GESTION COURANTE Numéro : 40.39 Page 1 de 7

DIRECTIVE SUR L'ANONYMISATION DES RENSEIGNEMENTS PERSONNELS

Adoption
Date : 2025-10-21
Délibération : Secrétariat général

Modifications
Date :
Délibération :
Article(s) :

TABLE DES MATIÈRES

GESTION COURANTE Numéro : 40.39

DIRECTIVE SUR L'ANONYMISATION DES RENSEIGNEMENTS PERSONNELS

Adoption
Date : 2025-10-21
Délibération : Secrétariat général

Modifications
Date :
Délibération :
Article(s) :

1. PRÉAMBULE

Dans le cadre de leurs fonctions et de leurs activités à l'Université, les membres de la communauté universitaire ainsi que des Tiers sont amenés à traiter des Renseignements personnels détenus par l'Université ou pour son compte, conformément à la *Politique de protection des renseignements personnels de l'Université* et à la *Directive sur la conformité des traitements de renseignements personnels*.

2. OBJET

La présente directive établit les règles relatives à l'Anonymisation des Renseignements personnels détenus par l'Université ou pour son compte. Elle définit également les rôles et responsabilités des parties prenantes.

3. CADRE NORMATIF

La présente directive s'inscrit dans un contexte régi notamment par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « **Loi sur l'accès** ») et la *Loi sur les renseignements de santé et de services sociaux* et leurs règlements, la *Politique de protection des renseignements personnels* de l'Université et par les règles des organismes subventionnaires en recherche.

4. DÉFINITIONS

« Anonymisation » : opération irréversible par laquelle les Renseignements personnels concernant une personne physique sont modifiés de façon à ce qu'ils ne permettent plus d'identifier directement ou indirectement cette personne. Un renseignement Anonymisé cesse d'être qualifié de Renseignement personnel et n'est plus soumis aux règles applicables en cette matière.

« Cycle de vie » : désigne l'ensemble des étapes visant le Traitement d'un Renseignement personnel, soit la collecte, l'utilisation, la communication, la conservation et la destruction de celui-ci.

« Dépersonnalisation » : opération par laquelle les Renseignements personnels permettant l'identification directe d'une personne physique, notamment les Renseignements identificatoires, sont retirés. Ces informations peuvent être remplacées par un code permettant la réidentification de la personne dans le futur. Un renseignement Dépersonnalisé continue d'être un Renseignement personnel, car l'identification indirecte de la personne concernée est toujours possible en combinant ses Renseignements identificatoires.

« Personne participant à l'Anonymisation » : désigne toute personne qui participe de manière opérationnelle aux étapes d'Anonymisation des Renseignements personnels.

« Personne compétente en matière d'Anonymisation » : désigne une personne ayant une compétence raisonnable dans la mise en œuvre de processus d'Anonymisation des Renseignements personnels, dans la protection des Renseignements personnels et la sécurité des données. Ce rôle est défini dans la Loi sur l'accès et ses règlements.

« Personne répondante en matière de PRP » : désigne la personne responsable de veiller au respect des exigences de protection des Renseignements personnels que l'unité collecte, utilise, communique, conserve ou détruit.

« Personne responsable du Traitement » : désigne la personne qui détermine les finalités et les moyens de réaliser un Traitement.

« Renseignement identificatoire » : désigne un Renseignement personnel incluant notamment mais non limitativement le nom, l'adresse du domicile, le numéro d'assurance sociale, le numéro d'assurance maladie ou le code postal d'une personne physique.

« Renseignement personnel » : toute information qui concerne une personne physique et qui peut permettre de l'identifier directement, c'est-à-dire par le recours à cette seule information ; ou indirectement, c'est-à-dire par recoupement avec d'autres informations.

« Renseignement personnel à caractère public » : un Renseignement personnel revêt un caractère public, et donc non confidentiel, lorsque la Loi sur l'accès ou l'un de ses règlements l'indique expressément.

