

Politique sur les renseignements personnels

Table des matières

Table des matières	1
PRÉAMBULE.....	2
OBJET ET CADRE NORMATIF	2
DÉFINITIONS	3
COLLECTE, UTILISATION ET CONSERVATION.....	4
TYPES DE RENSEIGNEMENTS PERSONNELS RECUEILLIS.....	4
FINALITÉS POUR LESQUELLES LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS, CONSERVÉS ET UTILISÉS	4
COLLECTE ET UTILISATION.....	6
CONSERVATION	6
CONSENTEMENT	7
ANONYMISATION ET DESTRUCTION	8
PARTAGE.....	9
ACCÈS ET DROITS DES PERSONNES CONCERNÉES.....	9
PLAINTES.....	10
INCIDENTS DE CONFIDENTIALITÉ ET PROCÉDURE DE SIGNALEMENT.....	11
MISES À JOUR	13
ENTRÉE EN VIGUEUR	13
ANNEXE A	14
ANNEXE B	16
ANNEXE C	17
ANNEXE D	19
ANNEXE E.....	30

PRÉAMBULE

La *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, c. P-39) (ci-après, la « Loi ») et les règlements adoptés en vertu de celle-ci ont pour objet d'encadrer l'accès et la protection des renseignements personnels détenus par les entreprises privées.

Le Groupe Rezo œuvre dans le secteur de l'affichage, de lettrage et des enseignes. Entre autres, elle offre des solutions en matière de lettrage d'automobiles et autres véhicules, d'affichage et de création d'enseignes publicitaires.

Dans le cours de ses activités, Le Groupe Rezo possède, traite, utilise, conserve, communique et détruit des Renseignements personnels concernant ses Employés, Clients et Fournisseurs. À ce titre, elle reconnaît l'importance du respect de la vie privée et de la protection des Renseignements personnels qu'elle détient et auxquels elle a accès.

Afin d'assurer sa conformité avec les obligations législatives en la matière, Le Groupe Rezo s'est dotée de la présente « Politique sur les renseignements personnels » (ci-après, « Politique »). Celle-ci décrit les principes applicables en matière de protection, traitement, conservation, anonymisation, entre autres, des Renseignements personnels détenus par Le Groupe Rezo.

OBJET ET CADRE NORMATIF

1. La présente Politique définit et encadre la collecte, la conservation, l'utilisation, le partage et la destruction des Renseignements personnels de tout Employé, Client, Fournisseur, dirigeant ou administrateur de Le Groupe Rezo.

Elle encadre la gestion des Renseignements personnels tout au long de leur Cycle de vie et l'exercice des droits des Personnes concernées. Elle désigne la personne responsable de la protection des Renseignements personnels.

Elle vise à mettre en place des mesures permettant de protéger la confidentialité des Renseignements personnels conformément à la Loi et ses règlements.

2. La personne responsable des renseignements personnels au sein de Le Groupe Rezo (ci-après, « Personne responsable ») a un accès aux Renseignements personnels de tout Employé, Client et Fournisseur. Elle est responsable des Renseignements personnels, des Renseignements personnels sensibles et de la manière dont ils sont protégés et traités tout au long de leur Cycle de vie.

La personne responsable des renseignements personnels de Le Groupe Rezo peut déléguer par écrit ses tâches à un ou à plusieurs de ses Employé(s). Cette ou ces personnes se doivent de signer une attestation écrite concernant le respect de la présente Politique.

3. Tout Employé de Le Groupe Rezo est informé du contenu de la présente Politique et se doit de la respecter.

Prenez note que Le Groupe Rezo n'est pas responsable des pratiques de ses Fournisseurs relativement à la vie privée et à la protection des renseignements personnels.

DÉFINITIONS

4. Les définitions qui suivent s'appliquent à la présente Politique.

Anonymiser/anonymisé(s) : changement irréversible aux Renseignements personnels qui rend l'identification de la Personne concernée impossible, que ce soit directement ou indirectement. Le terme « irréversible » implique qu'il ne doit pas être possible, au moment de l'anonymisation et en tout temps, et ce, en considérant un futur prévisible, d'identifier de nouveau la Personne concernée directement ou indirectement.

Client : personne physique ou morale ayant signé un contrat afin de bénéficier des services de Le Groupe Rezo.

Cycle de vie : l'ensemble des étapes visant le traitement d'un Renseignement personnel soit la collecte, l'utilisation, le partage, la conservation, la destruction et l'anonymisation de celui-ci.

Employé(s) : personne physique qui travaille pour Le Groupe Rezo moyennant rémunération ou une expérience pratique, telle qu'un stage.

Fournisseur(s) : personne physique ou morale qui fournit à Le Groupe Rezo de la marchandise, des services de d'impression, d'entretien, de gestion de données ou d'autres services ou marchandises, qui pourrait avoir accès à des Renseignements dans le cadre des services qui sont rendus, incluant tout sous-traitant exécutant une prestation de services.

Personne(s) concernée(s) : personne physique à qui se rapportent les Renseignements.

Personne responsable des renseignements personnels : la personne désignée responsable de la protection des renseignements personnels au sein de Le Groupe Rezo.

Politique : la présente « Politique sur les renseignements personnels ».

Renseignement(s) personnel(s) : toute information qui concerne une personne physique et qui permet de l'identifier.

Renseignement personnel sensible : un renseignement qui, par sa nature notamment médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

COLLECTE, UTILISATION ET CONSERVATION

5. Le Groupe Rezo se doit de détenir certains Renseignements personnels dans le but d'atteindre des objectifs précis, que ce soit envers leurs Employés, Clients ou Fournisseurs. Ces objectifs sont définis aux articles suivants.

TYPES DE RENSEIGNEMENTS PERSONNELS RECUEILLIS

6. Le Groupe Rezo recueille différents types de Renseignements personnels dans le cadre de ses activités et de ses prestations de services, incluant :
 - a. Des renseignements d'identité ou biographiques;
 - b. Des renseignements relatifs aux préférences de communication et de marketing;
 - c. Des renseignements financiers, bancaires et relatifs à la facturation;
 - d. Des renseignements relatifs au recrutement et à la gestion d'employés;
 - e. Des renseignements relatifs aux Clients et aux contrats de services;
 - f. Des renseignements fournis par des Clients ou Fournisseurs pour le compte de ceux-ci ou qui sont produits dans le cadre de la prestation de services;
 - g. Des renseignements d'identification ou de vérification d'antécédents;
 - h. Des renseignements relatifs aux personnes physiques et personnes morales œuvrant au sein des Clients et Fournisseurs de Le Groupe Rezo qui bénéficient des services de Le Groupe Rezo;
 - i. Tout autre renseignement fourni de plein gré par un Employé, Client ou Fournisseur.
7. Le Groupe Rezo ne recueille que les Renseignements personnels nécessaires à la réalisation de ses activités et aux fins spécifiques décrites ci-bas.

