



Protection des renseignements personnels, les règles à respecter à l'Université

Résumé de l'autoformation

La protection des renseignements personnels à l'Université

L'Université Laval est responsable d'assurer la protection des renseignements personnels qu'elle détient, incluant ceux dont elle confie la garde à un tiers, comme un prestataire de service. La [Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#) oblige l'Université et les membres de son personnel à prendre certaines mesures lorsqu'ils **recueillent, utilisent, communiquent, conservent et détruisent** ce type de renseignement.



Le [Bureau de la protection des renseignements personnels](#) soutient l'ensemble des unités administratives et veille au respect de leurs responsabilités en matière de protection des renseignements personnels. Il fait également la promotion du développement d'une culture de protection de la vie privée au sein de la communauté universitaire.

Il y a des **personnes répondantes** dans tous les secteurs de l'Université afin d'encourager la mise en place de bonnes pratiques qui respectent les règles de protection des renseignements personnels. Elles sont là pour répondre à vos questions, [consultez-les au besoin](#).



Règles de gouvernance

L'Université a adopté des règles de gouvernance à l'égard des renseignements personnels. Plusieurs documents officiels encadrent les rôles et les responsabilités des membres du personnel lorsqu'ils ont accès à ces renseignements :

- [Politique sur la protection des renseignements personnels](#)
- [Règles de protection des renseignements personnels](#)
- [Directive sur la gestion des incidents de confidentialité](#)



Afin de préserver la confiance du public envers l'Université, nous devons être capables de démontrer notre conformité à nos obligations. **C'est votre responsabilité d'en prendre connaissance !**

Qu'est-ce qu'un renseignement personnel ?

Un renseignement personnel c'est quelque chose de précieux qu'il faut protéger et utiliser avec beaucoup de précautions ! Il affecte la vie privée puisqu'il permet d'identifier, directement ou indirectement, une personne physique et il est confidentiel.



Voici ce qui le caractérise :

- Il fait connaître quelque chose de quelqu'un ;
- Il concerne une personne physique ;
- Il est susceptible de distinguer cette personne par rapport à une autre ou de reconnaître sa nature

L'Université recueille et détient des renseignements concernant des personnes étudiantes ainsi que des personnes qui utilisent les services que nous offrons à la communauté. Ces renseignements sont généralement tous considérés comme des renseignements personnels. Il en va de même pour les renseignements sur les membres du personnel qui servent à des fins de gestion des ressources humaines.

Tous les renseignements personnels sont confidentiels sauf si une loi prévoit qu'ils ont un *caractère public*, comme c'est le cas pour les *renseignements professionnels* sur nos employés ou ceux de nos partenaires. Cela inclut le nom, le titre de la fonction, le courriel, adresse, ainsi que le numéro de téléphone.

Certains renseignements personnels sont sensibles si en raison de leur nature, ou en raison du contexte de leur utilisation ou de leur communication, ils suscitent un haut degré d'attente raisonnable à la vie privée. Il faut considérer la source du renseignement, son degré d'intimité et les répercussions potentielles pour les personnes liées à sa divulgation.

En voici des exemples :

- Les renseignements financiers
- Les renseignements sur la santé
- Les résultats académiques
- Les renseignements pouvant mener à de la discrimination

Assurez-vous de mettre en place des mesures de protection supplémentaires lorsque vous manipulez des renseignements personnels sensibles.

Cycle de vie des renseignements personnels

L'Université **collecte, utilise, communique, conserve** et **détruit** des renseignements personnels dans le cadre de ses fonctions au quotidien. On appelle ceci le *cycle de vie* des renseignements personnels.

Collecte

- **Minimisez la collecte** de renseignements à ceux qui sont strictement nécessaires pour réaliser les activités de l'Université.
- Particulièrement en présence de renseignements sensibles, vous devez démontrer que tous les renseignements recueillis répondent à un besoin important, réel et légitime.
- Assurez-vous d'**informer adéquatement les personnes** de ce que nous ferons de leurs renseignements et à qui nous les communiquerons à ces fins, le cas échéant.

