Société du Centre des congrès de Québec

GESTION DES RENSEIGNEMENTS PERSONNELS

(2022-12-13)

1 OBJET

La protection des renseignements personnels est une priorité. Cette politique constitue le fondement des règles de gouvernance qui s'appliquent à ces renseignements.

2 BUTS

- Respecter les obligations légales en matière de protection des renseignements personnels.
- Établir les principes directeurs qui guident les pratiques de la Société dans sa gestion des renseignements personnels.
- Préciser les rôles et les responsabilités des acteurs concernés.

3 CHAMP D'APPLICATION

Tout le personnel de la Société.

Cette politique s'applique à tous les renseignements personnels détenus par la Société, incluant ceux dont la conservation est assurée par un tiers, quel que soit le support sur lequel ils sont conservés, et ce, de leur collecte à leur destruction.

4 PRINCIPES GÉNÉRAUX

La Société est responsable des renseignements personnels qu'elle détient et respecte les principes reconnus en la matière et aussi les obligations qui découlent notamment des lois suivantes :

- Code civil du Québec (RLRQ, c. CCQ-1991)
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1)

- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2)
- Loi concernant le cadre juridique des technologies de l'information (RLRQ, c. C-1.1)
- Loi sur les archives (RLRQ, c. A-21.1)

5 DÉFINITION – RENSEIGNEMENT PERSONNEL

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

6 RÔLES ET RESPONSABILITÉS

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

Le président-directeur général a désigné la secrétaire générale à titre de responsable de l'accès à l'information et de la protection des renseignements personnels. À ce titre, ses rôles et responsabilités sont :

- Veiller à assurer le respect et la mise en œuvre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et du *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* et de toute autre obligations législatives, administratives et règlementaires.

- Assurer le traitement des demandes d'accès et des plaintes. Prêter assistance à la personne qui adresse une demande.

- Exercer un rôle-conseil auprès des unités administratives afin d'assurer la protection des renseignements personnels tout au long du cycle de vie de ceux-ci, soit de la collecte à la destruction.

- Coordonner les travaux du comité sur l'accès à l'information et la protection des renseignements personnels et présider les rencontres.

- Évaluer la légitimité et la nécessité de recueillir de nouveaux renseignements personnels.

- Veiller à la sensibilisation et à la formation du personnel sur les obligations et les pratiques en matière d'accès à l'information et de protection des renseignements personnels.

- Proposer les politiques et les directives en matière de protection des renseignements personnels.

- Coordonner la révision des fichiers de renseignements personnels.

- Au besoin, coordonner la rédaction des ententes de collecte de renseignements par un autre organisme.

- Effectuer les redditions de comptes requises en matière d'accès à l'information et de protection des renseignements personnels, notamment :

- Tenir des registres en ce qui concerne les incidents de confidentialité, les communications de renseignements personnels, les ententes de collecte de renseignements et de l'utilisation de renseignements à d'autres fins que celles prévues lors de la collecte.

- S'il y a lieu, transmettre les ententes de collecte ou de communication de renseignements personnels à la Commission d'accès à l'information.

- Agir à titre de représentant auprès des autres organismes publics et de la Commission d'accès à l'information pour toutes les questions relatives à l'accès aux documents et à la protection des renseignements personnels.

En matière d'évaluations de facteurs de la vie privée :

- Évaluer la nécessité de procéder à une évaluation des facteurs relatifs à la vie privée.

- Informer le comité sur l'accès à l'information et la protection des renseignements personnels de tout projet de système d'information ou de prestation électronique de service qui traite des renseignements personnels, notamment s'il implique un fournisseur ou un prestataire de services.

- Réaliser les évaluations de facteurs de la vie privée (EVFP), en collaboration avec les unités administratives concernées.

Comité sur l'accès à l'information et protection des renseignements personnels (CAIPRP)

Le comité est composé des personnes ci-dessous. Cependant, dans le cadre de ses travaux, le comité peut s'adjoindre toute autre personne dont l'expertise lui est nécessaire.

- Secrétaire générale (responsable de l'accès à l'information et de la protection des renseignements personnels)
- Directeur de l'administration
- Responsable des technologies de l'information

Le comité a pour mandat de soutenir le responsable de l'accès à l'information et de la protection des renseignements personnels dans l'exercice de ses fonctions et dans l'exécution de ses obligations en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* notamment :

- Proposer les politiques et procédures en matière d'accès à l'information et protection des renseignements personnels. Veiller au respect de ces politiques et procédures.

- S'assurer de la réalisation d'un programme de sensibilisation et de formation sur la protection des renseignements personnels.

- Promouvoir les orientations, les directives et les décisions formulées par la Commission d'accès à l'information.

- Déterminer les orientations de la Société en matière de protection des renseignements personnels.

- Exiger des mesures de protection des renseignements personnels particulières pour tout projet lié à l'acquisition, au développement ou à la refonte de systèmes d'information ou de prestation électronique de service qui entraîne la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels, notamment si ce projet implique un fournisseur ou prestataire de services.

- Formuler des avis sur les mesures particulières à respecter quant à l'utilisation d'une technologie de vidéosurveillance, de données biométriques ou quant aux sondages qui recueillent des renseignements personnels.

- S'il y a lieu, autoriser la collecte de renseignements pour un autre organisme.

- S'il y a lieu, autoriser la communication de renseignements personnels à l'extérieur du Québec.

- Évaluer annuellement le niveau de protection des renseignements personnels.