FINALITÉS POUR LESQUELLES LES RENSEIGNEMENTS PERSONNELS SONT RECUEILLIS, CONSERVÉS ET UTILISÉS

8. En ce qui concerne les Employés de Le Groupe Rezo, les Renseignements personnels sont recueillis, conservés et utilisés pour les finalités suivantes :
 - a. Pour permettre au département de ressources humaines de maintenir un dossier d'employé à jour, afin de pouvoir, entre autres, identifier, évaluer et communiquer avec les Employés;
 - b. Pour assurer la santé et la sécurité des Employés;
 - c. Pour l'exécution des obligations contenues aux contrats de travail des Employés et leur évaluation de rendement;
 - d. Pour établir et maintenir une stratégie de recrutement pour de futurs Employés;
 - e. Pour satisfaire aux exigences légales et gouvernementales, notamment celles des autorités fiscales;
 - f. Pour des besoins administratifs et de gestion;

- g. Pour toutes autres fins compatibles avec les fins énoncées ci-dessus.

Cependant, Le Groupe Rezo se réserve le droit de modifier ces finalités avec un avis à la Personne concernée.

- 9. En ce qui concerne les Clients de Le Groupe Rezo, les Renseignements personnels sont recueillis, conservés et utilisés pour les finalités suivantes :
 - a. Pour traiter une demande de services et gérer les besoins en tant que Clients;
 - b. Pour offrir aux Clients un service continu, par l'entremise d'un serveur sécurisé et encrypté sur les postes de travail fixes (ordinateurs). La conservation de ces données est sauvegardée et protégée par mot de passe. Les données, incluant des Renseignements personnels, peuvent être conservées pour une durée n'excédant pas dix (10) ans, après quoi elles sont détruites;
 - c. Pour créer et maintenir des listes de contacts et d'envoi;
 - d. Pour confirmer l'identité des Clients et vérifier l'exactitude des renseignements fournis;
 - e. Pour établir un lien entre l'identité de la Personne concernée et l'organisme ou la personne morale concernée par la prestation de services;
 - f. Pour recevoir les paiements pour les services offerts;
 - g. Pour joindre les Clients afin de promouvoir de nouveaux services ou produits offerts par Le Groupe Rezo;
 - h. Pour analyser les données afin de prendre de meilleures décisions sur les services offerts aux Clients et la manière dont ils sont offerts;
 - i. Pour satisfaire aux exigences légales et gouvernementales, notamment celles des autorités fiscales;
 - j. Pour des besoins administratifs et de gestion;
 - k. Pour toutes autres fins compatibles avec les fins énoncées ci-dessus.

Cependant, Le Groupe Rezo se réserve le droit de modifier ces finalités avec un avis à la Personne concernée.

- 10. En ce qui concerne les Fournisseurs de Le Groupe Rezo, les Renseignements personnels sont recueillis, conservés et utilisés pour les finalités suivantes :
 - a. Pour établir, maintenir ou rompre toute relation contractuelle établie dans le cours des activités d'une entreprise;
 - b. Pour communiquer avec des personnes morales ou personnes physiques afin de faire la promotion des services offerts par Le Groupe Rezo;
 - c. Pour créer et maintenir des listes de contacts et d'envoi, par l'entremise de la conservation de ces données qui est sauvegardée et protégée par mot de passe. Les données, incluant des Renseignements personnels, peuvent être conservées pour une durée n'excédant pas dix (10) ans, après quoi elles sont détruites;
 - d. Pour satisfaire aux exigences légales et gouvernementales, notamment celles des autorités fiscales;
 - e. Pour des besoins administratifs et de gestion;
 - f. Pour toutes autres fins compatibles avec les fins énoncées ci-dessus.



Cependant, Le Groupe Rezo se réserve le droit de modifier ces finalités avec un avis à la Personne concernée.

COLLECTE ET UTILISATION

- 11.** Les Renseignements personnels sont recueillis par le biais d'interactions avec les Personnes concernées ou ses représentants autorisés, lorsqu'il y a une relation contractuelle existante ou qui s'apprête à être établie, entre Le Groupe Rezo et la Personne concernée, que ce soit un contrat de services ou un contrat de travail.

Les interactions peuvent être effectuées sous forme verbale ou écrite, de façon physique ou électronique.

- 12.** Le Groupe Rezo réalise une évaluation des facteurs susceptibles de porter atteinte à la vie privée des Personnes concernées, notamment dans le contexte des traitements suivants de Renseignements personnels :

- a. Avant d'entreprendre un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des Renseignements personnels ;
- b. Avant de recueillir des Renseignements personnels nécessaires à l'exercice des attributions ou à la mise en œuvre d'un programme d'un organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune ;
- c. Avant de communiquer des Renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces Renseignements personnels à des fins d'étude, de recherche ou de production de statistiques ;
- d. Avant de communiquer des Renseignements personnels sans le consentement des personnes concernées ;
- e. Avant de communiquer des Renseignements personnels à l'extérieur du Québec.

CONSERVATION

- 13.** Les Renseignements personnels des Employés, Clients et Fournisseurs recueillis sont conservés pour exécuter les finalités détaillées à l'article 8, 9, 10.
- 14.** Tous les Employés de Le Groupe Rezo s'obligent, comme condition d'emploi, à protéger les Renseignements personnels ou les Renseignements personnels sensibles et leur caractère confidentiel et à en assurer la sécurité. Cette obligation reste en vigueur même lorsqu'un Employé quitte Le Groupe Rezo.

Ceci s'applique aux Renseignements personnels et Renseignements personnels sensibles des Employés, Clients et Fournisseurs de Le Groupe Rezo.

15. Seuls les Employés autorisés ont accès aux Renseignements personnels et aux plateformes sur lesquels ils sont regroupés, traités ou entreposés. Les systèmes informatiques et les procédures de traitement des données sont munis de mécanismes de contrôles appropriés, lesquels sont vérifiés de façon continue pour garantir le respect des politiques de Le Groupe Rezo en matière de sécurité et de protection des Renseignements personnels.

Ceci s'applique aux Renseignements personnels et Renseignements personnels sensibles des Employés, Clients et Fournisseurs.

