Protection des renseignements personnels

Les informations contenues dans cette procédure reflètent les modifications apportées à la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP) par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (communément appelée Loi 25) et en vigueur le 22 septembre 2023.

Cette procédure vise à s'assurer que les professionnels en assurance de dommages et en règlement de sinistres connaissent et respectent les principes énoncés notamment dans la *Loi sur la protection des renseignements personnels dans le secteur privé.*

En effet, la Loi s'applique aux entreprises et individus (dont les certifiés en assurance de dommages) qui recueillent, détiennent, utilisent ou communiquent des renseignements personnels sur autrui (art. 3.1 LPRPSP).

L'entreprise doit, notamment, mettre en place les mesures, politiques et procédures pour protéger ces renseignements et s'assurer que ses employés comprennent et respectent leurs obligations en matière de confidentialité, qui s'appliquent à chacune des étapes du « cycle de vie » d'un renseignement personnel : collecte, communication, utilisation, détention, conservation et destruction (art. 3.2 LPRPSP).

Quant à vous, agents, courtiers et experts en sinistre, pour assurer la protection des renseignements personnels de vos clients, il est important de développer et maintenir de bons réflexes en matière de protection des renseignements, notamment de respecter les obligations liées à la collecte et au partage des renseignements personnels.

LA COLLECTE ET LA COMMUNICATION DES RENSEIGNEMENTS PERSONNELS

Lors de la collecte de renseignements personnels, il faut informer la personne concernée (art. 8 LPRPSP) :

- des finalités de la collecte et des moyens par lesquels les renseignements sont recueillis;
- du nom des tiers ou catégories de tiers à qui il est nécessaire de communiquer les renseignements personnels pour atteindre les objectifs par la collecte;
- de ses droits d'accès et de rectification aux renseignements personnels;
- du droit de retirer son consentement à l'utilisation ou la communication des renseignements.

Pour offrir un produit ou un service en assurance de dommages, l'entreprise peut collecter et utiliser les renseignements personnels du client dont elle a besoin pour lui offrir les produits et services demandés. Cependant, il faut respecter les paramètres suivants :

- Il faut définir de façon précise les fins pour lesquelles les renseignements sont recueillis avant toute collecte et en informer le client. Par exemple, un agent recueille des renseignements personnels pour évaluer les besoins du client, déterminer s'il répond aux critères de souscription de l'assureur et préparer une soumission. Un expert en sinistre recueille des renseignements personnels afin d'enquêter et de traiter une réclamation.
- Seuls les renseignements **nécessaires** doivent être recueillis, c'est-à-dire ceux indispensables pour atteindre les objectifs de la collecte, par exemple la souscription d'une assurance ou le traitement d'une réclamation.
- Les renseignements personnels doivent être recueillis auprès de la personne concernée, sauf si elle a donné son autorisation pour les recueillir auprès d'un tiers (c'est-à-dire une autre personne ou une autre entreprise). Il faut également obtenir le consentement de la personne concernée avant de vérifier ses renseignements personnels auprès d'un tiers.
- Une attention particulière doit être portée aux **renseignements sensibles**, c'est-à-dire ceux qui « de par [leur] nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de [leur] utilisation (…) suscite[nt] un haut degré d'attente raisonnable en matière de vie privée ». En assurance de dommages, il s'agit, par exemple, des renseignements financiers ou médicaux.

LE CONSENTEMENT

Le consentement à la collecte, à la communication ou à l'utilisation de renseignements personnels doit être manifeste, libre et éclairé et donné à des fins spécifiques. De plus, il doit être demandé en termes simples et clairs. La personne concernée a le droit de demander assistance pour comprendre la portée du consentement qui lui est demandé.

Afin de respecter ces exigences, toute demande de consentement devrait préciser les trois éléments suivants :

1. L'**identité des personnes ou entreprises** auprès desquelles l'assuré autorise une collecte ou une communication de renseignements personnels, par exemple des assureurs susceptibles d'accepter le risque si vous êtes courtier, ou le Fichier central des sinistres automobiles du Groupement des assureurs automobiles dans le cadre d'une soumission;
2. La **nature des renseignements** échangés, par exemple, l'historique des réclamations d'assurance automobile de l'assuré;
3. L'**utilisation** qui sera faite des renseignements recueillis ou communiqués, comme fixer la prime d'assurance;

À noter : l'utilisation d'un formulaire de consentement écrit permet de répondre aux exigences de la loi et facilite votre travail.

Lorsque la demande de consentement est faite par écrit, elle doit être dans un document distinct des autres informations communiquées (art. 14 LPRPSP).

CONSENTEMENT EXPRÈS

Dans le cas d'un renseignement personnel sensible, le consentement doit être obtenu de manière expresse (explicite) :

- lorsqu'une entreprise souhaite l'utiliser à d'autres fins que celles pour lesquelles il a été recueilli (art. 12 de la LPRPSP);
- lorsque ce renseignement sera communiqué à un tiers (art. 13 al. 2 de la LPRPSP).

Par exemple, des renseignements personnels sensibles sont recueillis dans le contexte de l'obtention d'une soumission en assurance automobile. Si le cabinet souhaite utiliser ces renseignements pour offrir de l'assurance habitation, un consentement exprès devra être obtenu, de manière distincte.

