Directive sur la gestion des incidents de confidentialité

Approbation :	Comité exécutif (Résolution CE-2023-67)
Entrée en vigueur :	14 mars 2023
Responsable :	Bureau du secrétaire général
Cadre juridique :	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1) Règlement sur les incidents de confidentialité

UNIVERSITÉ LAVAL

TABLE DES MATIÈRES

Préambule

Dans le cadre de ses activités en tant qu'établissement d'enseignement supérieur et de recherche, l'Université Laval (l'Université) recueille et utilise des renseignements personnels.

L'Université est un organisme public assujetti à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la Loi sur l'accès). Elle est responsable d'assurer la protection des renseignements personnels qu'elle détient et de démontrer sa conformité aux obligations légales qui lui incombent.

Conformément à l'article 63.8 de la Loi sur l'accès, lorsque l'Université a des motifs de croire qu'un incident de confidentialité impliquant des renseignements personnels qu'elle détient s'est produit, elle 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.

Si un incident présente un risque qu'un préjudice sérieux soit causé, elle doit, avec diligence, aviser la Commission d'accès à l'information ainsi que les personnes concernées.

L'Université est également tenue de consigner dans un registre tous les incidents de confidentialité dont elle a connaissance.

I. Objectifs

1. La présente directive encadre la gestion des incidents de confidentialité qui sont portés à la connaissance de l'Université ou du Bureau de la protection des renseignements personnels (le BPRP) par tout membre de l'Université. Elle décrit les étapes à suivre lorsqu'une personne détecte un incident de confidentialité.

II. Champs d'application

2. Cette directive s'applique à tout incident de confidentialité impliquant des renseignements personnels détenus par l'Université, réel ou présumé, détecté par un membre de l'Université.

3. Elle s'applique notamment aux incidents de confidentialité impliquant des renseignements personnels recueillis par un membre de l'Université et qui lui sert à des fins de recherche scientifique.

4. Elle s'applique également aux incidents de confidentialité impliquant des renseignements personnels confiés par l'Université dans le cadre de l'exécution d'un mandat ou d'un contrat de service.

III. Définitions

Dans la présente directive, les expressions et les mots suivants signifient :

Gestionnaire

Une administratrice ou un administrateur, une directrice ou un directeur ainsi que tout personnel cadre dont l'unité administrative dont elle ou il est responsable est la détentrice d'un renseignement personnel.

Incident de confidentialité

Tout incident, réel ou présumé, menant :

a) à l'accès non autorisé d'un renseignement personnel;

b) à l'utilisation non autorisée d'un renseignement personnel;

c) à la communication non autorisée d'un renseignement personnel;

d) à la perte d'un renseignement personnel ou;

e) toute autre atteinte à la protection d'un tel renseignement.

Les exemples suivants sont notamment considérés des incidents de confidentialité :

- La consultation de renseignements concernant des personnes étudiantes ou employées à des fins personnelles;
- La collecte de renseignements personnels qui ne sont pas nécessaires à l'exercice des fonctions du personnel de l'Université, au moment de la collecte;
- La transmission d'un courriel contenant des renseignements personnels à un mauvais destinataire;
- Le vol ou la perte d'un ordinateur portable qui contient des renseignements personnels;
- La communication de renseignements personnels à tout organisme public ou privé sans autorisation;
- La perte d'une clé USB qui contient des renseignements personnels;
- La divulgation, volontaire ou non, de renseignements personnels à des collègues qui ne sont pas autorisés à les consulter;
- Le piratage du serveur d'un prestataire de service qui héberge des renseignements personnels dont l'Université a la garde.

D'autres situations que celles énumérées ci-dessus peuvent également constituer des incidents de confidentialité.

Incident majeur

Tout incident de confidentialité qui, lors de son évaluation préliminaire, laisse croire qu'il est susceptible de causer un préjudice sérieux aux personnes concernées par les renseignements personnels, notamment en raison de la sensibilité des renseignements, des conséquences appréhendées de leur utilisation et de la probabilité qu'ils soient utilisés à des fins préjudiciables.

Toute perte ou tout vol de document ou de support technologique contenant des renseignements personnels est présumé un incident majeur.

Membre

Membre de l'Université au sens des Statuts de l'Université Laval, en l'occurrence les personnes étudiantes, le personnel enseignant, les administratrices et les administrateurs ainsi que le personnel administratif.

Personne répondante

Personne désignée afin de veiller à la conformité des règles et des obligations en matière de protection des renseignements personnels au sein d'un vice-rectorat, d'une faculté, d'une direction ou d'un service de l'Université.

Renseignement personnel

Tout renseignement détenu par l'Université qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Tiers

Toute personne physique ou morale, qui, sans être membre de l'Université, recueille, utilise, conserve, communique ou détruit des renseignements personnels au nom de l'Université ou qui assure autrement la gestion des renseignements personnels détenus par l'Université.

