Politique de confidentialité

RÉZO respecte le droit à la vie privée de chaque individu et s'engage à protéger la confidentialité des renseignements personnels recueillis auprès de tout.e Participant.e ou Employé.e. En règle générale, les renseignements personnels sont accessibles seulement aux personnes qui doivent y avoir accès dans l'exercice de leurs fonctions au sein de RÉZO.

1. DÉFINITIONS

« Employé.e »
Toute personne qui travaille pour RÉZO moyennant rémunération, incluant la personne occupant le rôle de directeur général (DG) ainsi que toutes personnes non rémunérées (bénévole, stagiaire).

« Événement »
Tout événement que RÉZO gère ou organise.

« Formulaire de signalement »
Le formulaire mis à la disposition de tout.e Employé.e ou Participant.e afin d'informer la personne responsable d'un incident de confidentialité.

« Incident de confidentialité impliquant un renseignement personnel »
Tout accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

«Risque de préjudice sérieux»
Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut conduire, par exemple : À l'humiliation; À une atteinte à la réputation; À une perte financière; À un vol d'identité; À des conséquences négatives sur un dossier de crédit; À une perte d'emploi.

« Participant.e »
Tout individu qui fournit des renseignements confidentiels à RÉZO ou consent à la cueillette de tels renseignements auprès d'un tiers par RÉZO en lien avec la réalisation d'un Évènement, la création d'une Publication, ou avec l'obtention d'un Service.

« Personne responsable »

La personne responsable de la protection des renseignements personnels désignée par RÉZO pour la protection des renseignements personnels. Le titre et les coordonnées de la personne responsable sont publiés sur le site Internet de l'entreprise; La personne

La personne ayant la plus haute autorité dans l'entreprise, par exemple son dirigeant, est par défaut responsable de la protection des renseignements personnels. Cette fonction peut cependant être déléguée par écrit, en tout ou en partie, à une personne en mesure d'assumer efficacement ce rôle. Dans ce cas, la Commission recommande de désigner une personne ayant les compétences requises et un pouvoir décisionnel important.

« Publication »

Toute publication produite par RÉZO ou à laquelle RÉZO contribue, sous quelque forme que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre).

« Anonymisation»

un renseignement concernant une personne physique est anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.

« Registre des incidents de confidentialité »

L'ensemble des renseignements consignés sur des incidents déclarés et concernant les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises en réaction à l'incident. Les dates pertinentes y figurent aussi : survenance de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.

« Risque sérieux de préjudices »

Le risque évalué à la suite d'un incident de confidentialité qui pourrait porter préjudice aux personnes concernées. Ce risque est analysé par la personne responsable. Pour tout incident de confidentialité, la personne responsable évalue la gravité du risque de préjudice pour les personnes concernées en estimant « la sensibilité des renseignements concernés », « les conséquences appréhendées de leur utilisation » et « la probabilité qu'ils soient utilisés à des fins préjudiciables ».

« Renseignement personnel »

Tout renseignement fourni ou communiqué à RÉZO sous quelque support que ce soit (verbal, écrit, audio, vidéo, informatisé ou autre) qui concerne un.e Participant.e ou un.e Employé.e et qui peut être utilisé pour l'identifier directement ou indirectement comme le définit les modifications de l'article 2 de la loi, y compris : son nom, son numéro de téléphone, son adresse, son courriel, le fait qu'il ou elle ait été ou soit un.e Participant.e ou un.e Participant.e potentiel.le, son genre, son orientation sexuelle et toute information concernant sa santé (incluant son statut sérologique). Pour plus de certitude :

- les renseignements qui ne permettent pas d'identifier un individu dans le cadre d'un témoignage ne sont pas des renseignements confidentiels ;
- les données statistiques ne sont pas des renseignements confidentiels puisqu'elles ne permettent

pas d'identifier un individu ;
- les photographies ou enregistrements qui ne permettent pas d'identifier un individu ne constituent pas un renseignement personnel relatif à cet individu.

« Service »
Tout service que RÉZO rend à un individu à la demande de celui-ci.

2. PHOTOGRAPHIES ET ENREGISTREMENTS

2.1
Tout individu a le choix d'être photographié ou non, ou d'être enregistré (audio/vidéo) ou non.

2.2
Les photographies ou enregistrements qui permettent d'identifier un individu comme Employ.é de RÉZO ne constituent pas un renseignement confidentiel relatif à cet individu.

