Politique générale sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels

1 Préambule

La présente politique est adoptée en application de l'article 12 de la Directive gouvernementale sur la sécurité de l'information.

Dans l'accomplissement de sa mission, l'Office de la protection du consommateur doit recueillir, détenir, utiliser, traiter, transmettre et archiver des renseignements (données, documents, etc.),

dont le volume s'accroît au fil des ans. L'information détenue par l'Office s'avère un actif précieux et indispensable dont la protection aura pour effet de renforcer la confiance des consommateurs, des commerçants et de ses partenaires. L'Office se doit donc de relever le défi majeur que constitue la gestion sécuritaire de l'ensemble de ses actifs informationnels et, à cette fin, de s'assurer du respect des lois, règlements et directives régissant l'utilisation de l'information auxquels il est assujetti, ainsi que de la conformité aux normes nationales et internationales en matière de sécurité de l'information.

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1, ci-après *Loi sur l'accès*) a comme objectif d'assurer la transparence de l'administration publique et la protection des renseignements personnels. Prenant appui sur des valeurs fondamentales de la société québécoise – démocratisation des rapports entre l'État et les citoyens et respect de la vie privée – la loi indique comment l'administration publique doit gérer l'information qu'elle détient. En matière d'accès à l'information et de protection des renseignements personnels, l'Office entend participer, pour ce qui est de sa mission, aux efforts de l'administration publique pour assurer une gestion de l'information conforme aux dispositions de la *Loi sur l'accès*. Par la présente politique, l'Office intègre les principes de la *Loi sur l'accès* dans les processus de gestion de l'information et confirme la responsabilité en matière d'accès à l'information et de protection des renseignements personnels des utilisatrices et utilisateurs, c'est-à-dire de tout le personnel, peu importe son statut, ou de toute personne physique ou morale qui, à titre de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels de l'Office ou y a accès, ainsi que de toute personne dûment autorisée par l'Office à y avoir accès.

2 Définitions, cadre légal et administratif

Les définitions ainsi que le cadre légal et administratif concernant cette politique peuvent être consultés dans le document *Lexique et cadre légal en matière de sécurité de l'information à l'Office de la protection du consommateur*.

3 Objectif de la politique

L'objectif de la présente politique est d'affirmer l'engagement de l'Office à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information qu'il détient, directement ou indirectement. Plus précisément, il s'agit d'assurer, tout au long du cycle de vie d'une information et quels que soient son support et sa localisation, les aspects suivants : sa disponibilité, son intégrité et sa confidentialité, l'irrévocabilité de tout acte accompli à l'égard de cette information, le contrôle de l'accès à celle-ci par une procédure d'authentification ainsi que la conformité de son traitement avec les lois et règlements applicables, de même qu'avec les orientations, les directives et les normes nationales et internationales.

Il s'agit également d'assurer la sécurité des ressources qui sous-tendent l'information durant son cycle de vie, notamment des supports, des systèmes informatiques, des infrastructures technologiques et des réseaux de télécommunication.

Cette politique énonce les principes et les obligations applicables à l'Office afin que l'accès aux documents et la protection des renseignements personnels soient assurés, en conformité avec les exigences de la *Loi sur l'accès*.

4 Champ d'application

La présente politique s'adresse à tous les utilisateurs, c'est-à-dire à tout le personnel de l'Office, peu importe son statut, ou à toute personne physique ou morale qui, à titre de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels de l'Office ou y a accès, ainsi qu'à toute personne dûment autorisée par l'Office à y avoir accès. L'information visée est celle que l'Office détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

Elle s'applique également à l'information appartenant à l'Office et que celui-ci exploite, ainsi qu'à celle lui appartenant et qu'un consultant, un partenaire, un fournisseur ou un tiers dûment autorisé exploite, et ce, tout au long du cycle de vie de cette information.

Finalement, cette politique couvre l'ensemble des activités relatives à l'information et, notamment, celles impliquant la collecte, la manipulation ou l'utilisation sous toutes ses formes de l'information de l'Office, que ces activités soient exercées dans ses bureaux, dans un autre lieu ou à distance.

5 Énoncés de principes généraux

5.1 Protection de l'information

- L'Office est responsable de l'information qu'il détient et il prend toutes les mesures nécessaires pour informer les utilisateurs des droits et des principes établis par la *Loi sur l'accès* pour la gestion des demandes d'accès à l'information et la protection des renseignements personnels.
- L'Office adhère au Cadre gouvernemental de gestion de la sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.
- L'Office reconnaît que les actifs informationnels qu'il détient sont essentiels à ses opérations courantes et, de ce fait, doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection dont les actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ces actifs informationnels sont exposés.
- L'Office est détenteur de l'information et il doit être en mesure de la localiser tout au long de son cycle de vie.

- La gestion de la sécurité des actifs informationnels s'appuie sur l'implication continue de tous les utilisateurs ainsi que sur une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

5.2 Accès à l'information et protection des renseignements personnels

L'Office est responsable de la protection des renseignements personnels qu'il détient, directement ou indirectement.