CONSENTEMENT

16. La collecte de Renseignements personnels se fait auprès de la Personne concernée sur la base d'un consentement manifeste, libre et éclairé et donné à des fins spécifiques. Celui-ci est donné via un formulaire fourni à l'**Annexe A**.
17. Le consentement de la Personne concernée est obtenu avant la collecte des données et après la divulgation des finalités pour lesquelles elles sont colligées.
18. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.
19. Les Renseignements personnels recueillis ne peuvent être utilisés que pour les fins pour lesquelles elles ont été collectées, sauf avec le consentement de la Personne concernée.
20. Le Groupe Rezo ne vend pas, ne troque pas et n'échange pas de Renseignements personnels recueillis. À moins d'être autorisé par la Loi, Le Groupe Rezo ne recueille aucun Renseignement personnel auprès de la Personne concernée sans obtenir d'abord son consentement à la collecte, à l'utilisation et au partage de ceux-ci.
21. Certaines circonstances pourraient justifier ou permettre l'utilisation ou la communication de Renseignements personnels par Le Groupe Rezo ou l'obliger à divulguer certains Renseignements personnels sans le consentement de la Personne concernée. De telles circonstances peuvent inclure notamment les suivantes :
 - a. Utilisation à des fins compatibles avec celles pour lesquelles le Renseignement personnel a été recueilli;
 - b. Utilisation manifestement au bénéfice de la Personne concernée;
 - c. Utilisation à l'occasion d'une transaction commerciale ou d'un contrat de services;
 - d. Utilisation nécessaire à des fins d'étude, recherche ou de production de statistiques, une fois que le Renseignement personnel ait été dépersonnalisé;

- e. Au besoin, pour permettre à Le Groupe Rezo d'exercer les recours disponibles ou limiter les dommages que Le Groupe Rezo pourrait subir;
 - f. Lorsque la loi, une ordonnance, un tribunal, un organisme gouvernemental ou tout autre tribunal l'exige;
 - g. Lorsque les renseignements sont publics;
- 22.** Une Personne concernée peut à tout moment refuser de consentir à ce que Le Groupe Rezo recueille, utilise ou communique des Renseignements personnels, ou peut retirer son consentement, en donnant à Le Groupe Rezo un préavis raisonnable, à la condition toutefois que ce refus ou ce retrait ne limite pas la capacité de Le Groupe Rezo d'offrir ses services, de se conformer aux lois applicables pour ce qui est des Renseignements personnels en sa possession et ne limite aucun des droits de Le Groupe Rezo en vertu de la Politique ou des droits qui lui sont accordés par la législation applicable.

Dans certains cas, si une Personne concernée refuse de donner son consentement, il y a un risque que Le Groupe Rezo soit dans l'impossibilité d'exécuter sa prestation de services ou de desservir son Client, son Employé ou son Fournisseur.

- 23.** Dans la mesure où Le Groupe Rezo a recours à une technologie qui comprends des fonctions d'identification, de localisation ou de profilage, la Personne concernée sera, au préalable, informée qu'une telle technologie est utilisée et des moyens offerts pour activer les fonctions d'identification, de localisation ou de profilage.

ANONYMISATION ET DESTRUCTION

- 24.** Lorsque les finalités pour lesquels ils ont été recueillis ont été atteintes, Le Groupe Rezo s'engage à détruire ou Anonymiser tout Renseignement personnel. Lorsque les Renseignements personnels sont détruits ou Anonymisés, Le Groupe Rezo veille à ce qu'il n'y ait aucun accès non autorisé.

Ceci s'applique aux Renseignements personnels et Renseignements personnels sensibles des Employés, Clients et Fournisseurs du Le Groupe Rezo.

- 25.** Le Groupe Rezo détruit de façon sécuritaire les Renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis sont accomplies, sous réserve des lois applicables quant à leur conservation.

Le terme « irréversible » implique qu'il ne doit pas être possible, au moment de l'anonymisation et en tout temps, et ce, en considérant un futur prévisible, d'identifier de nouveau la personne concernée directement ou indirectement.

PARTAGE

26. Le Groupe Rezo peut partager des Renseignements personnels de ses Clients ou Fournisseurs à d'autres Employés et Fournisseurs, des personnes ou organisations qui fournissent des services pour Le Groupe Rezo, dont notamment des personnes ou organisations qui s'occupent de la mise en place et de la maintenance des systèmes informatiques.
27. Le Groupe Rezo peut procéder au partage de Renseignements personnels de ses Employés, Clients ou Fournisseurs avec d'autres Fournisseurs, dans le but d'accomplir toute finalité inscrite à l'article 8, 9 ou 10 de cette Politique. Seuls les Renseignements personnels nécessaires sont partagés avec les Fournisseurs.

ACCÈS ET DROITS DES PERSONNES CONCERNÉES

28. Toute Personne concernée a les droits suivants sur les Renseignements personnels qui sont détenus par Le Groupe Rezo :
 - a. Droit d'accès au dossier;
 - b. Droit de rectifier tout renseignement incomplet ou inexact;
 - c. Droit d'être informée que les renseignements sont détenus pour d'autres fins que celles préalablement déterminées;
 - d. Droit d'être informée que les renseignements peuvent être utilisés pour rendre une décision fondée sur un traitement automatisé;
 - e. Droit d'être informée lorsque les renseignements sont utilisés afin de rendre une décision exclusivement basée sur un traitement automatisé.
29. Toute demande visée à l'article 28 doit être effectuée par écrit à la Personne responsable, dont les coordonnées se trouvent à l'article 34. La demande doit inclure de quel droit la Personne concernée veut se prévaloir, les motifs pour lesquels elle désire se prévaloir de ses droits et ses coordonnées. Cette demande peut être envoyée par courriel.
30. Le Groupe Rezo s'engage à transmettre un accusé de réception et s'engage à donner suite à la demande dans un délai raisonnable de trente (30) jours suivant sa réception.
31. Le Groupe Rezo ne fait la mise à jour des Renseignements personnels de ses Employés, Clients ou Fournisseurs que sur demande. Par conséquent, il est dans le meilleur intérêt de la Personne concernée d'informer Le Groupe Rezo sans tarder de tout changement de nom, d'adresse ou de tout autre Renseignement personnel pertinent.
32. Le Groupe Rezo se réserve le droit de ne pas communiquer certains Renseignements personnels, même lorsque demandés, dans certaines circonstances, notamment les suivantes :

- a. Cette opération entraînerait la communication de Renseignements personnels, y compris des opinions, sur une autre personne, vivante ou décédée;
 - b. La communication des Renseignements personnels entraînerait la divulgation de secrets commerciaux ou de renseignements confidentiels ou exclusifs à Le Groupe Rezo ou si une telle divulgation pourrait miner l'intégrité du processus d'embauche, d'évaluation d'Employé(s) ou tout autre processus interne de Le Groupe Rezo;
 - c. La communication des Renseignements personnels nuirait à des négociations contractuelles ou autres impliquant Le Groupe Rezo;
 - d. Les Renseignements personnels font l'objet d'un litige ou sont protégés par le secret professionnel ou par un autre privilège attaché à la profession juridique;
 - e. Les Renseignements personnels sont difficiles d'accès et le travail ou les coûts pour les extraire seraient hors de proportion avec leur nature ou leur valeur;
 - f. Les Renseignements personnels n'existent pas ou sont introuvables, ayant notamment été sujets à une Destruction ou une Anonymisation;
 - g. Les Renseignements personnels peuvent gêner ou entraver le travail d'agences d'application de la loi ou d'autres activités d'enquêtes ou de réglementation d'un organisme autorisé par la loi à mener ces activités;
 - h. La communication des Renseignements personnels peut être refusée ou est interdite par les lois applicables.
- 33.** Si Le Groupe Rezo refuse de donner accès aux Renseignements personnels de la Personne concernée, celle-ci recevra une explication écrite avec une référence à la disposition de la Loi pertinente, les recours s'offrant à la Personne concernées et les délais dans lesquelles elle devra agir, sauf si la loi l'interdit. Cette décision peut être contestée via un courriel à la Personne responsable, en suivant les mêmes modalités que celles détaillées à l'article 35.