3. OBLIGATION DE CONFIDENTIALITÉ

3.1
Les Employé.es, le conseil d'administration et les mandataires de RÉZO sont tenu.es de signer la présente entente de confidentialité (Annexe A) avant d'exercer leurs fonctions ou d'exécuter leurs mandats auprès de RÉZO.

3.2
L'obligation de confidentialité s'applique à la durée de la relation d'un.e Employé.e avec RÉZO et survit à la fin de cette relation.

4. COLLECTE ET USAGE DES RENSEIGNEMENTS PERSONNELS

4.1
RÉZO peut, au besoin et en raison d'un intérêt sérieux et légitime comme le mentionne l'article 1.1 de la loi., constituer un ou des dossiers contenant des renseignements confidentiels concernant les Employées. La constitution de tels dossiers a pour objet de :
- Maintenir les coordonnées à jour ;
- Documenter l'expérience de travail ou de bénévolat ;
- Permettre, dans le cas des Employé.es rémunéré.es, la réalisation des tâches administratives requises ou permises par la loi (impôt sur le revenu, assurances collectives, etc.).

4.2
RÉZO peut, au besoin et en raison d'un intérêt sérieux et légitime comme le mentionne l'article 1.1 de la loi, constituer un ou des dossiers contenant des renseignements personnels concernant les Participant.es. Rézo ne collecte que les renseignements nécessaires aux fins déterminées avant la collecte. La constitution de tels dossiers a pour objet de permettre à RÉZO de réaliser un Événement, une Publication, ou de fournir un Service.

4.3
RÉZO peut seulement recueillir les renseignements confidentiels qui sont nécessaires aux fins du

dossier et peut utiliser les renseignements confidentiels seulement à ces fins.

4.4

Les renseignements personnels peuvent seulement être recueillis auprès de la personne concernée, à moins que celle-ci consente à ce que la cueillette soit réalisée auprès d'autrui ou que la loi l'autorise.

5. GESTION DES RENSEIGNEMENTS PERSONNELS

5.1

La personne occupant le rôle de directeur général, comme personne exerçant la plus haute autorité dans l'organisation, est la personne responsable d'assurer la protection des renseignements personnels. La personne occupant le rôle de directeur général peut déléguer cette responsabilité en la constatant par écrit. Sur le principal site web de RÉZO, le nom de la personne responsable est partagé, ainsi que le titre « personne responsable de la protection des renseignements personnels » ainsi que le moyen de la joindre.

La personne responsable de la protection des renseignements personnels s'assure de la tenue d'un Registre des incidents de confidentialité.

5.2

Sous réserve de l'article 5.3, la personne occupant le rôle de directeur général est autorisée à accéder à tout renseignement confidentiel que détient RÉZO. Les autres Employé.es sont autorisé.es à accéder aux renseignements confidentiels dans la mesure où cet accès est nécessaire à la réalisation d'une tâche dans l'exercice de leurs fonctions.

5.3

Pour l'application de la Loi sur la protection des renseignements personnels dans le secteur privé, un **incident de confidentialité** correspond à tout accès, utilisation ou communication non autorisé.es par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

5.4

Lorsqu'un.e Employé.e ou un.e Participant.e constate un incident de confidentialité, il ou elle doit informer avec diligence la personne responsable de la protection des renseignements personnels afin qu'il soit inscrit au Registre des incidents de confidentialité. L'employé.e ou le ou la Participant.e doit, pour ce faire, compléter un formulaire de signalement, qui est automatiquement acheminé à la personne responsable de la protection des renseignements personnels.

Le registre doit conserver les informations sur un incident de confidentialité pour une période de cinq ans.

Doit être colligé dans le formulaire de signalement :

- Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description ;
- Une brève description des circonstances de l'incident ;
- La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;
- La date ou la période à laquelle l'organisation s'est aperçue de l'incident ;

- Le nombre de personnes concernées par l'incident (ou une approximation si cette information n'est pas connue).

5.5

La personne responsable de la protection des renseignements personnels consulte les membres de la direction ou du conseil d'administration disponibles afin de juger si l'incident présente un « risque de préjudice sérieux » comme le mentionne l'article 3.5. de la Loi. et des mesures à prendre afin de diminuer ce risque et d'éviter que de nouveaux incidents de même nature ne se produisent. Les incidents de confidentialité qui représentent un risque de préjudice sérieux sont versés au registre des incidents de confidentialité.

