que demandé, en procédant à une évaluation des facteurs relatifs à la vie privée.

Avant d'autoriser la communication de renseignements personnels à l'extérieur du Québec, la personne responsable PRP devra tenir compte de la sensibilité du renseignement, de la finalité de son utilisation, des mesures de protection dont bénéficierait le renseignement et le régime juridique applicable à l'endroit où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables.

La personne responsable PRP rend sa décision par écrit.

Si la personne responsable PRP autorise la communication à l'extérieur du Québec des renseignements personnels suivant son EFVP, une entente de communication doit être conclue entre l'Université et le tiers receveur, laquelle entente doit tenir compte des résultats de l'EFVP et

des modalités convenues avec la personne responsable PRP pour atténuer les risques identifiés dans cette EFVP.

Sur demande, la personne responsable PRP peut transmettre un modèle de clause.

L'Université ou un membre de la communauté universitaire peut communiquer les renseignements personnels demandés uniquement lorsque l'entente est signée par les deux parties.

Lorsqu'un membre de la communauté universitaire communique un renseignement personnel à l'extérieur du Québec pour l'Université, il doit s'assurer que la personne responsable PRP ait les informations nécessaires pour que cette dernière puisse inscrire cette communication au registre approprié, et doit également lui envoyer une copie signée de l'entente de communication.

6.4. CONSERVATION des renseignements personnels

La conservation réfère à la période durant laquelle l'Université garde des renseignements personnels, sous quelque forme que ce soit, peu importe que les renseignements soient activement utilisés ou non.

L'Université conserve les renseignements personnels pour la durée déterminée aux règles de son calendrier de conservation en conformité avec les lois applicables, notamment la *Loi sur les archives* et le *Code des professions*.

L'Université prend les mesures raisonnables pour assurer la sécurité des renseignements personnels durant la période où ils sont conservés.

6.5. DESTRUCTION et anonymisation des renseignements personnels

Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'Université doit le détruire, ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la *Loi sur les archives* ou du *Code des professions*.

Lorsqu'elle souhaite transformer un renseignement personnel en renseignement anonymisé, l'Université doit le faire selon les meilleures pratiques généralement reconnues et, le cas échéant, selon les critères et modalités déterminés par un règlement du gouvernement.

7. MESURES PARTICULIÈRES LORS D'UN PROJET DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES

L'Université procède à une EFVP lors de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Les projets visés concernent, entre autres, des bases de données, des logiciels d'application, des vidéos de surveillance. La réalisation de cette évaluation doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

Aux fins de cette évaluation, l'Université consulte dès le début du projet le CAIPRP. Le CAIPRP détermine des catégories de projets. Pour chaque catégorie déterminée, un sous-comité possédant une expertise pertinente sur la question reçoit l'EFVP effectuée et au besoin, traite dans les meilleurs délais toute problématique reliée à cette évaluation; ce sous-comité s'adjoint toute personne invitée dont l'expertise est requise. Les comptes-rendus d'un sous-comité sont déposés au CAIPRP.

L'Annexe schématise les différentes étapes et les différents éléments à considérer pour protéger les renseignements personnels lors d'un projet de conception d'un système d'information ou de prestation électronique de services. L'Université s'assure également que le projet permet qu'un renseignement

personnel informatisé recueilli auprès de la personne concernée pourrait lui être communiqué dans un format structuré et couramment utilisé.

À toute étape d'un tel projet, le CAIPRP peut suggérer des mesures de protection des renseignements personnels applicables à ce projet telles que :

- la nomination d'une personne responsable de la mise en œuvre des mesures de protection des renseignements personnels;
- des mesures de protection des renseignements personnels dans tout document relatif au projet, tel qu'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 personnes participantes au projet.