« Risque » : tout événement (action, situation, circonstance) ou toute absence d'événement inhérent à une activité et susceptible d'avoir une incidence sur la réalisation de la mission et des objectifs de l'Université. Cette incidence peut avoir un effet négatif (menaces) ou positif (opportunités) sur tout actif de l'Université. Le niveau de risque est évalué en mesurant la probabilité que le risque se concrétise et l'effet qu'il pourrait avoir sur l'Université.

« Risque inhérent » : désigne le niveau de Risque existant avant la mise en place de tout contrôle ou mesure de mitigation.

« Risque résiduel » : désigne le niveau de Risque qui subsiste malgré la mise en œuvre des contrôles et des mesures d'atténuation du Risque inhérent.

« Tiers » : désigne toute personne ou entité externe à la communauté universitaire, ou toute entité juridique distincte de l'Université.

« Traitement » : activité ou ensemble d'activités organisationnelles portant sur des Renseignements personnels ayant une finalité déterminée, quel que soit le procédé utilisé. Le Traitement peut couvrir une ou plusieurs phases du Cycle de vie telles que la collecte, l'utilisation, la communication, la conservation, l'Anonymisation ou la destruction.

« Université » : l'Université de Montréal, excluant ses écoles affiliées.

5. CHAMP D'APPLICATION

La présente directive s'applique aux Personnes responsables du Traitement et à toute personne habilitée à participer au Traitement de Renseignements personnels, aux Personnes répondantes en matière de PRP des unités, aux Personnes participant à l'Anonymisation, aux Personnes compétentes en matière d'Anonymisation et, enfin, aux Tiers traitant des Renseignements personnels pour le compte de l'Université.

La présente directive ne s'applique pas aux renseignements qui ne sont pas soumis aux règles de protection des Renseignements personnels, c'est-à-dire les Renseignements personnels à caractère public.

6. RÔLES ET RESPONSABILITÉS

6.1 Personne participant à l'Anonymisation

La Personne participant à l'Anonymisation doit contacter la Personne compétente en matière d'Anonymisation afin de permettre à celle-ci d'en encadrer le déroulement.

La Personne participant à l'Anonymisation s'assure de suivre les règles relatives à l'Anonymisation et à la Dépersonnalisation des Renseignements personnels définies à l'article 7, excluant les articles 7.2.4 et 7.2.5, réalisées uniquement par la Personne compétente en matière d'Anonymisation.

6.2 Personne compétente en matière d'Anonymisation

Les techniques d'Anonymisation de Renseignements personnels doivent être réalisées sous la supervision d'une personne possédant des compétences en la matière.

La Personne compétente en matière d'Anonymisation est responsable de la supervision de l'Anonymisation des Renseignements personnels, ainsi que de la bonne application des méthodes définies dans la présente directive.

6.3 Direction des Technologies de l'Information

La Direction des Technologies de l'Information consigne les informations suivantes dans un registre :

a) Une description des Renseignements personnels qui ont été Anonymisés (incluant un lien vers le jeu de données ou les instructions sur comment y accéder) ;

b) Les fins pour lesquelles seront utilisés ces renseignements Anonymisés ;

c) Les techniques d'Anonymisation utilisées et les mesures de protection et de sécurité choisies ;

d) La date à laquelle l'analyse des Risques de réidentification a été effectuée et, le cas échéant, la date à laquelle la mise à jour de l'analyse a été réalisée.

6.4 Personne responsable du Traitement et Personne répondante en matière de PRP

Conformément à la *Directive sur la conformité des traitements de renseignements personnels*, il relève de la responsabilité de la Personne responsable du Traitement et de la Personne répondante en matière de PRP de s'assurer de la conformité du Traitement, en l'occurrence l'élimination, et notamment de veiller au respect des exigences de protection des Renseignements personnels.

7. RÈGLES RELATIVES À L'ANONYMISATION ET À LA DÉPERSONNALISATION DES RENSEIGNEMENTS PERSONNELS

7.1 Finalités de traitement des Renseignements personnels Anonymisés ou Dépersonnalisés

Les finalités de Traitement des Renseignements personnels Anonymisés doivent être identifiées au préalable et évaluées conformément aux exigences règlementaires. Elles doivent être d'intérêt public. Advenant que ces fins initialement déterminées venaient à changer, l'Université devra s'assurer que les nouvelles finalités soient conformes à la loi.