La personne responsable de la protection des renseignements personnels, décide selon le degré du risque de préjudice d'aviser la Commission d'accès à l'information et les personnes concernées de tout incident présentant un risque de préjudice sérieux.

6. CONSERVATION DES RENSEIGNEMENTS PERSONNELS

6.1

Les Employé.es ayant accès aux dossiers en vertu de l'article 5 de la présente politique s'obligent à :

- S'assurer que les renseignements personnels soient gardés à l'abri de tout dommage physique, de tout accès, utilisation, ou communication non autorisé par la loi et par la présente politique ;
- S'assurer que tous les documents électroniques comportant des renseignements personnels , incluant ceux copiés sur un appareil de stockage portatif, soient cryptés et protégés par des mots de passe. Ces mots de passe doivent être modifiés deux fois par année, ainsi qu'à chaque fois que les personnes ayant accès aux dossiers concernés sont remplacées ;
- Garder les renseignements confidentiels en format papier dans des classeurs pouvant être verrouillés et s'assurer que les classeurs soient verrouillés à la fin de chaque journée de travail. Les clés des classeurs doivent être gardées dans des endroits sûrs.

6.2

Lorsqu'un.e Employé.e peut également, à certains égards, être qualifié.e de Participant.e, les renseignements personnels concernant chaque catégorie seront conservés séparément.

6.3

Les dossiers constitués en vertu de cette politique sont la propriété de RÉZO.

7. DESTRUCTION OU ANONYMISATION DES RENSEIGNEMENTS PERSONNELS

7.1

Sous réserve de l'article 7.2, les renseignements confidentiels ne sont conservés que tant et aussi longtemps que l'objet pour lequel ils ont été recueillis n'a pas été accompli, à moins que l'individu concerné ait consenti à ce qu'il en soit autrement. Ces renseignements confidentiels sont ensuite détruits de façon à ce que les données y figurant ne puissent plus être reconstituées.

7.2
Les dossiers concernant les Employé.es sont conservés par RÉZO.

7.3

Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, RÉZO se garde la discrétion détruire ou d'anonymiser les renseignements personnels pour les utiliser à des fins sérieuses et légitimes, sous réserve des délais de conservation prévu par la loi.

7.4
Pour plus de certitude, les renseignements personnels concernant un individu ayant offert un témoignage, tels que son nom et ses coordonnées, sont détruits une fois le témoignage publié ou diffusé, à moins que l'individu ait préalablement consenti à ce que les renseignements personnels le concernant soient conservés pour permettre à RÉZO de le recontacter dans le futur. Pour plus de certitude, chaque utilisation du témoignage d'une personne doit être approuvée par la personne elle-même.

8. COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À UN TIERS

8.1
Autre que dans les situations où la loi le requiert et sous réserve des autres dispositions du présent article 8, les renseignements personnels ne peuvent être communiqué qu'après l'obtention du consentement écrit, manifeste, libre et éclairé de la personne concernée. Un tel consentement ne peut être donné que pour une fin spécifique et pour la durée nécessaire à la réalisation de cette dernière.

8.2
Les renseignements personnels peuvent être communiqués sans le consentement de la personne concernée si la vie, la santé ou la sécurité de celle-ci est gravement menacée. La communication doit alors être effectuée de la façon la moins préjudiciable pour la personne concernée.

8.3
Tel que permis par la loi, RÉZO peut communiquer des renseignements personnels nécessaires à sa défense ou celle de ses Employé.es contre toute réclamation ou poursuite intentée contre RÉZO ou ses Employé.es, par ou de la part d'un.e Participant.e, d'un.e Employé.e, ou de l'une de ses personnes héritières, exécutrices testamentaires, ayants droit ou cessionnaires, y compris toute réclamation émanant de l'assureur d'un.e Participant.e ou d'un.e Employé.e.

9. COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À LA PERSONNE CONCERNÉE

9.1
Sous réserve de l'article 9.2, les Participant.es et Employé.es ont le droit de connaître les renseignements personnels que RÉZO a reçus, recueillis et conserve à leur sujet, d'avoir accès à de tels renseignements et de demander que des rectifications soient apportées à ceux-ci.