Comité de crise en ressources informationnelles

Un comité de crise en ressources informationnelles a également été formé. Celui-ci sera le centre de coordination de la réaction à un incident de confidentialité et il entrera en action seulement dans l'éventualité d'une gestion de reprise des systèmes à la suite d'un incident. Cette cellule d'intervention est formée des personnes suivantes :

- Responsable des technologies de l'information
- Responsable du réseau et de la sécurité de l'information
- Technicien en informatique
- Directeur de l'administration
- Secrétaire générale (responsable de l'accès à l'information et de la protection des renseignements personnels)

En cas de crise, ce comité peut s'adjoindre toute autre personne dont l'expertise lui est nécessaire.

Directeur des unités administratives

Les gestionnaires sont responsables de veiller à la protection des renseignements personnels détenus par leurs unités administratives. Ils doivent notamment :

- Veiller à ce que leur personnel utilise des moyens sécuritaires pour recueillir, utiliser, conserver, communiquer ou détruire des renseignements personnels et les sensibiliser à leurs responsabilités prévues dans la présente politique.

- Informer les ressources humaines de tout manquement d'un membre du personnel et appliquer les mesures appropriées.

- Informer et collaborer avec le responsable de l'accès à l'information et de la protection des renseignements personnels lorsqu'une évaluation des facteurs relatifs à la vie privée est requise, par exemple lors de toute utilisation d'une technologie de vidéosurveillance, de mesures biométriques ou lorsqu'il est nécessaire de recourir à un sondage. À cet égard :

    - Recenser les renseignements personnels que l'unité administrative souhaite recueillir et déterminer leurs fins lors de tout nouveau projet ou de toute nouvelle activité;

  - Solliciter l'avis du responsable de l'accès à l'information et de la protection des renseignements personnels sur la légitimité et la nécessité de recueillir de nouveaux renseignements personnels.

- Déclarer les fichiers de renseignements personnels dont ils sont responsables et collaborer à leur révision.

- Autoriser et réviser périodiquement les accès aux renseignements dont ils sont détenteurs et révoquer les accès qui ne sont plus nécessaires à l'exercice des fonctions des membres de leur personnel.

- Veiller à ce que les renseignements dont ils sont détenteurs soient utilisés uniquement pour les fins déterminées lors de leur collecte. S'il y a lieu, obtenir l'autorisation de la personne responsable de la protection des renseignements personnels avant d'utiliser des renseignements personnels pour une fin secondaire.

- Obtenir l'autorisation de la personne responsable de la protection des renseignements personnels avant de communiquer des renseignements personnels à une personne ou à un organisme.

- Informer le responsable de l'accès à l'information et de la protection des renseignements personnels de tout projet de communication de renseignements personnels à un fournisseur ou à un prestataire de services ainsi que de tout projet de collecte de renseignements par un tiers. Si le projet se concrétise :

  - Participer à la rédaction du contrat et remettre une copie dudit contrat.

  - Faire signer un engagement à la confidentialité à toute personne à l'emploi d'un fournisseur ou d'un prestataire de services et conserver les engagements de confidentialité.

  - À la fin du contrat, obtenir du fournisseur ou du prestataire de services une attestation de destruction des renseignements personnels.

- Pour les renseignements qu'ils détiennent, mettre en place les mesures nécessaires pour :

  - S'assurer d'une conservation sécuritaire.

  - S'assurer que les renseignements sont à jour, exacts et complets avant leur utilisation.

  - S'assurer du respect des règles de conservation et autoriser la destruction.

Membres du personnel

Les membres du personnel ont l'obligation de prendre les mesures nécessaires pour assurer la protection des renseignements personnels auxquels ils ont accès. Ils doivent notamment :

- Collecter uniquement les renseignements autorisés.

- Utiliser les renseignements personnels uniquement s'ils y sont autorisés et pour les fins prévues lors de leur collecte.

- S’assurer d’y être autorisé avant de communiquer des renseignements personnels.

- Utiliser des moyens sécuritaires pour recueillir, utiliser, conserver, communiquer ou détruire des renseignements personnels.

- Obtenir l’autorisation de leur gestionnaire avant de détruire des renseignements personnels.

- Informer leur gestionnaire de toute situation qui pourrait compromettre la protection des renseignements personnels détenus par la Société.

7 ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (EFVP)

L’évaluation des facteurs relatifs à la vie privée (EFVP) est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée. Elle consiste à considérer tous les facteurs qui auront un effet positif ou négatif pour le respect de la vie privée des personnes concernées, notamment :

- La conformité d’un projet à la législation en vigueur en matière de protection des renseignements personnels et au respect des principes qui l’appuient.
- L’identification des risques d’atteinte à la vie privée qu’un projet entraîne et l’évaluation de leurs impacts.
- La mise en place de stratégies pour éviter ces risques ou pour les réduire efficacement.

Conformément à la *Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels,* une EFVP doit être réalisée et celle-ci doit être soumise au comité sur l’accès à l’information et protection des renseignements personnels pour :

- Tout projet de système d’information ou de prestation électronique de services qui implique la collecte, l’utilisation, la communication, la conservation ou la destruction de renseignements personnels, notamment s’il implique un fournisseur ou un prestataire de services ;
- Tout projet qui implique l’utilisation d’une technologie de vidéosurveillance ou de mesures biométriques ;
- Toute collecte de renseignements pour un autre organisme ;
- Toute communication de renseignements à l’extérieur du Québec;
- Tout sondage qui recueille, utilise ou communique des renseignements personnels;
- Toute communication de renseignements à des fins d’étude, de recherche ou de production de statistiques ;
- Toute autre communication de renseignements à une personne ou à un organisme, lorsque cela est requis par la loi.

Ces EFVP doivent périodiquement être révisées, notamment lors de la signature d’un nouveau contrat avec un fournisseur ou un prestataire de services.