



POLITIQUE OPÉRATIONNELLE OPE-19

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

TABLE DES MATIÈRES

1. ÉNONCÉ	1
2. OBJECTIF	1
3. CHAMP D'APPLICATION	1
4. RÉFÉRENCES	2
5. DÉFINITIONS.....	2
6. PRINCIPES GÉNÉRAUX	2
7. MISE EN APPLICATION DES PROCESSUS DE SÉCURITÉ ET DE CONFIDENTIALITÉ.....	3
8. RÔLES ET RESPONSABILITÉS	4
9. GESTION DES INCIDENTS	7
10. RESPONSABILITÉS	8

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

OPE-19

Page 1 de 8

1. ÉNONCÉ

1.1 Cette politique s'inscrit dans le cadre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « Loi »), qui impose aux organismes publics, dont la Société¹, plusieurs obligations visant à assurer la protection des renseignements personnels.

1.2 Cette politique remplace la politique « Gestion de l'information » en renforçant les mesures de gestion de l'information qui y étaient énoncées et appliquées par Loto-Québec.

2. OBJECTIF

La présente politique vise à :

2.1 Assurer une gestion sécuritaire de la gestion de l'information et notamment à protéger la vie privée des personnes à l'égard desquelles la Société détient des renseignements personnels.

2.2 Encadrer la mise en place des mesures qui s'imposent pour assurer le contrôle, l'intégrité, la sauvegarde et la confidentialité de son information.

2.3 Établir les rôles et responsabilités des membres du personnel de la Société tout au long du cycle de vie des renseignements personnels (collecte, utilisation, communication, conservation, destruction).

3. CHAMP D'APPLICATION

Cette politique s'applique à l'ensemble du personnel de la Société, ainsi qu'à tout fournisseur ou sous-traitant auquel la Société pourrait accorder un accès à des renseignements personnels qu'elle détient.

¹ Le terme Société désigne Loto-Québec et ses filiales.

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

OPE-19

Page 2 de 8

4. RÉFÉRENCES

- *Loi sur la Société des loteries du Québec* (RLRQ, c. S-13.1).
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ c.A-2.1).

5. DÉFINITIONS

5.1 COMITÉ AIPRP : Le comité sur l'accès à l'information et la protection des renseignements personnels formé des représentants des différents secteurs de la Société et qui assure un rôle de surveillance en matière d'accès à l'information et protection des renseignements personnels.

5.2 RENSEIGNEMENTS PERSONNELS : Renseignements qui concernent une personne physique et qui permettent, directement ou indirectement, de l'identifier. Les renseignements personnels incluent, entre autres, la date de naissance, l'adresse civique de sa résidence, le numéro de téléphone personnel, le numéro de permis de conduire ou d'assurance maladie, les caractéristiques physiques ou les activités d'une personne.

6. PRINCIPES GÉNÉRAUX

6.1 La Société reconnaît l'importance de l'information qu'elle détient et considère que les informations en sa possession ou sous son contrôle sont un actif critique au même titre que ses ressources matérielles, financières ou humaines.

6.2 La Société s'assure de mettre en place les mesures nécessaires afin que la collecte, l'utilisation, la communication, la conservation ou la destruction des renseignements personnels dans le cadre de ses activités, soit faite de manière responsable et sécuritaire. Elle n'utilise ces renseignements qu'avec le consentement des personnes visées et dans les cas permis par la Loi.

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

OPE-19

Page 3 de 8

6.3 Dans le cadre de la gestion des renseignements personnels qu'elle détient, la Société s'assure de faire preuve de transparence, en informant les personnes visées de la nature des renseignements collectés et de leur utilisation, dans le cadre de leur inscription ou adhésion à tout programme, service ou offre de produit et par le biais d'une politique de confidentialité, accessible au public. La Société s'engage également, en tout temps, à ne pas vendre à des tiers les renseignements personnels qu'elle détient et à en assurer la sécurité.

6.4 À cette fin, la Société s'assure de mettre en place des mesures visant la protection des renseignements personnels, incluant :

- la sensibilisation et la formation des employés;
- un processus de gestion des incidents et de traitements des plaintes;
- la mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels;
- la mise en place d'un encadrement adéquat des projets et initiatives d'affaires ou technologiques impliquant des renseignements personnels afin de réduire les risques pour la vie privée.

7. MISE EN APPLICATION DES PROCESSUS DE SÉCURITÉ ET DE CONFIDENTIALITÉ

7.1 La Société fournit à ses employés l'information nécessaire à la réalisation du mandat qui leur est confié et il leur est interdit d'utiliser ces informations pour des fins autres.

7.2 L'information confidentielle et l'information essentielle aux opérations de la Société doivent être identifiées et faire l'objet de mesures de protection adéquates, notamment en ce qui a trait à la gestion des renseignements personnels.

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

OPE-19

Page 4 de 8

- 7.3 Des niveaux de confidentialité internes doivent être déterminés afin de permettre la mise en place de mesures de protection appropriées, conformes aux besoins de la Société.
- 7.4 Des mesures physiques ou logiques de protection doivent être prises de façon à garantir la sauvegarde, la sécurité, l'intégrité et la confidentialité des informations détenues par la Société.
- 7.5 Dans le cadre de l'environnement informatique et micro-informatique, la sécurité de l'information est garantie par le maintien de mesures spécifiques, adaptées à ces environnements et chaque usager des systèmes informatiques doit avoir accès seulement aux ressources logiques informatiques nécessaires à l'accomplissement de son travail.
- 7.6 La Société exige de tout contractant, sous-traitant ou toute autre personne qui a accès à de l'information, la signature d'un engagement à respecter les directives, normes et procédures.

