L'OBSERVATOIRE
de l'Abitibi-Témiscamingue

POLITIQUE SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Table des matières

PRÉAMBULE

Le droit au respect de la vie privée et le droit à l'information sont garantis au Québec. En septembre 2021, le gouvernement a adopté la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (aussi appelée « Loi 25 »). Cette loi vient notamment confirmer l'obligation des organisations à but non lucratif au Québec, dont fait partie l'Observatoire de l'Abitibi-Témiscamingue (OAT), de se conformer aux nouvelles dispositions encadrant les droits des personnes en regard des renseignements personnels les concernant. La Loi prévoit de nombreux changements quant à la protection des Renseignements personnels, notamment dans la *Loi sur la protection des renseignements personnels dans le secteur privé*.

L'OAT est responsable de la protection des renseignements personnels qu'il détient, et ce, que leur conservation soit assurée par l'OAT ou un tiers. La présente politique constitue le socle de l'OAT pour assurer le respect de ses obligations en matière de droit à la vie privée.

Comme une partie des activités de l'OAT est intégrée à celles de l'Université du Québec en Abitibi-Témiscamingue (UQAT), la présente politique s'appuie notamment sur la *Politique sur la sécurité de l'information* de l'UQAT. Aussi, le personnel de l'OAT étant constitué d'employés et d'employées de l'UQAT, la gestion de leurs renseignements personnels est assurée par la *Politique sur l'accès aux documents et sur la protection des renseignements personnels* de l'UQAT. La présente politique veille ainsi à répondre aux spécificités de l'OAT tout en assurant une cohérence avec les pratiques de l'UQAT.

La présente politique a été élaborée en réponse à la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25).

ARTICLE 1 – DÉFINITIONS

Collecte : La Collecte est l'opération par laquelle les Renseignements personnels sont recueillis (p. ex. : formulaires, sondages, outils analytiques Web), créés (p. ex. : matricules des membres du personnel) ou inférés à partir de données déjà accessibles aux membres du personnel de l'OAT.

Commission : Désigne la Commission d'accès à l'information.

Communication : Réfère à toute opération qui consiste à transmettre, transférer ou mettre à la disposition d'une personne morale ou physique externe à l'OAT, des Renseignements personnels détenus par l'OAT sans égard aux moyens de communication utilisés.

Conseil d'administration : Désigne le Conseil d'administration de l'OAT.

Consentement : Autorisation accordée par la Personne concernée quant à toute Collecte, tout traitement, toute Utilisation et toute Communication de ses Renseignements personnels. Pour être considéré comme valide, le Consentement doit respecter les critères présentés à l'article 6.2 de la présente politique.

Évaluation des facteurs relatifs à la vie privée (EFVP) : Démarche préventive visant à mieux protéger les Renseignements personnels et à respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs de risque qui peuvent entraîner des conséquences sur le respect de la vie privée et à y apporter les correctifs requis, au besoin.

Incident de confidentialité : Désigne toute consultation, Utilisation ou Communication non autorisée par la loi d'un Renseignement personnel sous la responsabilité de l'OAT, ou toute perte ou toute autre forme d'atteinte à sa protection.

OAT : Désigne l'Observatoire de l'Abitibi-Témiscamingue.

Personne concernée : Personne physique concernée par un ou plusieurs Renseignements personnels.

Registre des Incidents de confidentialité : Registre visant à inventorier tous les cas d'Incidents de confidentialité relativement à un Renseignement personnel.

Renseignement personnel : Désigne tout renseignement qui concerne directement une personne dans son individualité et permettant de l'identifier, soit par ce seul renseignement, soit indirectement par une combinaison avec d'autres Renseignements personnels.

Ces renseignements sont confidentiels et comprennent, sans s'y limiter : le nom et le prénom, l'âge, la date de naissance, les coordonnées (adresse, numéro de téléphone, adresse de courriel), les renseignements financiers, les caractéristiques morphologiques, etc. Lorsque ces renseignements sont pris de façon isolée, ils ne sont plus considérés comme des Renseignements personnels puisqu'ils ne permettent pas d'identifier avec assurance la Personne concernée.

Sauf indication contraire, un renseignement professionnel, soit un renseignement qui concerne une personne dans l'exercice de ses fonctions, n'est pas un Renseignement personnel.