IV. Protocole de gestion des incidents de confidentialité

A. Limiter et signaler l'incident

5. Tout membre qui détecte un incident de confidentialité ou qui en est informé doit prendre les actions raisonnables pour limiter son étendue et arrêter la pratique non autorisée, dans la mesure où cette personne a la capacité et l'autorité de le faire.

6. Cette personne doit signaler l'incident au BPRP, dans un délai maximal de 24 heures.

7. Tout tiers, tel un prestataire de service ou un mandataire, qui détient des renseignements personnels pour l'Université doit signaler tout incident de confidentialité au BPRP, dans un délai maximal de 24 heures.

8. Tout incident de confidentialité doit être signalé au BPRP, et ce, même si les circonstances laissent croire qu'il ne s'agit pas d'un incident réel ou qu'il ne causera aucun préjudice aux personnes concernées.

9. Après l'examen du signalement initial, le BPRP confirme s'il s'agit d'un réel incident de confidentialité selon la présente directive et entreprend les étapes subséquentes, le cas échéant.

10. Le BPRP, en collaboration avec l'officière ou l'officier de la sécurité de l'information, fournit aux unités administratives concernées les directives nécessaires afin de limiter l'atteinte et d'arrêter la pratique non autorisée.

11. Le BPRP détermine à quel moment cette étape est terminée et quand les renseignements personnels ne sont plus à risque d'être recueillis, utilisés, communiqués, conservés ou détruits d'une manière non autorisée, ou encore quand aucune autre action raisonnable ne peut être entreprise pour limiter l'incident (en cas de vol ou de perte de renseignements, par exemple).

Incident majeur

12. Lorsque le BPRP est d'avis qu'il pourrait s'agir d'un incident majeur, il forme une équipe d'intervention composée de l'officière ou officier de la sécurité de l'information, de représentants du Bureau du secrétaire général, de la Direction des communications ainsi que de toute unité administrative dont les ressources sont jugées utiles en fonction de la nature et de la portée de l'incident de confidentialité. Le BPRP en informe le rectorat.

13. Lorsqu'il s'agit d'un incident majeur, l'équipe d'intervention coordonne les actions visant à limiter l'incident.

B. Évaluer les risques et les impacts

14. Le BPRP doit, en collaboration avec les unités administratives concernées, prendre les mesures nécessaires afin de déterminer les causes et les circonstances de l'événement et d'évaluer si l'incident présente un risque de préjudice sérieux pour les personnes concernées.

    Cette étape vise notamment à évaluer les facteurs suivants :

    a) la nature et la sensibilité des renseignements personnels;

    b) la cause et l'étendue de cet incident;

    c) les conséquences appréhendées de l'utilisation des renseignements;

    d) les préjudices potentiels pour les personnes concernées;

    e) les probabilités que les renseignements soient utilisés à des fins préjudiciables.

Incident majeur

15. Lorsqu'il s'agit d'un incident majeur, l'équipe d'intervention doit prendre les mesures nécessaires afin de déterminer les causes et les circonstances de l'événement et d'évaluer les risques et les impacts pour les personnes concernées au plus tard 24 heures après le signalement.

C. Informer les personnes et les autres entités concernées

Personnes concernées

16. Lorsqu'il a été déterminé qu'un incident présente un risque sérieux de préjudice, le BPRP doit aviser les personnes concernées directement et, de préférence, par écrit. Cette communication doit comprendre :

    a) 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;

    b) une brève description des circonstances de l'incident;

    c) la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

    d) une brève description des mesures que l'Université a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

    e) les mesures que l'Université suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé afin d'atténuer un tel préjudice;

    f) les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

17. L'avis à la personne concernée peut être donné au moyen d'un avis public dans l'une ou l'autre circonstance suivante :

    a) lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée;

    b) lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour l'Université;

    c) lorsque l'Université n'a pas les coordonnées de la personne concernée.

18. Malgré ce qui précède, l'Université n'a pas à aviser la personne concernée si cela est 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.

19. Dans les cas où un incident ne présente pas un risque sérieux de préjudice pour les personnes concernées, le BPRP peut en informer les personnes, si des circonstances particulières le justifient.

20. Lorsqu'un incident est susceptible d'affecter la réputation de l'Université, notamment en raison de sa cause ou du nombre de personnes concernées, le BPRP en informe le rectorat et la Direction des communications avant d'aviser les personnes concernées.

Commission d'accès à l'information

21. Lorsqu'il a été déterminé qu'un incident présente un risque sérieux de préjudice, le BPRP doit également aviser la Commission d'accès à l'information.

    L'avis doit contenir l'information prescrite par le formulaire de déclaration de la Commission.

Autres notifications

22. Lorsque le BPRP constate des manquements d'un membre du personnel aux règles et aux obligations relatives à la protection des renseignements personnels, il les rapporte à la ou au gestionnaire responsable du membre du personnel concerné.

23. Si les résultats de l'évaluation laissent croire qu'une infraction criminelle pourrait avoir été commise, le BPRP en informe le Bureau du secrétaire général et le Service de sécurité et de prévention, qui communiquera avec le corps de police approprié.