Une demande d'accès ou de rectification à ces renseignements personnels ne peut être considérée que

si elle est faite par écrit par une personne justifiant de son identité à titre de personne concernée, de représentant, d'héritier, de successible de cette dernière, de liquidateur de la succession, de bénéficiaire d'assurance-vie ou d'indemnité de décès, de titulaire de l'autorité parentale même si l'enfant mineur est décédé ou à titre de conjoint ou de proche parent d'une personne décédée suivant l'article 40.1. de la Loi sur la protection des renseignements personnels dans le secteur privé.

Une telle demande est adressée au responsable de la protection des renseignements personnels. Lorsque la demande n'est pas suffisamment précise ou lorsqu'une personne le requiert, le responsable prête assistance pour identifier les renseignements recherchés.

9.2

RÉZO doit restreindre l'accès aux renseignements personnels lorsque la loi le requiert ou lorsque la divulgation révélerait vraisemblablement des renseignements personnels au sujet d'un tiers.

Le présent article ne restreint pas la communication à une personne d'un renseignement personnel la concernant ou sa rectification résultant de la prestation d'un service à lui rendre.

9.3

Une demande d'un.e Participant.e ou d'un.e Employé.e en lien avec l'article 9.1 doit être traitée dans un délai maximal de 30 jours.

9.4

L'accès aux renseignements personnels est gratuit. Toutefois, des frais raisonnables peuvent être exigés du requérant pour la transcription, la reproduction ou la transmission de ces renseignements.

10. MANQUEMENT AUX OBLIGATIONS DE LA PRÉSENTE POLITIQUE

10.1

Un.e Employé.e manque aux obligations de la présente politique lorsque cette personne :

- communique des renseignements personnels à des individus n'étant pas autorisés à y avoir accès ;
- discute de renseignements personnels et à l'intérieur ou à l'extérieur de RÉZO alors que des individus n'étant pas autorisés à y avoir accès sont susceptibles de les entendre ;
- laisse des renseignements personnels sur support papier ou informatique à la vue dans un endroit où des individus n'étant pas autorisés à y avoir accès sont susceptibles de les voir ;
- fait défaut de suivre les dispositions de cette politique et des dispositions de la loi.

10.2

Advenant un manquement aux obligations de la présente politique ou à toute disposition de la loi sur la protection des renseignements personnels dans le secteur privé , des mesures disciplinaires appropriées, pouvant aller jusqu'à la résiliation du contrat de travail ou de toute autre relation avec RÉZO, seront prises à l'égard de la partie contrevenante et des mesures correctives seront adoptées au besoin afin de prévenir qu'un tel scénario ne se reproduise.

11. RECOURS

11.1

S'il s'avère que les renseignements personnels d'une personne ont été utilisés de façon contraire à une disposition de cette politique ou de la loi, cette personne peut déposer une plainte auprès de la direction générale de RÉZO ou auprès du comité exécutif du conseil d'administration de RÉZO si la plainte concerne la direction générale.

11.2

Comme prévu par la loi, la personne dont la plainte concerne une demande d'accès ou de rectification des renseignements confidentiels la concernant peut déposer sa plainte auprès de la Commission d'accès à l'information pour l'examen du désaccord dans les 30 jours du refus de RÉZO d'accéder à sa demande ou de l'expiration du délai pour y répondre.

Adoptée par le Conseil d'administration de RÉZO le 22 septembre, 2023

DÉCLARATION RELATIVE À LA CONFIDENTIALITÉ

Je, soussigné.e, déclare avoir lu la Politique de confidentialité de RÉZO et m'engage à en respecter les termes. Je reconnais et accepte que mon obligation de confidentialité survit à la fin de mon emploi, stage ou bénévolat auprès de RÉZO.

Signé à Montréal le :

Nom en lettres moulées :

Signature :

INCIDENT DE CONFIDENTIALITÉ
PLAN DE RÉPONSE

Démarches à effectuer

Lorsqu'un.e Employé.e ou Participant.e constate un incident de confidentialité, il ou elle communique avec la personne responsable de la protection des renseignements personnels (responsable) par le biais d'un formulaire de signalement prévu à cette fin.

La personne responsable identifie les mesures raisonnables pour réduire le risque de préjudice et pour prévenir de nouveaux incidents.

La personne responsable évalue si l'incident présente un risque de préjudice sérieux?