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée ou illicite. Sont notamment considérés confidentiels, au sens de la *Loi sur l'accès*, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences néfastes, entre autres, sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs secrets industriels, financiers, commerciaux, scientifiques, techniques ou syndicaux, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

Tout renseignement recueilli ou utilisé dans le cadre d'un sondage doit faire l'objet de mesures de protection, dont une évaluation de la nécessité de recourir au sondage et une évaluation de l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

Toute personne a droit d'accès aux documents détenus par l'Office, sous réserve des restrictions prévues dans la *Loi sur l'accès*. L'Office rend accessibles les documents qu'il détient. Il assure cette accessibilité en conformité avec les procédures prévues dans la *Loi sur l'accès* et sous réserve des restrictions qui y sont également prévues.

Toute plainte relative à la protection des renseignements personnels est traitée par le Bureau de la qualité des services de l'Office, conjointement avec le responsable de l'accès à l'information et de la protection des renseignements personnels.

5.3 Sensibilisation et formation

L'accès à l'information et la protection des renseignements personnels sont au cœur du respect de la *Loi sur l'accès* et font partie de la culture organisationnelle de l'Office. Par conséquent, l'Office s'engage, sur une base régulière, à sensibiliser et à former les utilisateurs sur les enjeux, les responsabilités et les obligations qui leur incombent en matière d'accès, de protection des renseignements personnels et de sécurité de l'information. Entre autres, les principales activités sont :

- une formation sur la protection des renseignements personnels et la sécurité de l'information offerte aux gestionnaires ainsi qu'aux autres membres du personnel qui doivent gérer des renseignements personnels ou de l'information sensible dans l'exercice de leurs fonctions;
- des activités de sensibilisation organisées régulièrement pour rappeler à tout le personnel l'importance des enjeux en matière d'accès à l'information, de protection des renseignements personnels et de sécurité de l'information;
- divers outils mis à la disposition du personnel pour soutenir la mise en œuvre de la présente politique.

5.4 Droit de regard

L'Office exerce un droit de regard sur l'usage, par les utilisateurs, de ses actifs informationnels, et ce, en conformité avec la législation et la réglementation existantes.

5.5 Continuité des services essentiels de l'Office

En cas d'événement ou d'incident pouvant entraîner une interruption de services ou leur dégradation, l'Office doit disposer d'un plan de continuité des services essentiels, consigné par écrit, éprouvé et tenu à jour, comportant les mesures nécessaires en vue d'assurer, dans un délai raisonnable, la disponibilité des actifs informationnels jugés essentiels à la poursuite de ses activités et la disponibilité des services qu'il rend à la population et aux entreprises.

6 Rôles et responsabilités

Les principaux rôles et les principales responsabilités touchant la sécurité des actifs informationnels à l'Office, de même que les structures internes de coordination et de concertation, sont précisés dans le Cadre de gestion de la sécurité de l'information, de l'accès à l'information et de la protection des renseignements personnels de l'Office.

7 Obligations des intervenants clés en matière de sécurité de l'information et de protection des renseignements personnels

La présente politique fixe les obligations en matière de sécurité de l'information et de protection des renseignements personnels attribuées, notamment, au président, au chef de la sécurité de l'information organisationnelle, au répondant en matière de sécurité de l'information, au responsable de l'accès à l'information et de la protection des renseignements personnels, aux détenteurs, aux gestionnaires d'entités administratives et aux utilisateurs.

Président

Il est le premier responsable de la sécurité de l'information, de l'accès à l'information et de la protection des renseignements personnels pour l'Office.

Chef délégué de la sécurité de l'information (CDSI)

Le chef délégué de la sécurité de l'information assume, sous le lien fonctionnel du chef gouvernemental de la sécurité de l'information et pour les organismes publics auxquels il se rattache, les responsabilités découlant de la *Loi sur l'accès* et de ses textes d'application.

Comité de concertation sur la conformité et les projets

Ce comité est créé afin de faciliter, entre autres, la réalisation et le suivi de l'accès à l'information, de la protection des renseignements personnels et de la sécurité de l'information. Il assume des responsabilités multiples et est le principal mécanisme de concertation et de coordination à l'Office. Ce comité est notamment composé des principaux intervenants en sécurité de l'information, du responsable de l'accès à l'information et de la protection des renseignements personnels et de toute autre personne pouvant apporter une contribution aux travaux du comité. Les divers rôles et responsabilités sont décrits dans le Cadre de gestion de la sécurité de l'information, de l'accès à l'information et de la protection des renseignements personnels.

Chef de la sécurité de l'information organisationnelle (CSIO)

Le chef de la sécurité de l'information organisationnelle (CSIO) assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de l'Office.

Répondant en matière de sécurité de l'information (RSI)

Le répondant en matière de sécurité de l'information apporte, sur le plan tactique, son soutien au CSIO, notamment en ce qui concerne la mise en œuvre des mesures de sécurité et la mise en place des processus officiels de sécurité de l'information.

Responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP)

Cette personne est déléguée par le président pour assurer la gestion des demandes d'accès à l'information et la mise en place des mesures assurant la protection des renseignements personnels et des priorités d'intervention en la matière.

Détenteur de l'information

Membre du personnel appartenant à la classe d'emploi de niveau cadre, désigné par l'Office, dont le rôle consiste, entre autres, à s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

Gestionnaires

Ils sont chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.

Utilisateurs

Ils doivent se conformer aux directives gouvernementales, à la présente politique et aux règles qui leur sont applicables.

Les rôles et les responsabilités attribués à d'autres intervenants ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information sont définis dans le

Cadre de gestion de la sécurité de l'information, de l'accès à l'information et de la protection des renseignements personnels, en complément à la présente politique.

8 Obligations des utilisateurs

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par l'Office. À cette fin, il doit :

- prendre connaissance de la présente politique ainsi que des politiques, cadres, directives et procédures en découlant et y adhérer;
- signer l'Engagement à l'égard des renseignements et des actifs informationnels détenus par l'Office de la protection du consommateur, qui engage l'utilisateur :
  - à consulter, utiliser et communiquer seulement les renseignements personnels ou confidentiels nécessaires à l'exercice de ses fonctions, en conformité avec les lois applicables;
  - à ne jamais consulter, ni utiliser, ni communiquer un renseignement personnel ou confidentiel dans un but personnel ou par curiosité;
  - à ne pas permettre que soit consulté, utilisé ou communiqué un renseignement personnel ou confidentiel autrement qu'aux fins nécessaires à l'exercice de ses fonctions, en conformité avec les lois applicables;
  - à assurer la protection des renseignements personnels recueillis et produits dans le cadre de ses fonctions, et ce, tout au long du cycle de vie de ces renseignements;
  - à conserver uniquement les renseignements personnels nécessaires à ses fonctions;
  - à se conformer aux règles de confidentialité lorsqu'il discute d'un dossier, que ce soit dans le cadre de ses fonctions ou non, en faisant preuve de retenue et de discrétion dans ses propos afin d'éviter que des personnes non concernées puissent entendre et connaître la teneur de la communication;
  - à prendre les mesures nécessaires afin d'assurer en tout temps une protection adéquate de ses mots de passe ainsi que des équipements et des renseignements mis à sa disposition;
  - à utiliser les actifs informationnels mis à sa disposition en se limitant aux fins pour lesquelles ils sont destinés, uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions et en respect des droits d'accès qui lui sont attribués;
  - à respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et à ne pas modifier ni désactiver leur configuration;
  - à respecter et à protéger de plein droit et en tout temps tous les droits de propriété intellectuelle détenus par l'Office ou des tiers et, en conséquence, à ne pas télécharger, ni reproduire ou transmettre à un tiers tout élément protégé par des droits de propriété intellectuelle, sauf si une autorisation explicite à cet effet a été donnée au préalable par le propriétaire de ces droits;

- à ne pas chercher à prendre connaissance d'une information dont la connaissance n'est pas requise aux fins de son travail ni à tenter d'obtenir un accès non autorisé à des actifs informationnels;
- à signaler immédiatement à son gestionnaire tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection ou compromettre la sécurité des actifs informationnels ainsi que la protection des renseignements personnels disponibles à l'Office;
- au moment de son départ de l'Office, à remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout équipement mis à sa disposition dans le cadre de l'exercice de ses fonctions;
- à respecter toute autre obligation applicable aux employés de l'Office.

9 Sanctions

Tout utilisateur contrevenant à la présente politique, au cadre de gestion ou aux directives, normes et procédures en découlant, s'expose, selon la gravité de son geste, à une mesure administrative ou disciplinaire, telle qu'une suspension de privilèges, une réprimande, une suspension ou un congédiement, et ce, conformément aux dispositions des conventions collectives, conditions de travail, contrats ou ententes en vigueur.

L'Office peut transmettre à toute autorité judiciaire concernée les renseignements colligés et qui lui portent à croire qu'une infraction à toute loi ou à tout règlement en vigueur a été commise.

10 Dispositions finales

La présente politique entre en vigueur à la date de son approbation par la présidente ou le président de l'Office. Elle demeure en vigueur tant et aussi longtemps qu'elle n'est pas abrogée, modifiée ou remplacée par une autre politique. Elle doit être révisée lors de tout changement pouvant l'affecter. Elle est complétée par le Cadre de gestion de la sécurité de l'information, de l'accès à l'information et de la protection des renseignements personnels, de même que par des directives, standards et procédures visant à préciser les obligations qui en découlent.

La présente politique remplace la précédente Politique générale sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels du 7 mai 2019.

La présente Politique générale sur la sécurité de l'information, l'accès à l'information et la protection des renseignements personnels est approuvée par :

M^me^ Marie-Claude Champoux, présidente

12 octobre 2023

Date