Politique de confidentialité et de protection des données personnelles
Adoptée par le conseil d'administration le : 27 décembre 2024, Montréal

Table des matières

Introduction

Protéger la vie privée et assurer la confidentialité des données personnelles est une priorité pour l'ICRC. Nous nous engageons à protéger la vie privée de toutes les personnes qui nous confient des renseignements personnels et à respecter leurs droits en matière de protection des données. L'ICRC prend cette responsabilité au sérieux, gagnant la confiance de ceux que nous servons en respectant des normes professionnelles et éthiques élevées. La transparence, l'honnêteté et la responsabilité sont au cœur de notre travail, garantissant que nous méritons et maintenons constamment cette confiance.

Dans cet esprit, l'ICRC a élaboré la **Politique de confidentialité et de protection des données personnelles**, qui décrit les principes et les procédures que notre organisation suit pour garantir la confidentialité et la sécurité des données que nous collectons, utilisons et conservons. Cette politique s'appuie sur les meilleures pratiques en matière de protection des données, les réglementations canadiennes et internationales, ainsi que notre engagement envers l'éthique et la transparence.

La politique décrit les types de renseignements personnels collectés par l'ICRC, leur utilisation, les circonstances dans lesquelles ils peuvent être divulgués à des tiers et les mesures de sécurité prises pour les protéger. Nous vous encourageons à lire attentivement cette politique pour comprendre comment nous protégeons les renseignements personnels et pour adhérer à ces principes et procédures dans votre travail.

Il est important de noter que cette politique est également conforme à la **Loi 25 (2024)**, qui établit des exigences supplémentaires en matière de protection des données personnelles. Le CCBI veille au respect de toutes les dispositions de cette loi pour offrir le plus haut niveau de protection aux données personnelles qu'il traite.

N'hésitez pas à contacter la direction si vous avez des questions ou des préoccupations concernant cette politique ou son application à votre travail.

Responsable désigné.e de la protection des données

La gestion de l'ICRC assume la responsabilité de la protection et de la confidentialité des données au sein de l'organisation. En tant que responsable désigné.e de la protection des données, la direction supervise la mise en œuvre et la conformité aux politiques, procédures et principes liés à la confidentialité et à la sécurité des renseignements personnels. La direction est également responsable de répondre aux questions, préoccupations et demandes des membres de l'organisation et des personnes concernées concernant la protection des données.

Principes

1. **Responsabilité** : Chaque membre de l'organisation est responsable de protéger les renseignements personnels qu'iel traite en respectant cette politique de confidentialité et en suivant les directives de la direction.
2. **Minimisation des données** : Les renseignements personnels doivent être collectés uniquement dans la mesure nécessaire à l'exécution des responsabilités et conformément aux finalités identifiées.
3. **Non-divulgation** : Les renseignements personnels ne doivent pas être divulgués à des tiers non autorisés, qu'iels soient internes ou externes à l'organisation, sans le consentement explicite de la personne concernée ou une autorisation préalable de la direction.
4. **Confidentialité** : Les dossiers internes et les informations sensibles ne doivent pas être discutés avec des personnes non autorisées afin de préserver la vie privée et la confidentialité des personnes concernées.
5. **Sécurité des données** : Des mesures de sécurité appropriées doivent être mises en place pour protéger les renseignements personnels contre tout accès, divulgation, altération ou destruction non autorisés.
6. **Notification** : Toute atteinte à la confidentialité ou situation pouvant compromettre la sécurité des renseignements personnels doit être signalée immédiatement à la direction.
7. **Respect des droits** : Les droits des individu.e.s concernant leur vie privée, y compris l'accès, la correction et la suppression des renseignements personnels, doivent être respectés conformément à la politique de confidentialité de l'organisation.

Collecte et utilisation des renseignements personnels

Notre entreprise sociale collecte uniquement les informations personnelles nécessaires pour atteindre ses objectifs commerciaux et sociaux, tels que la préparation des déclarations fiscales, la distribution de fonds, l'évaluation du développement et de l'impact des programmes, le traitement des T4A et la gestion des partenariats. Les informations personnelles collectées peuvent inclure, sans s'y limiter :

- Nom légal complet
- Adresse postale
- Adresse e-mail
- Numéro de téléphone
- Date de naissance
- Informations financières (par exemple, relevés bancaires, détails fiscaux)
- Numéro d'assurance sociale
- Autres informations pertinentes, selon les besoins (par exemple, données démographiques, pertinence des programmes)

Ces informations sont collectées de manière légale et équitable et sont utilisées uniquement pour les fins pour lesquelles elles ont été collectées. Dans la mesure du possible, les informations personnelles sont collectées directement auprès de la personne concernée, sauf si un consentement explicite est donné pour les obtenir à partir d'une autre source.

Utilisation des informations collectées par l'ICRC:

- Déclaration des impôts
- Traitement des T4A
- Gestion des dossiers des collaborateur.tice.s, sponsor.e.s et partenaires
- Traitement des fonds et des prix
- Organisation de programmes et de sessions de formation
- Communication sur nos activités et services
- Conformité aux obligations légales et réglementaires des bailleurs de fonds
- Évaluation et amélioration des programmes et services

L'ICRC s'engage à obtenir le consentement des individu.e.s avant de collecter, utiliser ou divulguer leurs informations personnelles, sauf lorsque la loi ou des exigences contractuelles l'exigent. Le consentement peut être exprimé (par exemple, signature d'un formulaire) ou implicite (par exemple, la fourniture volontaire d'informations).