PLAINTES

- 34.** Toute question, commentaire, préoccupation ou plainte relativement au traitement des renseignements personnels, la présente Politique ou des pratiques en matière de protection de Renseignements personnels devraient être transmis à la Personne responsable dont les coordonnées sont les suivantes :

Noémie Martel – Directrice expérience clients

Personne responsable des renseignements personnels de Le Groupe Rezo

307 Rang Cabane Ronde, L'Épiphanie (QC) J5X 3N5

(450) 582-7824

ventes@legrouperezo.com

- 35.** La plainte doit être formulée en remplissant le document de « Description d'une plainte » fourni à l'**Annexe B**.

36. La plainte devra inclure une description de l'incident, des parties impliquées et des circonstances qui l'entoure. Les coordonnées de la personne qui effectue la plainte seront également requises.
37. La Personne responsable répondra à chaque demande dans un délai raisonnable de trente (30) jours.

INCIDENTS DE CONFIDENTIALITÉ ET PROCÉDURE DE SIGNALEMENT

38. Les membres de Le Groupe Rezo, leurs Clients, Fournisseurs ou Employés signalent sans délai à la Personne responsable des renseignements personnels de Le Groupe Rezo tout incident ou suspicion d'incident de confidentialité dont ils ont connaissance.

Noémie Martel – Directrice expérience clients

Personne responsable des renseignements personnels de Le Groupe Rezo

307 Rang Cabane Ronde, L'Épiphanie (QC) J5X 3N5

(450) 582-7824

ventes@legrouperezo.com

39. Lorsque possible, l'auteur du signalement prend les mesures adéquates afin de contenir l'incident et d'en limiter les torts ou dommages, et ce, le plus rapidement possible.
40. La personne responsable des renseignements personnels détermine s'il s'agit bien d'un incident de confidentialité, en répondant successivement aux deux (2) questions suivantes :
 1. Les informations objets de l'Incident sont-elles des Renseignements personnels confidentiels?
 2. Ces Renseignements personnels ont-ils fait l'objet :
 - a. d'une consultation par une personne/entité non autorisée à en prendre connaissance;
 - b. d'une transmission à une personne/entité non autorisée à les recevoir;
 - c. d'une utilisation à des fins non autorisées par la Loi ou par le titulaire de ces renseignements;
 - d. d'une perte ou d'un vol dans des circonstances telles que l'hypothèse a, b ou c soit possible ?

Dans l'affirmative, le processus se poursuit. La Personne responsable remplit une fiche décrivant l'incident, les circonstances l'entourant, les personnes concernées, les solutions qui ont été envisagées ou posées et toute autre information utile au sujet de l'incident de confidentialité.

Dans le cas où il n'y a qu'une seule question qui est répondue par l'affirmative, le processus cesse, n'étant pas en présence d'un incident de confidentialité.

41. La personne qui entend effectuer un signalement suit la procédure suivante établie à l'**Annexe C**.

42. Dans le cas d'un risque plausible de préjudice sérieux :

La Personne responsable informe les personnes et entités suivantes :

- A. La Commission d'accès à l'information du Québec (CAI);
 - a. Un avis écrit doit être soumis à la CAI selon les modalités détaillées sur le formulaire fourni à l'**Annexe D**.
- B. Le Commissariat à la protection de la vie privée du Canada (CPVPC);
 - a. Un avis écrit doit être soumis au CPVPC selon les modalités détaillées sur le formulaire fourni à l'**Annexe E**.
- C. La Personne concernée par l'incident;
 - a. Cet avis se fait par tout moyen qui permet de joindre la Personne concernée dans un délai raisonnable. Il peut notamment s'agir d'un courriel ou d'une lettre postale.

Dans certains cas particuliers d'incident impliquant des Personnes concernées résidant hors du Québec, il est possible qu'une autre autorité régulatrice (au Canada ou à l'étranger) doive être informée de l'incident.

Par ailleurs, si l'incident constitue un crime, Le Groupe Rezo en informe le service de police compétent.

43. En l'absence d'un risque plausible de préjudice sérieux :

La Personne responsable détermine s'il pertinent d'informer la Personne concernée de l'incident. Elle peut choisir de le faire pour des raisons de transparence ou de gestion. Ces raisons sont documentées dans le *Registre des incidents de confidentialité*, tel que décrit à l'article 45.

44. La Personne responsable des renseignements personnels:

- Applique les mesures correctrices qui s'imposent, afin de faire cesser l'incident;
- Adopte les mesures préventives qui lui paraissent appropriées, afin d'éviter qu'un tel incident ne se reproduise;
- Mentionne dans le *Registre des incidents* toutes les mesures prises.

45. Le *Registre des incidents* permet de documenter tous les incidents de confidentialité survenus. Outre son rôle essentiel lors d'un éventuel audit de conformité, ce registre permet de bonifier les plans de résilience, d'orienter au besoin l'offre de formation et de sensibilisation et d'améliorer en continu la gestion des incidents.

Le registre répertorie notamment, pour chaque incident :

- Sa nature;
- Sa date de survenance;
- La date à laquelle il a été découvert;
- La date à laquelle il a été déclaré à la personne concernée;
- Le type de renseignements personnels compromis;
- Le nombre des personnes concernées;

- Les conséquences de l'incident sur Le Groupe Rezo et les personnes concernées;
- Les mesures prises pour remédier, atténuer ou contenir les conséquences négatives de l'incident et celles pour éviter qu'un tel incident ne se reproduise;
- Les dates et moyens d'une notification de l'incident.

MISES À JOUR

46. Afin de suivre l'évolution du cadre normatif applicable en matière de protection des Renseignements personnels et d'assurer sa conformité avec la réglementation en vigueur, Le Groupe Rezo se réserve le droit de modifier et mettre la présente Politique en tout temps.

47. La dernière mise à jour de la présente Politique a été effectuée en : septembre 2023.

ENTRÉE EN VIGUEUR

48. La présente Politique entre en vigueur à partir du 12 septembre 2023.



ANNEXE A

FORMULAIRE D'OBTENTION DU CONSENTEMENT (EMPLOYÉ)

En vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé*, Le Groupe Rezo est autorisé à recueillir des renseignements personnels à votre sujet en tant qu'employé.

