Aéro Auditeur
Consultant en aviation

Politique sur la protection des renseignements personnels

Description

Énoncé de la politique

Aéro Auditeur garantit la sécurité et la confidentialité des renseignements personnels selon les lois en vigueur.

Objectifs

Cette politique vise à assurer la collecte, l'utilisation, le stockage et la divulgation des renseignements personnels conformément aux lois applicables et aux meilleures pratiques.

Portée

Tous les employés, dirigeants, consultants, sous-traitants et fournisseurs sont concernés dans le cadre de leurs fonctions.

Définitions

- Renseignements personnels (RP) : Informations permettant d'identifier une personne physique, confidentielles et non communicables sans consentement.
- Responsable de la protection des RP : La personne ayant la plus haute autorité veille au respect des lois sur la protection des RP et peut déléguer cette fonction.
- Commission d'accès à l'information du Québec (CAI) : Organisme qui surveille l'application des lois sur l'accès aux documents et la protection des RP.
- Incident de confidentialité : Tout accès, utilisation ou communication non autorisés, perte ou atteinte aux RP (ex. : consultation non autorisée, cyberattaque).
- Consentement : Accord donné librement, clairement et en connaissance de cause, pour des fins précises et pour la durée nécessaire.

Rôles et responsabilités

Personne responsable des RP dans l'entreprise

Le titre et les coordonnées de la personne se trouvent sur le site Internet de l'entreprise. Au sein de l'entreprise, le responsable est Michel Payette, président.

La loi lui confie des rôles spécifiques. En cas d'incident de confidentialité impliquant un renseignement personnel, notamment, elle doit :

- Enregistrer les communications effectuées à toute personne ou tout organisme susceptible de diminuer le risque pour la personne concernée suivant l'incident;
- Prendre part à l'évaluation du préjudice causé par l'incident;

- Elle doit également réaliser une évaluation des facteurs relatifs à la vie privée (ÉFVP) lorsque la loi l'exige, par exemple avant de communiquer des RP à l'extérieur du Québec ou lors de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des RP. Guide d'accompagnement – ÉFVP

Toute personne impliquée dans un incident de confidentialité impliquant un RP :

La loi lui confie des rôles spécifiques. En cas d'incident de confidentialité impliquant un renseignement personnel, notamment, elle doit :

- Enregistrer les communications effectuées à toute personne ou tout organisme susceptible de diminuer le risque pour la personne concernée suivant l'incident;
- 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 ne se produisent;
- Aviser la Commission et la personne concernée si l'incident présente un risque de préjudice sérieux;
- Tenir un registre des incidents dont une copie devra être transmise à la Commission à sa demande.

Protection des renseignements personnels

L'entreprise qui recueille, utilise, communique à des tiers, conserve ou détruit des renseignements personnels a plusieurs obligations à respecter en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Cycle de vie d'un renseignement personnel

Collecte

La collecte constitue la première étape du cycle de vie des renseignements personnels. Elle comprend plusieurs modes, tels que le recueil (par exemple via formulaire d'abonnement, sondage ou outils analytiques Web), la création (comme un numéro de membre ou de permis de conduire) et l'inférence (profil de consommateur déduit à partir d'autres données). La simple visualisation d'un renseignement personnel, même sans conservation ultérieure, est considérée comme une collecte. Celle-ci peut être effectuée par l'entreprise ou par un tiers, tel qu'un mandataire ou un prestataire de services.

À cette phase, plusieurs obligations doivent être appliquées :

- Définir les objectifs de la collecte, lesquels doivent reposer sur un intérêt sérieux et légitime pour constituer un dossier.
- Limiter la collecte aux renseignements nécessaires aux fins fixées ; en cas de doute, considérer un renseignement comme non nécessaire.
- Utiliser uniquement des moyens légaux et légitimes pour recueillir les renseignements, généralement auprès de la personne concernée.
- Informer la personne avant la constitution d'un dossier, notamment sur : l'objet du dossier, l'utilisation prévue des données, les catégories d'accès au sein de l'entreprise, le lieu de stockage, ses droits d'accès et de rectification.
- Obtenir le consentement préalable de la personne avant la collecte de données auprès d'un tiers, sauf exception légale (cf. article 18 – Loi sur la protection des RP dans le secteur privé).

En règle générale, l'Entreprise ne peut refuser un bien, service ou emploi si une personne refuse de fournir un renseignement personnel, sauf disposition contraire prévue par la loi.

Utilisation

L'utilisation correspond à la période où les renseignements personnels sont employés par des personnes autorisées au sein de l'entreprise. À ce stade, il convient de limiter l'accès aux seules personnes habilitées lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions, et de restreindre leur exploitation conformément au consentement de la personne concernée, sauf exception prévues par la loi, une fois l'objectif du dossier atteint.

Communication

La communication désigne la période durant laquelle les renseignements personnels sont transmis, par exemple via des systèmes électroniques de prestation de services, courriel, service à la clientèle, sites Web ou à un tiers.

Les obligations comprennent :

- L'obtention du consentement des personnes concernées avant toute communication à un tiers (ex. : assureur, prestataire), sauf exception légales ;
- Le respect des dispositions légales lors de la divulgation sans consentement ;
- L'application des règles spécifiques pour la communication de renseignements personnels hors Québec.

Conservation

La conservation concerne la période pendant laquelle l'entreprise garde les renseignements personnels, quel que soit leur état d'usage.

Les responsabilités à respecter incluent :

- Maintenir la qualité des renseignements personnels afin qu'ils soient à jour et exacts lors de décisions relatives à la personne concernée ;
- Mettre en œuvre des mesures de sécurité appropriées pour assurer la protection des renseignements personnels.