8. MODALITÉS D'EXERCICE DES DROITS DES PERSONNES CONCERNÉES

8.1. Exercice des droits d'accès et de rectification

À l'égard des renseignements personnels qui la concernent, toute personne concernée a les droits suivants :

- d'obtenir l'information visée à la section 6.1 lors de leur collecte;
- d'être informée de leur existence au sein d'un fichier de l'Université;
- d'y accéder et d'en obtenir communication. Plus précisément, la personne concernée qui a le droit d'accéder à un renseignement personnel peut le faire sur place pendant les heures habituelles de travail ou à distance. Elle peut également en obtenir une copie et demander à ce qu'un renseignement personnel informatisé lui soit communiqué sous la forme d'une transcription écrite ou intelligible. L'exercice de ce droit est gratuit;
- de les faire corriger et compléter. Plus précisément, la personne concernée qui reçoit confirmation de l'existence d'un document comprenant 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 LADPRP, exiger que ce document soit rectifié. Si une telle demande est refusée, la personne concernée peut demander que la demande soit enregistrée. Si une telle demande est acceptée, l'Université délivre sans frais à la personne concernée, une copie de tout renseignement personnel modifié ou ajouté, ou, selon le cas, une attestation du retrait d'un renseignement personnel;
- d'être informée d'un incident de confidentialité qui peut lui causer un préjudice sérieux;
- de restreindre ou retirer son consentement à la collecte, l'utilisation ou la communication des renseignements personnels ou de les faire supprimer, si la loi le permet.

Pour exercer les droits d'accès et de rectification ci-dessus, la personne concernée doit faire sa demande par écrit et justifier son identité à titre de personne concernée, à titre de représentant, d'héritier ou de successible de cette dernière, à titre 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 conjoint ou de proche d'une personne décédée. La demande doit être adressée à la personne responsable PRP par courriel à l'adresse suivante : rprp@USherbrooke.ca; elle doit inclure les éléments énoncés aux paragraphes 8.2 ou 8.3 si la situation s'applique.

L'Université répond à toute demande d'exercice de droit dans les 20 jours suivants sa réception, sauf lorsque la LADPRP permet une extension de ce délai. Toute extension du délai devra se faire par avis écrit donné à la personne requérante dans le délai prévu. La personne responsable PRP rend sa décision par écrit et en transmet une copie à la personne requérante. La personne responsable PRP doit motiver tout refus d'accéder à une demande et indiquer la disposition de la LADPRP sur laquelle ce refus s'appuie. Elle doit également prêter assistance à la personne requérante qui le demande pour l'aider à comprendre sa

décision et l'informer du recours en révision et du droit d'appel prévus à la LADPRP et du délai pour les exercer.

8.2. Exigences particulières lors d'une demande de renseignement personnel ou de rectification d'une conjointe ou d'un conjoint ou d'un proche parent de la personne concernée dans son processus de deuil

L'Université peut communiquer au conjoint ou au proche parent d'une personne décédée un renseignement personnel qu'elle détient concernant cette personne, si la connaissance de ce renseignement personnel est susceptible d'aider la personne requérante dans son processus de deuil et que la personne décédée n'a pas consigné par écrit son refus d'accorder ce droit d'accès.

La demande écrite doit contenir les éléments suivants :

- identification de la personne requérante à titre de conjoint ou de proche parent en fournissant un document faisant état de son lien avec la personne décédée, par exemple, un certificat de mariage ou d'union civile, une preuve de résidence à la même adresse, un certificat de naissance ou tout autre document permettant d'établir son lien familial;
- renseignements personnels pour l'identification de la personne décédée en fournissant un document faisant état du décès, par exemple, un certificat de décès ou une publication de décès;
- description des informations demandées;
- illustration de la façon dont ces renseignements sont susceptibles d'aider la personne requérante dans son processus de deuil.

8.3. Exigence particulière lors d'une demande de renseignement personnel ou de rectification du liquidateur de la succession, du bénéficiaire d'une assurance vie ou d'une indemnité de décès ou d'un héritier ou d'un successible de la personne concernée

L'Université peut communiquer au liquidateur de la succession, au bénéficiaire d'une assurance vie ou d'une indemnité de décès ou à un héritier ou un successible de la personne concernée décédée un renseignement personnel qu'elle détient concernant cette personne, que dans la mesure où cette communication met en cause ses intérêts ou ses droits à titre de liquidateur, de bénéficiaire, d'héritier ou de successible.