Il est nécessaire d'obtenir votre consentement pour que Le Groupe Rezo puisse obtenir et conserver ces renseignements. Le Groupe Rezo ne peut transmettre vos renseignements personnels à aucune personne ou organisation sans votre consentement écrit, sauf lorsque la loi le permet. À l'heure actuelle, Le Groupe Rezo utilise ces technologies de profilage afin d'évaluer ses employés : Microsoft Office Suite 365, SAGE et 3CX (UC-365). Vous ou votre représentant autorisé avez le droit de demander une copie des renseignements contenus dans votre dossier et de demander la correction de ceux-ci. Vous pouvez faire ce genre de demande en écrivant un courriel à la personne responsable des renseignements personnels de Le Groupe Rezo, aux coordonnées suivantes :

Noémie Martel – Directrice expérience clients

Personne responsable des renseignements personnels de Le Groupe Rezo

307 Rang Cabane Ronde, L'Épiphanie (QC) J5X 3N5

(450) 582-7824

ventes@legrouperezo.com

Consentement

Par la présente, vous autorisez Le Groupe Rezo à recueillir, conserver et utiliser vos renseignements personnels. Veuillez noter que les finalités pour lesquelles nous recueillons et utilisons vos renseignements sont détaillées dans notre *Politique sur les renseignements personnels*.

Renseignements personnels		
Préfix (M., Mme, etc.)	Prénom(s) et Nom(s)	
Adresse postale (numéro, rue, app.)		Ville
Province ou territoire	Pays	Code postal



Numéro Assurance Sociale	Téléphone	Courriel
Contact d'urgence (Nom, # téléphone, relation)		

J'autorise Le Groupe Rezo à obtenir des renseignements personnels à mon sujet et dans le but d'exécuter leurs obligations en tant qu'employeur.

En tant qu'employé, je m'engage à prendre connaissance de la *Politique sur les renseignements personnels* et de la respecter.

(NOM DE L'EMPLOYÉ)

(DATE)

Dans ce document, l'emploi du masculin pour désigner des personnes n'a d'autres fins que celle d'alléger le texte.

ANNEXE B

DESCRIPTION D'UNE PLAINTE

Renseignements de la personne qui porte la plainte		
Préfix (M., Mme, etc.)	Prénom(s) et Nom(s)	
Adresse postale (numéro, rue, app.)		Ville
Province ou territoire	Pays	Code postal
Courriel		Téléphone

Description des événements, personnes concernées, des dommages potentiels, de l'enjeu soulevé par cette plainte :

ANNEXE C

FORMULAIRE DE SIGNALEMENT EN CAS D'INCIDENT DE CONFIDENTIALITÉ PRÉSENTANT UN RISQUE PLAUSIBLE DE PRÉJUDICE SÉRIEUX

Vous avez cliqué sur un lien douteux? Un de vos comptes a été compromis? Vous êtes au courant d'un risque pour la sécurité des systèmes de Le Groupe Rezo ? Vous êtes au bon endroit pour signaler ce problème!

Tout incident qui compromet la disponibilité, l'intégrité et la confidentialité des informations détenues par Le Groupe Rezo, tel que :

- Le piratage (une tentative de piratage doit également être signalée);
- La fraude informatique;
- L'intrusion dans un système informatique;
- L'infection d'un poste de travail par un virus ou d'autres codes malicieux;
- L'utilisation non autorisée, l'altération ou la destruction de données, de logiciels, d'applications ou de matériel informatique;
- Le vol ou la perte de matériel informatique;
- Le vol d'identité;
- L'accès non autorisé à des installations informatiques;
- La distribution non autorisée d'informations confidentielles;
- L'utilisation des installations informatiques pour commettre des actes illégaux;
- L'utilisation du courrier électronique à des fins commerciales non liées à Le Groupe Rezo, de harcèlement ou de menace;
- En remplissant le formulaire ci-dessous, un enregistrement d'incident de sécurité sera créé et celui-ci sera géré jusqu'à sa résolution.

Informations de la personne qui effectue le signalement		
Préfix (M., Mme, etc.)	Prénom(s) et Nom(s)	
Adresse postale (numéro, rue, app.)		Ville
Province ou territoire	Pays	Code postal
Courriel		Téléphone

S'agit-il d'un incident lié à la protection des renseignements personnels ? (Oui/Non)
Description du problème

Informations sur la personne concernée par l'incident		
Préfix (M., Mme, etc.)	Prénom(s) et Nom(s)	
Adresse postale (numéro, rue, app.)		Ville
Province ou territoire	Pays	Code postal
Courriel		Téléphone



ANNEXE D

AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

CONCERNANT UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS ET QUI PRÉSENTE UN RISQUE DE PRÉJUDICE SÉRIEUR

[Page suivante]



Imprimer le formulaire

Formulaire : Rapport d'atteinte à la LPRPDE

Destiné aux organisations du secteur privé déclarant des atteintes aux mesures de sécurité au Commissariat à la protection de la vie privée du Canada (Commissariat)

Qu'est-ce qu'une atteinte aux mesures de sécurité (« atteintes »)?

Une « atteinte aux mesures de sécurité » est définie comme suit dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) : communication non autorisée ou perte de renseignements personnels, ou accès non autorisé à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation prévues à l'article 4.7 de l'annexe 1 de la LPRPDE ou du fait que ces mesures n'ont pas été mises en place.

Suis-je tenu de soumettre un rapport au Commissariat si mon organisation a subi une atteinte?

La *Loi sur la protection des renseignements personnels numériques* a été adoptée le 18 juin 2015. Cette loi comprend une modification à la LPRPDE exigeant que les organisations déclarent au Commissariat les atteintes aux mesures de sécurité impliquant des renseignements personnels dont elles ont la gestion s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à un individu.

Cette obligation entre en vigueur le 1^{er} novembre 2018. Consultez notre [document d'orientation](#) pour de plus amples renseignements. Le présent formulaire peut être utilisé par les organisations qui ont subi une atteinte à la vie privée afin de respecter leurs obligations juridiques aux termes de la [LPRPDE](#) et du [Règlement sur les atteintes aux mesures de sécurité : DORS/2018-64](#).

Je suis une personne visée par une atteinte. Est-ce que je devrais utiliser ce formulaire?

Les intéressés qui souhaitent porter plainte à propos d'une atteinte à leur vie privée par une organisation ne devraient pas utiliser ce formulaire. Consultez plutôt la section [Signaler un problème](#) de notre site Web.

Devrais-je inclure des renseignements personnels dans ce formulaire?

Non. Il n'est pas nécessaire d'inclure dans le formulaire des renseignements personnels autres que les coordonnées des personnes qui peuvent répondre, au nom de l'organisation, aux questions de suivi du Commissariat. Par exemple, il n'est pas nécessaire d'inclure les noms des intéressés, ou d'autres détails permettant de les identifier, à moins qu'ils ne soient nécessaires afin d'expliquer la nature des renseignements personnels visés. Il a pour but de fournir des renseignements au sujet de l'atteinte et de la nature des renseignements.



Combien de temps après l'atteinte dois-je soumettre ce formulaire?

Les organisations doivent signaler une atteinte aux mesures de sécurité au Commissariat dès que possible après que l'organisation détermine que l'atteinte s'est produite, même si tous les renseignements (p. ex., la cause, ou les mesures d'atténuation prévues) ne sont pas connus ou confirmés. Vous pouvez ajouter ou corriger des renseignements, au fur et à mesure qu'ils sont disponibles.

Que peut-il arriver une fois qu'une atteinte est déclarée au Commissariat?