24. Si l'incident de confidentialité est lié à des renseignements personnels obtenus auprès d'un organisme public ou d'une autre personne avec laquelle l'Université est liée par une entente, le BPRP en informe l'organisme concerné.

D. Prévenir les incidents ultérieurs

25. Lorsque les étapes précédentes sont réalisées, le BPRP doit effectuer un bilan de l'incident et déterminer les mesures à adopter afin de prévenir les incidents ultérieurs.

    Il produit un rapport incluant les éléments suivants, sauf lorsque les circonstances ne le justifient pas :

    a) une liste des actions prises pour limiter l'incident;

    b) une évaluation des causes et des circonstances de l'incident;

    c) une description des renseignements personnels en jeu;

    d) une analyse des risques et des impacts pour les personnes concernées;

    e) un examen des mesures de sécurité en vigueur au moment de l'incident;

    f) une description des mesures correctives prises à la suite de l'incident;

    g) une évaluation des actions prises pour gérer l'incident;

    h) des recommandations visant à réduire les risques et à éviter que d'autres incidents similaires surviennent, le cas échéant.

26. Le BPRP transmet une copie du rapport aux unités administratives qui ont joué un rôle dans l'incident ou qui sont visées par des recommandations.

27. Le BPRP tient un registre des incidents de confidentialité.

Incident majeur

28. Lorsque l'analyse des risques et des impacts de l'incident démontre qu'il pourrait causer un préjudice sérieux aux personnes concernées, le BPRP doit effectuer une reddition de compte de l'intervention au plus tard 30 jours après le signalement initial et la transmettre au comité exécutif.

V. Rôles et responsabilités

A. Membres

a) Effectuer les actions nécessaires pour limiter l'étendue de l'incident de confidentialité, dans la mesure où ils ont la capacité et l'autorité de le faire.

b) Signaler au BPRP tout incident de confidentialité qu'ils détectent ou qui est porté à leur connaissance;

B. Bureau de la protection des renseignements personnels

a) Déterminer si un incident constitue un réel incident de confidentialité en vertu de la présente directive;

b) Déterminer s'il s'agit d'un incident majeur, définir la composition de l'équipe d'intervention et informer le rectorat, le cas échéant;

c) Fournir les directives nécessaires pour limiter l'incident de confidentialité et pour arrêter la pratique non autorisée;

d) Déterminer à quel moment l'incident de confidentialité est circonscrit et quand aucune autre action raisonnable ne peut être entreprise;

e) Examiner les causes et les circonstances de l'incident;

f) Évaluer les risques et les impacts de l'incident pour les personnes concernées;

g) Aviser les personnes concernées et la Commission d'accès à l'information de toute atteinte qui pourrait causer un préjudice sérieux aux personnes concernées;

h) Signaler les incidents au Bureau du secrétaire général et au Service de sécurité et de prévention lorsque les circonstances laissent croire qu'il pourrait y avoir eu une infraction au Code criminel ou à toute autre loi;

i) Produire un rapport d'incident, sauf lorsque les circonstances ne le justifient pas;

j) Rapporter à la ou au gestionnaire concerné les manquements d'un membre du personnel aux règles et aux obligations relatives à la protection des renseignements personnels;

k) Informer le comité exécutif de tout incident lorsque l'analyse des risques et des impacts de l'incident démontre qu'il pourrait causer un préjudice sérieux aux personnes concernées par les renseignements personnels;

l) S'assurer que les membres de l'Université sont en mesure de reconnaître et de signaler les incidents de confidentialité.

C. Officière ou officier de la sécurité de l'information

a) Fournir les directives nécessaires pour limiter l'incident de confidentialité et pour arrêter la pratique non autorisée;

b) Collaborer à l'examen des causes et des circonstances de l'incident et participer à l'équipe d'intervention, le cas échéant.

D. Bureau du secrétaire général et Service de sécurité et de prévention

a) Signaler les incidents au corps de police approprié, lorsque requis.

E. Personnes répondantes

a) Fournir l'aide et l'assistance requises lorsque l'incident de confidentialité est lié à des renseignements personnels détenus par une unité administrative dont elles sont responsables.

F. Gestionnaires

a) Collaborer avec la personne répondante, le BPRP et avec l'équipe d'intervention, le cas échéant, afin de fournir l'aide et l'assistance requises lorsque l'incident de confidentialité est lié à des renseignements personnels détenus par l'unité administrative dont ils sont responsables;

b) S'assurer de la mise en œuvre de toute recommandation du BPRP visant à réduire les risques et à éviter que d'autres incidents similaires surviennent, le cas échéant.

VI. Révision

29. La présente directive est sous la responsabilité du Bureau du secrétaire général. Elle est révisée au besoin, mais au minimum tous les trois ans à compter de sa date d'adoption.

VII. Entrée en vigueur

30. La présente directive entre en vigueur lors de son adoption par le Comité exécutif.