Utilisation

- **Limitez l'utilisation** des renseignements personnels aux raisons pour lesquelles ils ont été obtenus au départ.
- Il est parfois possible d'utiliser des renseignements à d'autres fins, avec ou sans le consentement des personnes. **Assurez-vous d'être autorisé par le Bureau de la protection des renseignements personnels avant de procéder.**
- En tant que membre du personnel, vous devez uniquement accéder à des renseignements que lorsque cela est nécessaire à votre travail, sans plus.
- Il est interdit d'accéder à des renseignements personnels à des fins personnelles ou de les partager à des personnes qui ne sont pas autorisées à y accéder.

Communication

- L'Université doit restreindre la **communication** ou la **divulcation** de renseignements personnels, c'est-à-dire la transmission ou le partage de renseignements à des tiers ou d'autres personnes externes à l'Université.
- Il est interdit de communiquer des renseignements sans le consentement des personnes, à moins que la loi l'autorise autrement.

En cas de doute, vaut mieux demander à votre gestionnaire. Vaut mieux prévenir que guérir !

Conservation et destruction

- L'Université doit conserver les renseignements personnels pour une durée limitée, établie en fonction de la raison pour laquelle elle les a recueillis au départ et en conformité avec les règles prévues au [calendrier de conservation de l'Université](#).
- Les renseignements doivent être détruits lorsque cette durée établie est écoulée.

- Attention, certains renseignements personnels doivent être versés aux archives pour une conservation permanente. **Avant de détruire des renseignements personnels, assurez-vous d'être autorisés par votre gestionnaire.**

Pour plus d'information sur l'application du calendrier de conservation, veuillez communiquer à l'adresse supportgid@sq.ulaval.ca.

Mesures de sécurité

Tout au long du cycle de vie, vous devez utiliser des **moyens sécuritaires** lorsque vous transigez avec des renseignements personnels.

Vous avez un rôle à jouer pour réduire les risques tels que la perte des données, leur accès, la destruction, l'utilisation, la modification ou la divulgation non autorisée.

Pour plus d'information, communiquer avec le [Centre de services en TI](#) qui dessert votre unité.

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

Tout incident, réel ou présumé, menant :

- À l'accès non autorisé d'un renseignement personnel ;
- À l'utilisation non autorisée d'un renseignement personnel ;
- À la communication non autorisée d'un renseignement personnel ;
- À la perte d'un renseignement personnel ou ;
- Toute autre atteinte à la protection d'un tel renseignement.



Il peut s'agir d'un acte accidentel, d'une erreur ou d'un acte malveillant.

Voici des exemples concrets d'incidents :

- La consultation d'un dossier académique d'une personne étudiante par un membre du personnel à des fins personnelles ou par curiosité ;
- La perte d'une clé USB qui contient des documents sur des employés ;
- Le partage de documents confidentiels dans un espace commun accessible à d'autres employés qui ne sont pas autorisés à en prendre connaissance ;
- La diffusion de renseignements personnels sur un site Web ;
- La communication non autorisée de renseignements personnels à un tiers externe.

Signaler un incident de confidentialité



L'Université a une obligation d'agir rapidement pour diminuer les risques qu'un préjudice soit causé par un incident.

Lorsque vous détectez un incident de confidentialité, il faut le signaler, dans un **délai de 24 heures**, au Bureau de la protection des renseignements personnels en remplissant le [formulaire de signalement](#).

En agissant rapidement, ceci permet de limiter les conséquences négatives pour les personnes concernées. Il faut limiter l'étendue de l'incident, lorsque nous avons la capacité ou l'autorité de le faire.

Le Bureau de la protection des renseignements personnels déterminera de valider l'incident et d'informer les personnes concernées, le cas échéant. Le BPRP travaille ensuite avec l'unité pour identifier des mesures correctives afin de prévenir de nouveaux incidents.

Tous les incidents doivent être signalés, sans faute !

Référez-vous à la [Directive sur la gestion des incidents de confidentialité](#).

Dernière révision : 28 novembre 2024