Responsable de la protection des Renseignements personnels (Responsable PRP) : Personne désignée par la plus haute autorité de l'OAT, soit le Conseil d'administration, qui est responsable de superviser l'application de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

UQAT : Désigne l'Université du Québec en Abitibi-Témiscamingue.

Utilisation : Désigne les opérations se rapportant aux Renseignements personnels effectuées à l'interne par les membres du personnel de l'OAT. Il peut s'agir notamment de leur organisation, structuration, adaptation, modification, extraction ou consultation.

ARTICLE 2 – OBJECTIFS

La présente politique vise les objectifs suivants :

a. informer des principes directeurs de l'OAT en matière de protection des Renseignements personnels;

b. informer des procédures mises en place par l'OAT à l'égard de la Collecte, de l'Utilisation, de la Conservation, de la Communication et de la destruction des Renseignements personnels ainsi que des droits des Personnes concernées;
c. clarifier l'application des principes de protection des Renseignements personnels en distinguant les responsabilités de l'OAT de celles relevant de l'UQAT.

ARTICLE 3 – CHAMP D'APPLICATION

La présente politique s'applique à tout Renseignement personnel détenu par l'OAT dans l'exercice de ses fonctions et activités, que sa conservation soit assurée par l'OAT ou un tiers. Les Renseignements personnels peuvent être collectés et/ou détenus et/ou utilisés par l'OAT ou par un tiers au bénéfice et au nom de l'OAT. La présente politique s'applique, quelle que soit la forme des documents : écrite, graphique, sonore, visuelle, informatisée ou autre.

La présente politique vise tout le personnel de l'OAT, incluant les personnes dont le lien d'emploi est terminé, ainsi que les membres des instances de l'organisme. Toute personne ou tout prestataire de services lié à l'OAT par un contrat de service ou d'approvisionnement y est également assujetti s'il a accès aux documents et aux Renseignements personnels détenus par l'OAT, ou s'il les conserve en son nom.

ARTICLE 4 – CADRE LÉGAL

La présente politique s'inscrit dans le respect des lois, politiques et règlements en vigueur, notamment :

- La *Loi sur la protection des renseignements personnels dans le secteur privé*, qui établit les règles relatives à l'accès à l'information et à la protection des Renseignements personnels au sein des organismes privés.
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25), qui renforce les obligations des organismes quant à la gestion et la protection des Renseignements personnels.
- La *Politique sur la sécurité de l'information* de l'UQAT.

ARTICLE 5 – RESPONSABILITÉS ET IMPUTABILITÉ

5.1 Conseil d'administration

Le Conseil d'administration a délégué la fonction de Responsable de la protection des Renseignements personnels (« Responsable PRP ») à la personne occupant le poste de direction à l'OAT.

5.2 Responsable de la protection des Renseignements personnels

La ou le Responsable PRP doit :

- S'assurer de la protection et de la gestion des Renseignements personnels détenus par l'OAT;
- Répondre aux demandes d'information ou aux plaintes relatives à la gestion des Renseignements personnels ou référer la demande à qui de droit à l'UQAT en ce qui concerne les Renseignements personnels qu'elle ou qu'il détient;

- Assurer la révision périodique des politiques et procédures relatives à la confidentialité;
- Assurer l'Évaluation des facteurs relatifs à la vie privée (EFVP);
- Participer à la révision du risque de préjudice lors d'un Incident de confidentialité;
- Tenir le Registre des communications;
- Aviser la Commission advenant un incident présentant un risque de préjudice sérieux.

5.3 Coordination

La ou le Responsable PRP est soutenu dans ses fonctions par la personne assurant la coordination de l'OAT. Selon les demandes de la ou du Responsable PRP, les fonctions de la coordination sont de :

- Soutenir la ou le Responsable PRP dans la mise en œuvre des pratiques et des mesures de protection et de sécurité des renseignements personnels détenus par l'OAT;
- Répondre aux demandes d'information, de communication et de rectification de renseignements personnels;
- Appliquer les décisions prises par la ou le Responsable PRP ainsi qu'en cas d'Incident de confidentialité;
- Transmettre les instructions de la ou du Responsable PRP à toute personne ou tout prestataire de services lié à l'OAT;
- Soutenir la ou le Responsable PRP dans la mise à jour des renseignements contenus au registre;
- Élaborer la *Politique de confidentialité* de l'OAT, selon les directives de la ou du Responsable PRP;
- Déposer la *Politique de confidentialité* sur le site Web de l'OAT.