Les Renseignements personnels Dépersonnalisés peuvent être utilisés à des fins d'étude, de recherche ou de production de statistiques, sans le consentement des personnes concernées, dans les limites permises par la loi. Des mesures raisonnables doivent être prises pour que les informations qui relient les renseignements Dépersonnalisés à une personne précise, comme des Renseignements identificatoires, soient conservés séparément et ne soient pas accessibles au personnel qui les utilise qu'à des fins d'étude, de recherche ou de production de statistiques.

7.2 Étapes de l'Anonymisation des Renseignements personnels

7.2.1 Retrait des Renseignements identificatoires

Afin de préparer le jeu de données à Anonymiser, il convient d'en retirer tous les Renseignements identificatoires. À ce stade, il s'agit de renseignements Dépersonnalisés.

7.2.2 Analyse préliminaire des Risques de réidentification

Lorsque les Renseignements identificatoires ont été retirés des données, une analyse préliminaire des Risques de réidentification doit être effectuée. Cette analyse doit notamment être fondée sur :

a) Le critère d'individualisation : soit l'impossibilité d'isoler ou de distinguer une personne dans un ensemble de données ;

b) Le critère de corrélation : soit l'impossibilité de relier entre eux des ensembles de données qui concernent une même personne ;

c) Le critère d'inférence : soit l'impossibilité de déduire des Renseignements personnels à partir d'autres renseignements disponibles ;

d) Les Risques que d'autres renseignements raisonnablement disponibles, notamment dans l'espace public, permettent d'identifier directement ou indirectement une personne lorsqu'ils sont combinés avec les données Dépersonnalisées.

7.2.3 Sélection des techniques d'Anonymisation et de sécurité appropriées

Les techniques d'Anonymisation doivent être déterminées en fonction des Risques de réidentification identifiés lors de l'analyse préliminaire et conformément aux meilleures pratiques généralement reconnues. Le choix de la solution optimale doit être évalué au cas par cas et nécessite souvent une combinaison de techniques différentes, telles que la randomisation, la généralisation, la suppression, etc.

Des mesures de protection et de sécurité raisonnables doivent être prises pour diminuer les Risques de réidentification. Il pourrait s'agir, mais sans s'y limiter, de séparation des données, de contrôle des accès, de l'enregistrement de toute action liée aux données pour réduire la possibilité de les combiner avec d'autres sources de données, etc.

7.2.4 Analyse approfondie des Risques de réidentification après Anonymisation

Une fois les techniques d'Anonymisation effectuées, une analyse approfondie des Risques de réidentification doit être réalisée, dont les résultats doivent démontrer qu'il est en tout temps raisonnable de prévoir que les renseignements Anonymisés ne permettent plus, de façon irréversible, d'identifier une personne, directement ou indirectement.

Le Risque résiduel n'a pas à être nul, mais il doit être très faible lorsque l'on prend en compte les éléments suivants :

a) Les circonstances liées à l'Anonymisation des Renseignements personnels, notamment les fins pour lesquelles seront utilisés les renseignements Anonymisés ;

b) La nature des renseignements ;

c) Les critères d'individualisation, corrélation et inférence ;

d) Les Risques que d'autres renseignements raisonnablement disponibles, notamment dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne ;

e) Les moyens nécessaires pour réidentifier les personnes, en considérant les efforts, les ressources et le savoir-faire requis pour mettre en œuvre ces moyens.

7.2.5 Mise à jour périodique des Risques de réidentification

Les Risques de réidentification doivent être régulièrement réévalués afin de s'assurer que les renseignements Anonymisés le demeurent au fil du temps. La fréquence de mise à jour des Risques de réidentification doit être déterminée en fonction des Risques résiduels initialement identifiés.

8. ENTRÉE EN VIGUEUR

La présente directive et toute modification à celle-ci entre en vigueur lors de son adoption par le secrétaire général.