Lorsque le Commissariat prend connaissance d'une atteinte, il pourrait demander des renseignements supplémentaires aux organisations concernées et ensuite chercher à déterminer et à résoudre tout problème de conformité à la LPRPDE. Il peut aussi tenter d'atténuer tout effet dommageable de l'incident.

De quelle façon le Commissariat traitera-t-il les renseignements fournis par les organisations dans un rapport d'atteinte?

De façon générale, le Commissariat a le devoir de préserver la confidentialité des rapports d'atteinte qui sont soumis au commissaire à la protection de la vie privée en application de la LPRPDE. Cependant, il y a certaines exceptions à cette obligation. Par exemple, le Commissariat pourrait divulguer des renseignements contenus dans un rapport d'atteinte à :

- ses homologues nationaux et internationaux, conformément à des ententes ou à des arrangements visant l'échange de renseignements; ou
- une institution gouvernementale, si le commissaire a des motifs raisonnables de croire que les renseignements seraient utiles dans une enquête sur une contravention au droit fédéral ou provincial.

Le commissaire peut aussi divulguer des renseignements publiquement lorsqu'il estime qu'il est dans l'intérêt public de le faire. Les communications de renseignements dans l'intérêt public sont examinées attentivement au cas par cas et le commissaire ne communiquerait normalement pas publiquement des renseignements qui présenteraient un risque pour la sécurité.

Les renseignements fournis dans un rapport d'atteinte destiné au Commissariat pourraient parfois être utilisés comme fondement pour amorcer une enquête et dans toute enquête qui s'ensuit.

La *Loi sur la protection des renseignements personnels numériques* modifie également la *Loi sur l'accès à l'information* (LAI) afin de créer une exception, en vertu de la loi, à la divulgation de tout rapport d'atteinte à la sécurité des données en réponse à des demandes d'accès à l'information présentées aux termes de la LAI.

Où puis-je obtenir de plus amples renseignements sur la façon de répondre à une atteinte à la vie privée?

Veuillez consulter notre document d'orientation intitulé : [Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité.](#)



Rapport d'atteinte à la LPRPDE

Dans le présent formulaire, l'astérisque (*) indique les champs obligatoires, c'est-à-dire qui sont exigés par la loi. Les autres champs sont optionnels.

rapport initial

rapport modifié ou mis à jour

Renseignements de l'organisation

* Nom officiel de l'organisation :

Adresse de l'organisation :

* Coordonnées d'une personne qui peut répondre, au nom de l'organisation, aux questions du Commissariat au sujet de l'atteinte :

* Veuillez en choisir un : Représentant interne Représentant externe

* Nom :

* Titre/poste :

Code pays :

* Téléphone :

Poste :

* Courriel :

* Adresse municipale :

* Ville :

* Province/territoire :

* Code postal :

* Pays :



Description de l'atteinte

* **Le nombre d'individus visés par l'atteinte ou, s'il n'est pas connu, une approximation de ce nombre :** (Si possible, veuillez également fournir le nombre total de Canadiens visés par cette atteinte.)

* Total des intéressés :

Canadiens touchés :

Commentaires :

* **La date à laquelle l'atteinte a eu lieu :**

(Veuillez indiquer la date ou la période où l'atteinte a eu lieu, y compris une plage de dates, le cas échéant.)

* Date à laquelle l'atteinte a débuté :

Date à laquelle l'atteinte a pris fin :

Commentaires :

Type d'atteinte :

(Veuillez choisir l'option parmi les choix ci-dessous celle qui décrit le mieux le type d'atteinte.)



*** Les circonstances de l'atteinte et, si elle est connue, sa cause :**

1. description de toutes les organisations visées par l'atteinte y compris leur rôle en ce qui a trait aux renseignements personnels en question,
2. comment et pourquoi l'atteinte a eu lieu (veuillez inclure quelques détails techniques concernant l'atteinte y compris une description de la méthode utilisée lors de l'attaque si celle-ci s'est produite),
3. quand l'atteinte a été découverte,
4. où l'atteinte a eu lieu,
5. qui peut avoir eu accès aux renseignements personnels (dans la mesure où ces personnes sont connues).



Description des mesures de sécurité pertinentes en place au moment de l'atteinte afin d'empêcher le type d'incident qui a eu lieu :

*** La nature des renseignements personnels visés par l'atteinte dans la mesure où elle est connue :**

Décrivez le type et la nature des renseignements personnels faisant l'objet de l'atteinte (par exemple, nom, numéro de téléphone, adresse courriel, numéro de compte, numéro d'assurance sociale, etc.). Veuillez préciser si les renseignements personnels du client ou de l'employé ont été consultés.

IMPORTANT : Il n'est pas exigé d'inclure dans la présente section des renseignements identificatoires, à moins qu'ils ne soient nécessaires pour expliquer la nature et la sensibilité des renseignements.



Avis

Le [Règlement sur les atteintes aux mesures de sécurité](#) prévoit que tout avis concernant une atteinte représentant un risque réel de préjudice grave doit contenir certains éléments précisés à l'article 3 dudit règlement.

*** Description des mesures que l'organisation a prises ou a l'intention de prendre pour aviser les intéressés :**

* Est-ce que les intéressés ont été avisés?

Oui

Non

Date à laquelle l'avis a débuté (ou est prévu) :

Date à laquelle l'avis a pris fin :

Méthode de notification utilisée pour les intéressés. (Veuillez choisir l'option parmi les choix ci-dessous.)

*** Décrivez la forme de l'avis :**

(Par exemple, cela peut comprendre les moyens suivants : directement par lettre, courriel, téléphone; indirectement par annonce dans les journaux, etc.)

IMPORTANT : Ne pas inclure de renseignements personnels identificatoires.



Si possible, veuillez fournir une copie de l'avis (ou le scénario de l'avis) et veuillez confirmer que l'avis est conforme aux exigences prévues dans le [Règlement](#).

Si vous avez choisi d'aviser indirectement les intéressés, veuillez décrire la raison pour ce faire, ainsi que le type d'avis indirect utilisé (c.-à-d. par quel moyen il a été livré à un public cible):

Atténuation des risques

* Les mesures que l'organisation a prises (autres que la notification des intéressés) afin de réduire le risque de préjudice à l'endroit des intéressés, ou afin d'atténuer un tel préjudice :

Par exemple, ceci peut comprendre ce qui suit :

- prendre des mesures comme réinitialiser les mots de passe, offrir des services de surveillance du crédit le cas échéant, récupérer les renseignements envoyés à un mauvais destinataire, obtenir la confirmation des personnes auxquelles les renseignements n'étaient pas destinés qu'elles ont détruits ces renseignements et qu'elles ne les ont pas diffusés;
- aviser les tierces parties ou les organisations qui peuvent réduire le risque de préjudice, comme la police, les centres de traitement des paiements ou les sociétés émettrices de cartes de crédit.