5.4 Personnel de l'OAT

Tout le personnel de l'OAT a la responsabilité de collecter, d'utiliser et de communiquer des Renseignements personnels avec précaution et en conformité avec la présente politique. Il doit également :

- Participer aux activités de sensibilisation et de formation sur la protection des Renseignements personnels qui lui sont destinées, notamment les formations offertes par l'UQAT;
- Signaler à la ou au Responsable PRP tout Incident de confidentialité et toute situation qui présente des risques en matière de protection des Renseignements personnels ou de confidentialité des documents;
- Collaborer lors de la recherche de documents et d'information faisant l'objet d'une demande d'accès ou de rectification.

Au terme de son lien d'emploi, le personnel ne peut conserver et utiliser à d'autres fins aucun Renseignement personnel porté à sa connaissance dans le cadre de l'exercice de ses fonctions.

5.5 Personnes concernées par les Renseignements personnels

Toute personne qui souhaite retirer son Consentement ou demander la rectification de ses Renseignements personnels peut communiquer à l'adresse : observatoire@observat.qc.ca.

L'ensemble des membres du personnel ou de l'administration qui reçoivent une demande d'une telle nature doivent la soumettre à la ou au Responsable PRP.

5.6 Tiers ayant accès à des Renseignements personnels détenus par l'OAT

L'OAT peut, dans le cadre de ses activités, accorder un accès limité aux Renseignements personnels qu'il détient à des tiers (p. ex. : fournisseurs de services numériques). L'OAT s'assure que les tiers respectent des normes équivalentes aux siennes en matière de protection des Renseignements personnels.

ARTICLE 6 – ENCADREMENT DE LA GESTION DES RENSEIGNEMENTS PERSONNELS

6.1 Collecte

L'OAT recueille uniquement les Renseignements personnels qui sont nécessaires à la réalisation de ses activités. Avant d'effectuer la Collecte, l'OAT détermine que ces Renseignements personnels sont nécessaires et utilisés à des fins limitées. La Collecte de Renseignements personnels se fait auprès de la Personne concernée, qui consent, de façon libre et éclairée, à leur Utilisation.

La Collecte de Renseignements personnels peut être réalisée par le personnel de l'OAT par l'intermédiaire de moyens technologiques (p. ex. : Google Analytics, Mailchimp, Google Forms) ou par des tiers (p. ex. : sous-traitants).

Sans s'y limiter, la Collecte de Renseignements personnels peut se faire par l'inscription à l'Infolettre, l'utilisation du site Web (témoins [*cookies*]), l'inscription aux activités organisées par l'OAT, une demande d'information (téléphone ou formulaire en ligne), un sondage électronique ou une correspondance avec des membres du Conseil d'administration.

6.1.1 Règles liées à la Collecte

L'OAT doit prendre les mesures de sécurité nécessaires afin de maintenir la protection des Renseignements personnels qu'il collecte sur toute Personne concernée, notamment en s'assurant que :

1. seuls les Renseignements personnels nécessaires sont recueillis et exclusivement aux fins annoncées;
2. lors de la Collecte des Renseignements personnels, la Personne concernée détient toutes les informations nécessaires afin d'accorder son Consentement libre et éclairé. Il peut s'agir notamment :
    a. des fins auxquelles les renseignements sont recueillis;
    b. du caractère obligatoire ou facultatif de la demande;
    c. des droits d'accès ou de rectification prévus;
    d. de la possibilité que les Renseignements personnels recueillis soient conservés par des tiers, le cas échéant;
3. lorsqu'une technologie permettant d'identifier, de localiser ou de profiler la Personne concernée est utilisée pour la Collecte, l'OAT informe la Personne concernée de l'utilisation de cette technologie et des options disponibles pour activer ou désactiver ces fonctions;
4. lorsque nécessaire, l'OAT veille à ce que les tiers qui collectent des Renseignements personnels pour son compte (p. ex. : administration de sondages) adoptent des mesures de

sécurité adéquates et disposent de politiques claires garantissant qu'ils ne transmettront jamais les Renseignements personnels à qui que ce soit d'autre.

6.1.2 Règles liées à la Collecte lors de sondages

Avant de recueillir des Renseignements personnels dans le cadre d'un sondage, l'OAT doit procéder à une évaluation de la nécessité d'y recourir. Si le sondage est réalisé, l'OAT doit prendre les mesures suivantes pour :

- assurer la participation volontaire au sondage des participantes et participants;
- assurer la confidentialité des participantes et participants;
- assurer la confidentialité des participantes et participants lors de la diffusion des résultats du sondage.