8. RÔLES ET RESPONSABILITÉS

8.1 SECRÉTARIAT GÉNÉRAL ET VICE-PRÉSIDENTE À LA DIRECTION JURIDIQUE

- 8.1.1 La secrétaire générale et vice-présidente à la direction juridique, à titre de responsable de la protection des renseignements personnels s'assure, en collaboration avec le vice-président et chef de la transformation numérique et des technologies, de déployer les ressources nécessaires pour voir au respect par la Société de ses obligations en matière de protection des renseignements personnels.

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

OPE-19

Page 5 de 8

8.1.2 Le Secrétariat général et Vice-présidence à la direction juridique assure un accompagnement aux unités d'affaires et corporatives relativement au respect des obligations de la Société et à la mise en place de bonnes pratiques en matière de protection des renseignements personnels.

8.1.3 Le Secrétariat général et Vice-présidence à la direction juridique s'assure de mettre en place un processus de traitement des plaintes relatives à la protection des renseignements personnels et d'informer le public des moyens par lesquels une plainte peut être déposée.

8.1.4 Il s'assure notamment, en collaboration avec la Vice-présidence corporative à la transformation numérique et aux technologies, que des capsules d'information et de sensibilisation en matière de sécurité et protection des renseignements personnels soient rendues disponibles périodiquement à l'ensemble du personnel de la Société.

8.2 VICE-PRÉSIDENTE CORPORATIVE À LA TRANSFORMATION NUMÉRIQUE ET AUX TECHNOLOGIES

8.2.1 La Vice-présidence corporative à la transformation numérique et aux technologies de l'information s'assure de voir à la mise en place et au contrôle des mesures permettant d'assurer le contrôle, l'intégrité, la sécurité, la sauvegarde et la confidentialité de l'information et des renseignements personnels, conformément à l'application de la présente politique.

8.2.2 Elle assure également de favoriser l'utilisation de moyens technologiques pour optimiser le traitement et la gestion de l'information et de mettre en place des mesures de protection physiques ou logiques appropriées, adaptées aux environnements dans lesquels l'information est sauvegardée ou utilisée, afin d'en assurer la sécurité.

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

OPE-19

Page 6 de 8

8.3 UNITÉS D'AFFAIRES ET CORPORATIVES

8.3.1 Chaque unité d'affaires et corporative est responsable d'assurer la gestion et la protection des renseignements personnels dans le respect des principes établis à la présente politique et selon les obligations prévues par la Loi.

8.3.2 Avant le début d'un projet ou initiative d'affaires ou de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de service, chaque unité doit s'assurer de prévoir un encadrement adéquat afin de minimiser les risques liés à toute utilisation de renseignements personnels qui pourrait être envisagée.

8.4 MEMBRES DU PERSONNEL

8.4.1 Chaque membre du personnel qui est impliqué dans la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels doit s'assurer d'en faire une gestion responsable et sécuritaire afin d'en assurer la protection dans le respect des obligations prévues par la Loi conformément aux instructions qu'il a reçues.

8.5 COMITÉ AIPRP

Le Comité AIPRP a pour rôle de soutenir la responsable de la protection des renseignements personnels dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la Loi. À cette fin, il s'assure, entre autres, de :

8.5.1 Approuver les règles de gouvernance à l'égard de la protection des renseignements personnels et la politique de confidentialité de la Société.

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LA GESTION DE L'INFORMATION

OPE-19

Page 7 de 8

8.5.2 Veiller à la réalisation des activités de sensibilisation et de formation des employés et gestionnaires de la Société relativement aux obligations et aux bonnes pratiques en matière d'accès à l'information et de protection des renseignements personnels.

8.5.3 Encadrer la réalisation des évaluations des facteurs relatifs à la vie privée qui doivent être faites par les unités d'affaires et corporatives, dans le cadre des projets visés par la Loi.

8.5.4 Recevoir un rapport des incidents inscrits au registre des incidents de confidentialité, le cas échéant.

9. GESTION DES INCIDENTS

9.1 Tout employé qui a connaissance d'actes ou de brèches concernant un usage non autorisé ou tout incident de sécurité doit les signaler rapidement à l'une des personnes suivantes :

- La secrétaire générale et vice-présidente à la direction juridique;
- Le vice-président corporatif et chef de la transformation numérique et des technologies.

9.2 Suite à la réception d'une telle information, les vérifications jugées nécessaires doivent être effectuées afin d'évaluer la gravité du risque.

9.3 Si l'analyse révèle qu'il y a un risque de préjudice sérieux, la Société doit aviser la Commission d'accès à l'information et les personnes concernées de l'incident.

9.4 Le non-respect de cet engagement, par l'utilisation, la modification, la destruction ou la divulgation non autorisée d'informations, peut entraîner des sanctions disciplinaires pouvant aller jusqu'au congédiement immédiat ou des poursuites judiciaires.

10. RESPONSABILITÉS

Les responsabilités pour la recommandation, l'approbation, l'application et la révision de la présente politique incombent aux instances et personnes suivantes :

10.1. RECOMMANDATION

Marie-Christine Tremblay
Secrétaire générale
et vice-présidente à la direction juridique

Denis Daly
Vice-président corporatif
et chef de la transformation numérique
et des technologies

10.2. APPROBATION

Le conseil d'administration.

10.3. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur dès son approbation par le conseil d'administration.

Date de dernière révision : 1^{er} septembre 2023

Date de dernière modification : 1^{er} septembre 2023