Description de toute autre organisation ou institution gouvernementale avisée de l'atteinte et non mentionnée ci-dessus (par exemple, ordres professionnels ou autres commissariats à la protection de la vie privée) :

Nom de l'organisation :

Date de l'avis :

Description des mesures qui ont été prises afin de réduire le risque qu'un événement similaire se produise à l'avenir :

Par exemple :

- un cabinet expert en TI a été embauché afin d'examiner le programme de sécurité d'une organisation et celle-ci s'est engagée à apporter toute amélioration recommandée;
- tous les nouveaux contrats conclus avec des fournisseurs de service Web comprendront les dispositions de contrôle de la qualité suivantes . . . ;
- un module de formation sur la protection des renseignements personnels a été élaboré et est maintenant obligatoire pour tout le personnel;
- tous les ordinateurs portables seront cryptés;
- le protocole de gestion des modifications du logiciel a été mis à jour; etc.



Veillez soumettre le présent formulaire par l'un des moyens suivants :

Par l'entremise du portail de déclaration sécurisé :

[Soumettre une déclaration d'atteinte à la vie privée](#)
(Nous invitons tous les organisations à nous soumettre leur rapport par l'entremise du portail sécurisé de soumission de déclarations d'atteinte.)

Par la poste ou en personne :

Agent de réponse en matière d'atteinte à la LPRPDE
Commissariat à la protection de la vie privée du
Canada
30, rue Victoria, 1^{er} étage
Gatineau, QC K1A 1H3

Si vous souhaitez obtenir des renseignements supplémentaires sur les exigences en matière de déclaration aux termes de la LPRPDE, veuillez consulter le document d'orientation du Commissariat intitulé : [Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité](#).



ANNEXE E

AVIS AU COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA

CONCERNANT UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS
PERSONNELS ET QUI PRÉSENTE UN RISQUE DE PRÉJUDICE SÉRIEUX

[Page suivante]

AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION

CONCERNANT UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS ET QUI PRÉSENTE UN RISQUE DE PRÉJUDICE SÉRIEX

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
Loi sur la protection des renseignements personnels dans le secteur privé

Objet du présent formulaire

Ce formulaire vise à permettre aux organisations¹ d'aviser la Commission d'accès à l'information (la Commission) de tout incident de confidentialité impliquant un renseignement personnel qu'elles détiennent et présentant un risque de préjudice sérieux.

On entend par « incident de confidentialité » :

- l'accès non autorisé par la loi à un renseignement personnel;
- l'utilisation non autorisée par la loi d'un renseignement personnel;
- la communication non autorisée par la loi d'un renseignement personnel;
- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Assurez-vous de ne pas transmettre de renseignements personnels permettant d'identifier une personne dans ce formulaire et dans tout autre document que vous transmettez à la Commission.

Si vous manquez d'espace dans l'un des champs, joignez une annexe présentant l'ensemble de votre réponse lorsque vous transmettez le formulaire à la Commission et inscrivez « Voir annexe » dans le champ concerné.

Vous pouvez transmettre le formulaire et les documents joints par courrier électronique, par la poste ou par télécopieur aux coordonnées suivantes :

Commission d'accès à l'information

525, boulevard René-Lévesque Est, Bur. 2.36

Québec (Qc) G1R 5S9

Téléphone : 418 528-7741 – Sans frais : 1 888 528-7741 – Télécopieur : 418 529-3102

Courrier électronique : cai.communications@cai.gouv.qc.ca

¹ On entend par « organisation » : organisme public, personne qui exploite une entreprise, ordre professionnel, parti politique, député indépendant ou candidat indépendant, syndicat, association, organisme à buts non lucratifs, travailleur autonome et pigiste.

Obligations de l'organisation

- ✓ Évaluer si un incident de confidentialité représente un risque qu'un préjudice sérieux² soit causé aux personnes concernées par l'incident de confidentialité;
- ✓ Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que d'autres incidents de même nature se produisent. Le fait de déclarer un incident de confidentialité à la Commission ne dispense pas une organisation de cette obligation;
- ✓ Aviser toute personne dont un renseignement personnel a été compromis par un incident de confidentialité si cet incident présente un risque qu'un préjudice sérieux soit causé. En cas de défaut, la Commission pourrait ordonner de le faire;
- ✓ Aviser la Commission, avec diligence, d'un incident de confidentialité impliquant un renseignement personnel qu'elle détient lorsque l'incident présente un risque qu'un préjudice sérieux soit causé aux personnes concernées;
- ✓ Transmettre à la Commission, dans les meilleurs délais, tout renseignement complémentaire dont elle prend connaissance après lui avoir transmis le présent avis;
- ✓ Inscrire l'incident déclaré dans son registre des incidents de confidentialité et communiquer ce dernier à la Commission sur demande.

Vous pouvez obtenir plus de renseignements au sujet de vos obligations en matière d'incident de confidentialité impliquant des renseignements personnels sur notre site Web à l'adresse <https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/>

Rôle de la Commission au regard des incidents de confidentialité

- La Commission s'assure que l'organisation respecte ses obligations légales lors d'un incident de confidentialité et qu'elle met en place les mesures nécessaires pour éviter que de nouveaux incidents de même nature ne se produisent.
- La Commission n'accompagne pas l'organisation dans la gestion des incidents de confidentialité.
- La Commission ne procède pas à la validation des mesures prises par l'organisation pour diminuer les risques qu'un préjudice soit causé ou pour éviter que de nouveaux incidents de même nature se produisent.
- Le fait d'aviser la Commission d'un incident de confidentialité ne peut servir à établir la conformité des pratiques d'une organisation à l'égard de ses obligations légales.

² Le préjudice sérieux n'a pas à s'être matérialisé. Il peut seulement être susceptible de se produire.



1. Identification de l'organisation concernée par l'incident de confidentialité (Veuillez remplir la section A pour un organisme public et la section B pour une entreprise)

A. Identification de l'organisme public

Nom :

Adresse :

Personne à contacter relativement à l'incident

Nom :

Fonction :

Téléphone :

Courriel :

Personne responsable de la protection des renseignements personnels

Même que précédent

Nom :

Fonction :

Téléphone :

Courriel :

B. Identification de l'entreprise

Nom :

Adresse du siège social :

Numéro d'entreprise au Québec (selon le Registraire du Québec) :

Dirigeant principal

Nom :

Titre / fonction :

Téléphone :

Courriel :

Personne à contacter relativement à l'incident

Même que précédent

Nom :

Fonction :

Téléphone :

Courriel :

Personne responsable de la protection des renseignements personnels

Même que précédent

Nom :

Fonction :

Téléphone :

Courriel :

2. Date et période de l'incident de confidentialité

Date de l'incident :

Date de découverte de l'incident :

L'incident a eu lieu sur une période de :

3. Type d'incident de confidentialité

Accès non autorisé par la loi à un renseignement personnel

Utilisation non autorisée par la loi d'un renseignement personnel

Communication non autorisée par la loi d'un renseignement personnel

Perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement

3.1 Causes et circonstances de l'incident de confidentialité

Selon le type d'incident sélectionné ci-dessus, identifiez la ou les cause(s) de celui-ci :