Destruction des renseignements personnels

À la fin de leur cycle de vie, les renseignements personnels doivent être détruits de manière sécurisée dès que leur utilisation n'est plus requise, sauf obligation légale de conservation supplémentaire (ex. : exigences fiscales). Depuis septembre 2023, ils peuvent aussi être anonymisés pour une réutilisation légitime, à condition qu'il soit impossible d'identifier une personne.

Il est obligatoire de mettre en place des mesures de sécurité adaptées à la sensibilité, la finalité, la quantité et le support des données, et de respecter les droits d'accès et de rectification dans un délai de 30 jours. Une réponse tardive équivaut à un refus, qui peut être contesté devant la Commission d'accès à l'information.

La procédure interne doit prévoir :

- L'inventaire des documents contenant des renseignements personnels ;
- La définition des niveaux de confidentialité ;
- L'adaptation de la méthode de destruction au type de support (papier, numérique, etc.) et au niveau de confidentialité ;
- Le respect d'un calendrier de conservation conforme à la loi.

La destruction peut être assurée en interne ou confiée à un prestataire externe via contrat, avec des garanties sur la confidentialité et la traçabilité.

En cas d'incident de confidentialité impliquant des renseignements personnels, l'Entreprise doit agir rapidement pour limiter les risques et prévenir de futurs incidents.

Les questions suivantes permettent d'évaluer la situation :

Qui : personnes concernées par l'incident (employés, clients, partenaires d'affaires) et accès potentiel aux renseignements personnels.

Combien : nombre de personnes touchées.

Quoi : nature des renseignements personnels visés, sensibilité de ces données, risques pour les personnes concernées.

Quand : date de l'incident et date de sa découverte.

Où : lieu de l'incident (au sein de l'organisation, secteur précis, ou chez un tiers).

Pourquoi : causes et mesures de sécurité présentes lors de l'incident ainsi que leur efficacité.

L'identification des mesures à prendre dépend de cette évaluation, chaque situation présentant ses particularités. Les informations pertinentes peuvent ne pas être connues immédiatement, mais il convient d'agir sans délai. L'organisation adapte ses mesures au fur et à mesure de l'évolution de la situation.

Évaluation du risque de préjudice sérieux

Pour chaque incident, il est nécessaire d'évaluer la gravité du risque de préjudice pour les personnes concernées, en tenant compte de la sensibilité des renseignements, des conséquences appréhendées de leur utilisation et de la probabilité d'utilisation à des fins préjudiciables. La consultation du responsable de la protection des renseignements personnels est recommandée, avec le recours possible à d'autres acteurs internes ou externes. Si un risque sérieux est identifié, la Commission ainsi que les personnes concernées doivent être avisées. Dans le cas contraire, il est recommandé de poursuivre l'amélioration des mesures de protection.

Avis à la Commission et aux personnes concernées

Lorsqu'un risque de préjudice sérieux est identifié, la Commission doit être avisée dans les meilleurs délais. Toutes les personnes dont les renseignements sont concernés reçoivent également un avis, sauf si cet avis peut entraver une enquête légale.

Le règlement sur les incidents de confidentialité précise le contenu et les modalités des avis destinés à la Commission et aux personnes concernées.

Avis à la Commission d'Accès à l'Information (CAI)

En cas de risque de préjudice sérieux, l'avis à la Commission doit être transmis par écrit via le formulaire d'avis à CAI. Toute nouvelle information pertinente doit être communiquée rapidement à la Commission.

Aéro Auditeur
Consultant en aviation

Avis aux personnes concernées

L'avis doit préciser la portée et les conséquences de l'incident, inclure une description des renseignements personnels visés, une brève explication des circonstances, la période de l'incident, les mesures prises ou prévues, ainsi que des recommandations pour limiter les risques. Les coordonnées d'une personne ou d'un service de contact doivent être fournies. Un avis public peut être diffusé dans certains cas particuliers définis par la réglementation.

Avis aux personnes susceptibles d'intervenir

Toute personne ou organisme susceptible de réduire le risque de préjudice sérieux peut également être informé, en limitant la transmission aux seuls renseignements nécessaires. Ces communications sont enregistrées par le responsable.

Registre des incidents de confidentialité

Chaque organisation constitue un registre consignant tous les incidents impliquant des renseignements personnels, qu'ils présentent ou non un risque de préjudice sérieux. Ce registre comporte les éléments exigés réglementairement, doit être mis à jour, et conservé cinq ans minimum après découverte de l'incident.

Pouvoir d'ordonnance de la Commission

La Commission est habilitée à ordonner toute mesure visant à protéger les droits des personnes concernées. Elle peut notamment exiger la restitution ou la destruction des renseignements impliqués ou imposer l'envoi d'avis.

Responsabilité relative aux renseignements détenus par des tiers

Lorsqu'un tiers conserve les renseignements personnels, l'organisation reste responsable des obligations associées (mesures, tenue du registre, avis).

Traitement des plaintes

Pour tout questionnement ou plainte concernant la gestion ou la confidentialité des renseignements, il convient de s'adresser au responsable de la protection des renseignements personnels désigné : M Michel Payette (michelpayette@aeroauditeur.ca). Les plaintes sont traitées de façon confidentielle, une réponse écrite étant fournie dans les 30 jours suivant la réception de tous les renseignements nécessaires. Les dossiers de plainte sont documentés et archivés. Il est également possible de saisir la Commission de l'accès à l'information ou tout autre organisme compétent, mais il est recommandé d'attendre d'abord la fin du processus interne.

Sources :

Obligations complètes – site CIA

https://www.cai.gouv.qc.ca/documents/CAI_Guide_obligations_entreprises_vf.pdf

Loi sur la protection des RP dans le secteur privé

https://www.legisquebec.gouv.qc.ca/fr/document/lc/P-39.1