Lorsque le cas s'applique, l'OAT doit par ailleurs s'assurer que les tiers réalisant un sondage pour son compte prennent des mesures de sécurité adéquates.

6.2 Consentement

Conformément à la *Loi sur la protection des renseignements personnels dans le secteur privé*, toute Collecte, toute Utilisation et toute Communication de Renseignements personnels requiert d'obtenir le Consentement de la Personne concernée.

L'OAT s'engage à obtenir le Consentement des Personnes concernées pour chaque fin visée dans un langage accessible et clair.

6.2.1 Mise à jour du Consentement

Pour cesser de recevoir des courriels de la part de l'OAT, une personne peut à tout moment cliquer sur le lien « vous désinscrire » au bas des infolettres ou écrire à observatoire@observat.qc.ca en indiquant « Désinscription infolettre » dans l'objet de son courriel.

6.3 Utilisation

L'OAT utilise les Renseignements personnels dans le cadre de ses activités uniquement aux fins pour lesquelles ils ont été recueillis, à moins d'obtenir le Consentement de la Personne concernée.

L'OAT peut utiliser les Renseignements personnels à des fins secondaires sans le Consentement de la Personne concernée dans les situations suivantes :

- lorsque l'Utilisation est à des fins compatibles avec celles pour lesquelles les Renseignements personnels ont été recueillis;
- lorsque l'Utilisation est nécessaire à l'application d'une loi au Québec;
- au moment où les Renseignements ont été dépersonnalisés à des fins de production de statistiques, afin de limiter les risques que quiconque puisse procéder à l'identification des Personnes concernées.

6.4 Communication

L'OAT reconnaît que les Renseignements personnels sont confidentiels et qu'ils ne peuvent être communiqués à un tiers, à moins d'obtenir le Consentement de la Personne concernée ou de bénéficier d'une exception prévue par les lois sur la protection des Renseignements personnels.

La Communication d'un Renseignement personnel sans le Consentement de la Personne concernée (Incident de confidentialité) doit être inscrite au Registre des communications.

6.5 Traitement des plaintes

Toute personne visée par un Renseignement personnel collecté, utilisé, communiqué ou conservé par l'OAT peut déposer une plainte à la ou au Responsable PRP en cas de manquement aux obligations prévues à la *Loi sur la protection des renseignements personnels dans le secteur privé* et à la présente politique. La plainte doit être formulée par écrit.

Toute demande ou plainte concernant les pratiques de protection des Renseignements personnels doit être transmise à la ou au Responsable PRP aux coordonnées inscrites sur le site Web de l'OAT.

6.6 Gestion des accès et protection des Renseignements personnels

L'UQAT gère les droits d'accès du personnel de l'OAT aux ressources informatiques et technologiques, de même qu'au bâtiment où se déroulent les activités quotidiennes de l'OAT. L'UQAT applique des mesures de sécurité physiques, techniques, technologiques et organisationnelles, incluant notamment :

- l'attribution d'un identifiant unique et de facteurs d'authentification;
- l'obligation d'utiliser un mot de passe robuste respectant des critères de complexité;
- le verrouillage automatique de session en cas d'inactivité sur le poste après un délai déterminé;
- l'utilisation d'un logiciel de détection et de prévention des logiciels malveillants régulièrement mis à jour;
- l'installation de plusieurs pares-feux aux endroits clés dans l'infrastructure réseau;
- la sécurisation des accès distants;
- le contrôle des accès physiques aux locaux de l'OAT, aménagés avec du mobilier sécuritaire pour conserver les Renseignements personnels.

Par la présente politique, l'OAT veille également à la sécurisation de son site Web par des mesures de sécurité raisonnables pour assurer la protection des informations et des Renseignements personnels. Ces mesures incluent, sans toutefois s'y limiter :

- la sécurisation des formulaires (p. ex. : avec CAPTCHA) et des adresses courriel (pour prévenir le moissonnage du Web [*web scraping*]);
- l'application d'une règle de mot de passe robuste et l'activation de l'authentification multifacteur pour tous les comptes administrateur du site Web;
- l'activation des fonctions de journalisation disponibles pour auditer les accès administrateur au site Web, au besoin;
- l'activation d'un bandeau indiquant la politique de collecte de témoins de navigation de l'OAT;

- l'activation d'un avis de Consentement à la Collecte de Renseignements personnels lorsqu'une personne remplit un formulaire de contact;
- l'activation des mises à jour automatiques pour les extensions.