La demande écrite doit contenir les éléments suivants :

- Identification de la personne requérante à titre de liquidateur, bénéficiaire, héritier ou successible et renseignements personnels pour l'identification de la personne décédée :
 - La ou le titulaire de l'autorité parentale, dans le cas d'une personne mineure décédée, doit transmettre :
 - un certificat de décès;
 - un certificat de naissance ou le jugement d'adoption.
 - La liquidatrice ou le liquidateur de la succession désigné dans un testament doit fournir :
 - un certificat de décès;
 - un testament;
 - deux certificats de recherche testamentaire, délivrés par la Chambre des notaires du Québec et par le Barreau du Québec, pour confirmer qu'il s'agit du dernier testament.
 - La liquidatrice ou le liquidateur de la succession sans testament doit joindre :
 - un certificat de décès;

- deux certificats de recherche testamentaire, délivrés par la Chambre des notaires du Québec et par le Barreau du Québec, pour démontrer que la personne décédée n'avait pas de testament;
 - une désignation d'une liquidatrice ou d'un liquidateur de succession par les héritières et les héritiers;
 - une déclaration notariée qui atteste le statut de la liquidatrice ou du liquidateur de la succession.
 - La ou le bénéficiaire d'une assurance vie ou d'une indemnité de décès doit fournir :
 - un certificat de décès;
 - un document qui atteste qu'elle ou qu'il est bénéficiaire de l'assurance vie ou de l'indemnité de décès.
 - L'héritière ou l'héritier ou encore la personne successible ayant un testament doit produire :
 - un certificat de décès;
 - un testament;
 - deux certificats de recherche testamentaire, délivrés par la Chambre des notaires du Québec et par le Barreau du Québec, pour confirmer qu'il s'agit du dernier testament.
 - L'héritière ou l'héritier ou la personne successible sans testament doit remettre :
 - un certificat de décès;
 - deux certificats de recherche testamentaire, délivrés par la Chambre des notaires du Québec et par le Barreau du Québec, qui prouvent que la personne décédée n'avait pas de testament.
- Précisions illustrant la nécessité d'obtenir les renseignements ou les documents en faisant valoir les intérêts ou les droits de la personne requérante.

8.4. Traitement des plaintes

Toute personne visée par un renseignement personnel recueilli, utilisé, communiqué ou conservé par l'Université peut déposer une plainte à la personne responsable PRP en cas de manquement aux obligations prévues à la présente Directive. La plainte doit être formulée par écrit et indiquer la nature des faits reprochés, le nom de la ou des personnes en cause, la date à laquelle l'incident s'est produit, ainsi que ses attentes quant à l'issue de la plainte. La plainte doit être adressée à la personne responsable de la protection des renseignements personnels par courriel à l'adresse suivante : rprp@USherbrooke.ca.

La personne responsable PRP accuse réception de la plainte et traite celle-ci dans un délai raisonnable. Lorsque la plainte est recevable, elle fait enquête sur les faits allégués par tout moyen approprié. Elle communique avec diligence une réponse écrite à la personne à l'origine de la plainte.

9. RESPONSABILITÉ

La Directive est sous la responsabilité de la secrétaire générale ou du secrétaire général.

10. ENTRÉE EN VIGUEUR

La Directive entre en vigueur le jour de son adoption par le comité de direction de l'Université.

ANNEXE

(VOIR ANNEXE À LA PAGE SUIVANTE)



OUTIL DE RÉFLEXION : CONCEPTION D'UN SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES

article 63.5 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels) – entrée en vigueur le 22 septembre 2023

Cet outil ne se substitue pas à l'évaluation des facteurs relatifs à la vie privée et ne tient pas compte des obligations administratives.



1. Mise en place d'un système d'information ou d'une prestation électronique de services

- Détermination de l'activité à concevoir ;
- Description des objectifs, des finalités, du cadre juridique, de la valeur ajoutée, etc. ;
- Recommandation en matière de protection des renseignements personnels :
 - Description des rôles et des responsabilités des personnes participantes au projet ;
 - Désignation d'une personne chargée du suivi et de la mise en œuvre de ces mesures ;
 - Planification d'activités de formation ou de sensibilisation ;
- Détermination des risques envisagés, à priori, et des mesures de mitigation.



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

Le comité peut suggérer, à toute étape du projet, la mise en place de mesures complémentaires de protection des renseignements personnels dans le projet y incluant les contrats, les ententes, etc.