Altération délibérée	Communication accidentelle	Communication délibérée sans autorisation	Consultation non autorisée
Cyberattaque (virus, logiciel espion, etc.)	Défaillance technique	Destruction accidentelle	Destruction volontaire sans autorisation
Divulgence accidentelle	Divulgence délibérée sans autorisation	Erreur humaine	Hameçonnage (phishing)
Ingénierie sociale	Perte d'accès aux renseignements	Perte de renseignements	Rançongiciel
Utilisation incompatible	Vol de renseignements	Autre Précisez :	

Selon le type d'incident sélectionné ci-dessus, décrivez les circonstances de celui-ci :

Sur quel(s) support(s) les renseignements personnels étaient-ils conservés au moment de l'incident :

Ordinateur de bureau	Dispositif amovible électronique
Papier	Clé USB
Serveur	CD
Bande sonore	Téléphone portable
Infonuagique (cloud)	Tablette
Vidéosurveillance	Ordinateur portable
Photo	Autre Précisez :

4. Description des renseignements personnels visés par l'incident de confidentialité

Nom Prénom	Adresse du domicile	Date de naissance ou Année Mois Jour Âge
Numéro de téléphone au domicile	Numéro du cellulaire	Adresse courriel personnelle
Numéro de permis de conduire	Numéro d'assurance sociale	
Numéro d'assurance maladie	Numéro de passeport	
Salaire	Fonction / occupation	
Renseignements sur des employés, clients ou bénéficiaires Précisez :		
Renseignements médicaux Précisez :		
Renseignements génétiques Précisez :		
Renseignements scolaires / académiques Précisez :		
Renseignements bancaires / numéro de compte / institution / placements / hypothèque Précisez :		



Numéro de carte de crédit	Numéro d'identification personnel (NIP)	Nom du détenteur	Code de sécurité à trois chiffres
Numéro de carte de débit	Numéro d'identification personnel (NIP)	Nom du détenteur	

Autres renseignements personnels

Précisez :

Impossible de fournir une description des renseignements personnels visés

Expliquez :

5. Personnes concernées par l'incident de confidentialité

Nombre de personnes concernées par l'incident :

Nombre de personnes concernées par l'incident qui résident au Québec :

Si possible, ventilez le nombre de personnes concernées par l'incident selon leur lien avec l'organisation, qu'il s'agisse d'employés, de clients, d'étudiants, de patients, de membres, de bénévoles, de fournisseurs, etc., actuels ou anciens :

6. Évaluation par l'organisation du fait qu'un risque de préjudice sérieux puisse être causé aux personnes concernées par l'incident de confidentialité

Décrivez les éléments amenant l'organisation à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées. Ce risque peut être attribuable au fait qu'il s'agisse de renseignements personnels sensibles ou à la possibilité que ces renseignements soient utilisés à des fins malveillantes ou préjudiciables. Dans ce cas, indiquez les conséquences appréhendées de leur utilisation sur les personnes concernées.



Décrivez les raisons qui supportent l'existence d'un risque de préjudice sérieux pour les personnes concernées par l'incident.

Le responsable de la protection des renseignements personnels de votre organisation a-t-il été consulté pour procéder à l'évaluation du risque de préjudice?

Oui Non

7. Avis de l'organisation aux personnes concernées (Vous pouvez joindre une copie de l'avis transmis aux personnes concernées)

L'organisation a-t-elle avisé les personnes concernées par l'incident de confidentialité?

Non

Oui. L'avis a été fait par :

Lettre transmise par courrier	Courriel	Message texte
Verbal (ex. par téléphone)	En personne	Autre Précisez :

Date de l'avis :

Si les personnes concernées n'ont pas encore été avisées, quelles mesures seront prises par l'organisation afin de le faire?

Lettre transmise par courrier	Courriel	Message texte
Verbal (ex. par téléphone)	En personne	Autre Précisez :

Date de l'avis prévu :

Aucune notification de l'incident aux personnes concernées n'est prévue.

Expliquez :

7.1 Contenu de l'avis aux personnes concernées

Sélectionnez les éléments contenus dans l'avis transmis aux personnes concernées par l'organisation.

Une description des renseignements personnels visés par l'incident

Une brève description des circonstances de l'incident

La date ou la période où l'incident a eu lieu

Une brève description des mesures que l'organisation a prises ou entend prendre, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé

Les mesures que l'organisation suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice

Les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident

Y a-t-il des personnes concernées par l'incident qui ne seront pas avisées par l'organisation?

Non.

Oui. Combien :

Expliquez :

7.2 Avis public aux personnes concernées

L'avis aux personnes concernées a-t-il été fait, exceptionnellement, au moyen d'un avis public?

Non

Oui. Sélectionnez la raison applicable :

Le fait de transmettre l'avis est susceptible de causer un préjudice accru à la personne concernée.
Expliquez :

Le fait de transmettre l'avis est susceptible présenter une difficulté excessive pour l'organisation.
Expliquez :

L'organisation n'a pas les coordonnées des personnes concernées.
Expliquez :



Par quels moyens l'avis public a-t-il été fait?

Un avis dans les médias

Précisez lesquels :

Date de diffusion :

Un communiqué de presse

Date de diffusion :

Un avis sur le site Web de l'organisation

Une conférence de presse

Lieu :

Date :

Une publication diffusée dans les médias sociaux

Précisez lesquels :

Autre

Précisez :

Est-ce que l'organisation a avisé d'autres autorités de protection des renseignements personnels à l'extérieur du Québec?

Commissaire à la protection de la vie privée du Canada

Office of the information and privacy commissioner of Alberta

Office of the information and privacy commissioner of British Columbia

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Autre.

Précisez :



8. Obligation de diminuer le risque de préjudice

Quelles mesures ont été prise dès la découverte de l'incident, notamment afin de réduire les risques de préjudice aux personnes concernées?

Dans quel délai ces mesures ont-elles été prises?

Est-ce que des mesures ont été prises après la découverte de l'incident afin d'éviter que de nouveaux incidents de même nature se reproduisent?

Non

Oui. Précisez :

Y a-t-il des mesures prévues qui n'ont pas encore été prises?

Non

Oui. Précisez :

Indiquez la date de mise en place des mesures prévues :

Une organisation doit transmettre à la Commission tout renseignement relatif à l'incident de confidentialité dont elle prend connaissance après lui avoir transmis le présent avis. L'information complémentaire doit alors être transmise dans les meilleurs délais à compter de cette connaissance.

Est-ce que des informations supplémentaires seront transmises à la Commission concernant l'incident rapporté?

Non

Oui. Précisez lesquelles et indiquez l'échéancier prévu :



9. Signature

Prénom :

Nom :

Fonction :

Lieu / Ville :

Date de transmission du formulaire à la Commission :

Pour le compte de : l'organisme l'entreprise

Je déclare que les renseignements concernant l'incident de confidentialité fournis dans la présente déclaration sont complets et conformes aux faits.

Signature :