6.7 Conservation et destruction

L'OAT s'assure que les Renseignements personnels qu'elle conserve sont à jour, exacts et complets. Lorsque les fins pour lesquelles un Renseignement personnel a été recueilli ou utilisé sont accomplies, l'OAT veille à la destruction sécuritaire ou à l'anonymisation du Renseignement personnel.

La destruction sécuritaire des Renseignements personnels se fait par le dépôt dans des boîtes de destruction sécurisées. Pour les documents numériques, incluant les courriels, la présente politique s'appuie sur le Service des technologies de l'information de l'UQAT, qui gère la sauvegarde et la suppression définitive des contenus supprimés par l'utilisatrice ou l'utilisateur sur la base des règles administratives fixées par l'établissement.

ARTICLE 7 – GESTION DES INCIDENTS DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS

L'OAT s'engage à gérer les Incidents de confidentialité impliquant des Renseignements personnels avec diligence et transparence, dans la mesure des dispositions prévues par la *Loi sur la protection des renseignements personnels dans le secteur privé*.

7.1 Obligation de déclaration de risques et d'incidents en matière de protection des Renseignements personnels

Toute personne ayant connaissance d'un risque pouvant affecter la protection des Renseignements personnels gérés par l'OAT doit le signaler immédiatement en communiquant aux adresses suivantes : observatoire@observat.qc.ca et securite-information@uqat.ca.

De même, toute personne ayant eu connaissance d'un Incident de confidentialité impliquant des Renseignements personnels doit communiquer immédiatement avec l'équipe du Service des technologies de l'information de l'UQAT en téléphonant au 819-762-0971 poste 2525.

7.2 Gestion des incidents et soutien aux personnes touchées

Les incidents en matière de protection des Renseignements personnels sont gérés conformément au *Plan de gestion des incidents de sécurité de l'information* produit et tenu à jour par le Service de sécurité de l'information de l'UQAT. Ceux-ci sont inscrits au Registre des Incidents de confidentialité de l'OAT que la ou le Responsable PRP tient à jour et soumet, sur demande, à la Commission.

En cas de déclaration d'un Incident de protection des Renseignements personnels présentant un risque qu'un préjudice sérieux soit causé, l'OAT s'engage à notifier sans délai :

- la Commission, par l'entremise de sa ou son Responsable PRP;
- toutes les personnes touchées par l'incident, dès que la notification à ces personnes ne risque pas d'entraver la conduite de l'enquête faite par une personne ou par une organisation qui, en vertu de la loi, est chargée de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois;
- tout tiers avec laquelle l'OAT est lié par une entente encadrant la protection de ces Renseignements personnels et/ou l'Utilisation de la plateforme technologique dans laquelle ces renseignements sont contenus.

Également, en cas de déclaration d'un incident, l'OAT peut aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les Renseignements personnels nécessaires à cette fin sans le Consentement de la Personne concernée. Dans ce dernier cas, la ou le Responsable PRP doit enregistrer la Communication.

7.3 Éléments à considérer lors d'une évaluation du risque d'un préjudice

Lorsque la ou le Responsable PRP évalue le risque qu'un préjudice soit causé à une personne dont un Renseignement personnel est concerné par un Incident de confidentialité, elle ou il doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son Utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

ARTICLE 8 – MÉCANISMES DE SUIVI ET SANCTIONS

Toute personne qui enfreint les dispositions de la présente politique ou les lois et la réglementation applicable en matière de protection des Renseignements personnels s'expose, en plus des pénalités prévues aux lois et règlements, à des mesures administratives ou disciplinaires en fonction de la gravité et des conséquences du geste. La direction générale de l'OAT est chargée de décider de l'opportunité d'appliquer la mesure appropriée, le cas échéant.

ARTICLE 9 – DISPOSITIONS FINALES

9.1 Entrée en vigueur

La présente politique entre en vigueur le jour de son adoption par le Conseil d'administration.

9.2 Révision et mise à jour

La révision et la mise à jour de la présente politique sont effectuées, au minimum, tous les cinq ans, ou dès l'entrée en vigueur de changements qui pourraient l'affecter.

La nouvelle version disponible est rendue accessible sur le site Web de l'OAT en indiquant la date de la dernière mise à jour.