Dans le cas où l'incident présente un risque de préjudice sérieux, la personne responsable prévient sans délai la Commission d'accès à l'information (CAI) via le formulaire prévu à cette fin et toute personne dont les renseignements personnels sont affectés.

La personne responsable tient un registre de tous les incidents.

La personne responsable répond à la demande de la CAI d'avoir une copie du registre, le cas échéant.

INCIDENT DE CONFIDENTIALITÉ
CONTENU DE LA COMMUNICATION AUX PERSONNES CONCERNÉES

Quand

Le **Règlement sur les incidents de confidentialité** stipule aussi qu'un organisme doit aviser « avec diligence » toutes les personnes dont les renseignements personnels ont été touchés par un incident de confidentialité qui serait susceptible de leur causer un préjudice sérieux. Elle peut également aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée. Cet avis doit être envoyé directement aux personnes concernées, à moins qu'un tel avis ne leur cause un préjudice additionnel ou ne nuise à l'organisme et/ou si l'organisme ne possède pas les coordonnées de la personne. Le cas échéant, l'organisme peut aviser les personnes concernées au moyen d'un avis public.

Une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

Contenu

Comme c'est le cas pour l'avis écrit à la CAI, l'avis écrit aux personnes concernées doit contenir les éléments suivants :

- Le nom de RÉZO dont le numéro d'entreprise est le 1140493876
- Une description des renseignements personnels touchés par l'incident ou, si cette information est inconnue, les raisons pour lesquelles il est impossible de fournir une telle description ;
- Une brève description des circonstances de l'incident et, si elle est connue, sa cause;
- La date ou la période à laquelle a eu lieu l'incident (ou une approximation si cette information n'est pas connue) ;
- Une brève description des mesures que l'organisme a prises ou entend prendre suite à l'incident dans le but de réduire les risques de préjudice ;
- Les mesures que l'organisme suggère à la personne concernée de prendre dans le but de réduire/atténuer les risques de préjudice ;
- Les coordonnées de la personne auprès de laquelle la personne concernée peut obtenir de plus amples renseignements à propos de l'incident.

INCIDENT DE CONFIDENTIALITÉ
QUESTIONNAIRE D'ÉVALUATION DU
« RISQUE SÉRIEUX DE PRÉJUDICE GRAVE »

Évaluer si l'incident présente un risque de préjudice sérieux[1]

Pour tout incident de confidentialité, l'organisation doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, notamment :

1. Quelle est la **sensibilité** des renseignements concernés ?
2. Quelles sont les **conséquences appréhendées** de leur utilisation ?
3. Quelle est la probabilité qu'ils soient utilisés à des **fins préjudiciables ?**

1. Renseignements sensibles

- Documents financiers ;
- Dossiers médicaux ;
- Les renseignements personnels que l'on communique de manière courante ne sont généralement pas considérés comme sensibles (nom, adresse) ;
    - Sauf si le contexte en fait des renseignements sensibles : nom, adresses associé.es à des périodiques spécialisés ou à des activités qui les identifient.

2. Préjudice grave

- Humiliation ;
- Dommage à la réputation ou aux relations ;
- Perte de possibilité d'emploi ou d'occasion d'affaires ou d'activités professionnelles ;
- Perte financière ;
- Vol d'identité ;
- Effet négatif sur le dossier de crédit ;
- Dommage aux biens ou leur perte ;

3. Pour déterminer la probabilité d'un mauvais usage

- Qu'est-il arrivé et quels sont les risques qu'une personne subisse un préjudice en raison de l'atteinte ?
- Qui a eu accès aux renseignements personnels ou aurait pu y avoir accès ?
- Combien de temps les renseignements personnels ont-ils été exposés ?
- A-t-on constaté un mauvais usage des renseignements ?

- L’intention malveillante a-t-elle été démontrée (vol, piratage) ?
- Les renseignements ont-ils été exposés à des entités ou à des personnes susceptibles de les utiliser pour causer un préjudice ou qui représentent un risque pour la réputation de la ou des personnes touchées ?

Si l’analyse fait ressortir un risque de préjudice sérieux, l’organisation doit aviser la Commission et les personnes concernées de l’incident. Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu’un incident de même nature se produise à nouveau.

[1] Le questionnaire respecte le **Règlement sur les incidents de confidentialité**