- Consultation, dès le début du projet, afin de présenter celui-ci en portant une attention particulière aux éléments mentionnés précédemment ;
- Consultation, lors d'enjeux en matière de protection des renseignements personnels et d'accès, qui nécessite une expertise ;
- Consultation ponctuelle quant aux répercussions considérables de l'évolution du projet sur l'évaluation des facteurs relatifs à la vie privée.



3. Conception du projet

Les différents éléments à considérer pour protéger les renseignements personnels.

3.1 Nécessité de la collecte

- Quel programme ou attribution est applicable à la collecte ?
 - Est-ce que le projet offre à la personne concernée un produit ou un service technologique ayant des paramètres de confidentialité (article 63.7)?
- Devez-vous collecter des renseignements personnels ?
 - Est-ce que ces renseignements concernent une personne mineure (articles 53.1 et 64.1)?
- Avez-vous vérifié la possibilité :
 - de recourir à des renseignements personnels déjà collectés, si la Loi le permet, lors d'une utilisation à une autre fin avec ou sans le consentement (article 65.1)?
 - de faire une collecte en collaboration avec un autre organisme public (article 64)?
 - de collecter des renseignements moins précis, comme une tranche d'âge ?
- Quel est le support utilisé ?
- Est-ce que la collecte sera faite par un tiers (article 67.2)?
 - Est-ce que ce tiers est à l'extérieur du Québec (article 70.1)?

3.2 Limitation de l'utilisation

- L'utilisation et les finalités sont-elles conformes à celles qui avaient été prévues lors de la collecte (article 65.1)?
- Est-ce que les renseignements personnels utilisés sont de qualité ?
- Avez-vous recensé d'autres types d'utilisation (article 65.1)?
 - Est-ce qu'un consentement est requis (articles 53.1 et 64.1)?
 - Est-ce que la dépersonnalisation des renseignements est requise ou possible ?
 - Est-ce qu'une décision fondée exclusivement sur un traitement automatisé est mise en place (article 65.2)?
 - Est-ce qu'un recours à une technologie pour l'identification, la localisation ou le profilage est nécessaire (article 67.1)?
- Est-ce que l'utilisation sera faite par un tiers (article 67.2)?
 - Est-ce que ce tiers est à l'extérieur du Québec (article 70.1)?

3.3 Communication

- Est-ce qu'une communication de renseignements personnels est nécessaire :
 - avec le consentement (articles 53, 53.1 et 64.1)?
 - sans le consentement (article 59)?
- Est-ce que l'exercice d'un mandat ou l'exécution d'un contrat est requis (article 67.2)?
- Est-ce que la communication est faite à l'extérieur du Québec (article 70.1)?
- Quels sont les renseignements personnels nécessaires à la communication ?
- Quel est le support utilisé ?

3.4 Délai de conservation

- Est-ce que les renseignements personnels seront conservés pour servir aux fins pour lesquelles ils sont recueillis ou utilisés (article 72)?
 - Quelles sont les mesures pour conserver des renseignements personnels à jour, exacts et complets ?
 - Quel est le délai de conservation à respecter ?

3.5 Moyen de destruction

- Est-ce que les renseignements personnels doivent être détruits (article 73)?
 - Est-ce que les renseignements personnels peuvent être anonymisés pour une utilisation à des fins d'intérêt public ?
 - Quels sont les renseignements personnels à anonymiser ?
- Est-ce que les renseignements personnels seront détruits conformément au délai prévu dans le calendrier de conservation ?

3.6 Sécurité et gouvernance

N'oubliez pas de :

- mettre en place les mesures de sécurité raisonnables propres à assurer la protection des renseignements, de la conception à la production et lors de modifications (article 63.1), incluant les profils d'accès, la journalisation, les alertes d'incident de confidentialité, etc. ;
- prévoir l'exercice du droit d'accès de la personne concernée et du droit à la portabilité ;
- planifier des activités de formation pour que les membres du personnel visé puissent exercer leurs fonctions en toute confidentialité ;
- mettre à jour de façon continue l'évaluation des facteurs relatifs à la vie privée ;
- planifier les encadrements administratifs et les règles qui encadrent la gouvernance (article 63.3);
- prévoir des audits et des tests d'intrusion, notamment afin de prévenir les incidents de confidentialité et de rehausser la protection et la sécurité en fonction des avancées technologiques.