UTILISATION DES RENSEIGNEMENTS PERSONNELS

Les renseignements personnels peuvent être utilisés seulement pour les fins pour lesquelles ils ont été obtenus (art. 12 LPRPSP). Par conséquent, un nouveau consentement doit être obtenu auprès de la personne concernée avant toute nouvelle utilisation ou toute nouvelle communication des renseignements recueillis, par exemple :

- lorsque vous offrez une assurance habitation à votre client que vous assurez déjà en automobile,
- si vous effectuez un transfert de clientèle vers un nouvel assureur et prévoyez continuez à procéder aux prélèvements bancaires.

L'entreprise doit également prendre des mesures pour restreindre la consultation des renseignements contenus dans les dossiers, qu'ils soient sur support papier ou support numérique. Ainsi, l'entreprise doit limiter l'accès des collaborateurs, employés et fournisseurs aux renseignements qui sont nécessaires à l'exercice de leurs tâches. Par exemple, un employé du service de comptabilité devrait avoir accès seulement aux renseignements nécessaires à la facturation et non à l'ensemble du dossier (art. 20.2 LPRPSP).

Il est d'ailleurs recommandé que les employés non certifiés ayant accès aux dossiers signent un **engagement de confidentialité**, étant entendu que les employés certifiés sont soumis aux codes de déontologie et doivent respecter la confidentialité des renseignements personnels.

DÉTENTION ET CONSERVATION DES RENSEIGNEMENTS PERSONNELS

Tous les moyens nécessaires, tant matériels qu'administratifs, doivent être pris pour assurer, en tout temps, la protection et la confidentialité des renseignements personnels détenus par l'entreprise. En tant que certifié, cette obligation demeure même si votre mandat est terminé et que la personne concernée n'est plus votre client.

En vertu de la Loi et de votre code de déontologie, vous devez assurer la protection des renseignements, peu importe le lieu où ils se trouvent ou leurs supports de conservation. À titre d'exemple :

- Évitez de laisser vos dossiers contenant des renseignements personnels à la vue du public, de vos collègues de bureau qui ne sont pas concernés par ces dossiers ou des résidents de votre domicile. Rangez-les dans des classeurs (ou des dossiers virtuels sécurisés).
- Utilisez des outils technologiques adéquats mis à votre disposition : mots de passe confidentiels, systèmes de cryptage de données, pare-feu, etc.
- Assurez-vous que votre poste de travail à domicile n'est pas situé dans une aire ouverte où vos conversations téléphoniques d'affaires confidentielles pourraient être entendues.

UN RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET UN REGISTRE DES INCIDENTS

Depuis le 22 septembre 2022, les entreprises doivent désigner un responsable de la protection des renseignements personnels au sein de celles-ci. Dans bien des cas, il s'agit d'un haut dirigeant (art. 3.1 LPRPSP). Cette personne veille à ce que l'entreprise traite les données personnelles qu'elle détient conformément aux lois. Elle doit, notamment, gérer les incidents de confidentialité.

Comme certifié, il est de votre responsabilité de savoir qui est la personne ou le service responsable de la protection des renseignements personnels au sein de votre entreprise. En cas d'incident de confidentialité, vous devez communiquer avec cette personne ou le service responsable pour :

- l'informer de tout incident de confidentialité pour lequel vous êtes impliqué;
- prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé aux personnes concernées et éviter que de nouveaux incidents de même nature se produisent.

Exemples d'incidents de confidentialité :

- envoi d'un courriel contenant des renseignements personnels à un mauvais destinataire;
- vol d'un ordinateur portable contenant des renseignements personnels de clients;
- piratage ou intrusion informatique menant à un vol ou une perte de données;
- extraction de données par une personne non autorisée.

DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Les entreprises doivent conserver leurs dossiers dans leur intégralité jusqu'à l'expiration du délai de cinq ans après la dernière transaction intervenue dans ceux-ci.

Ensuite, les dossiers conservés sur support papier ou support numérique doivent être détruits de façon sécuritaire pour en préserver la confidentialité.

Si vous confiez la destruction de vos dossiers à une entreprise spécialisée, assurez-vous que votre contrat contient un engagement de confidentialité et exigez que celui-ci soit signé par toute personne qui aura à manipuler vos documents.

MODALITÉS ET EXERCICE DU DROIT D'ACCÈS AUX RENSEIGNEMENTS PERSONNELS PAR LA PERSONNE CONCERNÉE

Sauf exception, toute personne a le droit d'avoir accès aux renseignements personnels la concernant et détenus par l'entreprise (art. 27 LPRPSP). Elle a également le droit de demander la rectification d'un renseignement personnel inexact, incomplet ou équivoque dont la collecte, la communication ou la conservation n'est pas autorisée par la Loi (art. 28 LPRPSP). Toute demande d'accès doit être écrite (art. 30 LPRPSP) et traitée dans les 30 jours de sa réception par la personne responsable des renseignements personnels (art. 32 LPRPSP).

Pour en savoir davantage sur le contenu d'un dossier-client, consultez la procédure *Tenue de dossiers-clients et notes aux dossiers.*

Voici une fiche contenant les extraits pertinents de la *Loi sur la protection des renseignements personnels dans le secteur privé*.