Les individu.e.s ont le droit de retirer leur consentement à tout moment, sous réserve des restrictions légales ou contractuelles et d'un préavis raisonnable. Si le

consentement est retiré, l'ICRC informera l'individu.e des conséquences de ce retrait, y compris de l'impact potentiel sur les services et avantages fournis.

Destruction des données

L'ICRC conserve les renseignements personnels aussi longtemps que nécessaire pour atteindre les objectifs pour lesquels ils ont été collectés ou pour se conformer aux obligations légales. Une fois ces objectifs atteints, les données personnelles seront détruites de manière sécuritaire, conformément aux pratiques standards.

Clause de confidentialité

Tous les employé.e.s, bénévoles et collaborateur.trice.s de l'ICRC doivent signer une entente de confidentialité qui les engage à protéger les renseignements personnels et à respecter cette politique en tout temps.

Divulgation des renseignements personnels

L'ICRC ne partage pas les renseignements personnels avec des tier.ses, sauf dans les cas suivants :

1. Avec le consentement explicite de la personne concernée.
2. Lorsque requis par la loi ou pour répondre à une demande légitime des autorités compétentes.
3. Lorsque nécessaire pour fournir les services demandés (p. ex. : transmettre des informations à Revenu Québec pour une déclaration fiscale).

Sécurité des renseignements personnels

L'organisation met en œuvre des mesures de sécurité afin de protéger les données personnelles contre la perte, le vol ou l'accès non autorisé. Ces mesures comprennent :

1. **Barrières physiques et techniques** : Protection des locaux où les informations personnelles sont stockées, utilisation de pare-feu, de logiciels antivirus et de cryptage des données.

2. **Procédures de sauvegarde et de récupération** : Mesures de sécurité contre la perte accidentelle d'informations personnelles grâce à des systèmes de sauvegarde et de récupération des données.
3. **Gestion des accès** : Mise en place de procédures pour garantir que seules les personnes autorisées puissent accéder aux informations personnelles.
4. **Sensibilisation du personnel** : Formation des employé.e.s sur l'importance de la confidentialité et établissement de politiques et de procédures pour garantir la protection des informations personnelles.
5. **Gestion des incidents** : Création de procédures pour gérer les urgences et les incidents de sécurité.
6. **Gestion des fournisseurs** : Mise en place de procédures pour garantir que les fournisseur.euse.s ayant accès à des informations personnelles respectent les pratiques appropriées en matière de confidentialité.
7. **Mesures physiques** : Stockage sécurisé des informations personnelles et accès restreint aux zones où ces informations sont conservées.

L'ICRC s'efforce de maintenir des mesures de sécurité à jour et évalue régulièrement les risques pour la confidentialité des informations. En cas d'incident de sécurité, l'ICRC prendra les mesures appropriées pour contenir l'incident, en évaluer l'impact et informer les personnes concernées conformément aux exigences légales applicables.

Il est important de noter que, bien que l'ICRC fasse tout son possible pour protéger les informations personnelles, aucune méthode de transmission ou de stockage électronique n'est complètement infaillible. Par conséquent, l'ICRC ne peut garantir une sécurité absolue des informations personnelles, mais s'engage à prendre toutes les mesures possibles pour assurer leur protection. L'organisation s'engage également à mettre régulièrement à jour ces mesures pour s'adapter aux progrès technologiques et aux menaces en constante évolution.

Accès, correction et mise à jour des renseignements personnels

Les individu.e.s ont le droit d'accéder à leurs informations personnelles détenues par l'ICRC et de demander des corrections ou des mises à jour si les informations sont inexactes ou incomplètes.

Les demandes d'accès ou de correction peuvent être faites en contactant le responsable de la protection des données de l'organisation. Afin de garantir la sécurité, il se peut que les individu.e.s soient tenu.e.s de vérifier leur identité avant d'accéder à leurs informations ou de les modifier.

L'ICRC s'engage à répondre aux demandes d'accès et de correction dans les plus brefs délais, généralement dans un délai de trente (30) jours. Dans les cas où l'accès est refusé, l'organisation fournira une explication, sauf si la loi l'interdit.

Utilisation de cookies et de technologies similaires

Le site web de l'ICRC utilise des cookies pour améliorer l'expérience utilisateur.trice. Ces cookies permettent de collecter des données anonymes sur la navigation, comme les pages visitées et les préférences. Ces données ne sont pas liées à des renseignements personnels identifiables et peuvent être désactivées via les paramètres du navigateur. En utilisant le site web, les utilisateurs consentent à l'utilisation de cookies conformément à cette politique.

Liens vers d'Autres Sites Web

Le site web de l'ICRC peut contenir des liens vers des sites web tiers à des fins d'information. Ces sites externes fonctionnent de manière indépendante et ne sont pas régis par cette politique de confidentialité.

L'ICRC n'est pas responsable des pratiques en matière de confidentialité ou du contenu de ces sites tiers. Les utilisateur.trice.s sont encouragé.e.s à consulter les politiques de confidentialité de tout site externe qu'iels visitent.

Modifications de la politique de confidentialité

L’ICRC se réserve le droit de modifier cette politique de confidentialité à tout moment. En cas de modification importante, nous vous en informerons par le biais de notre site web ou par communication directe. Toute mise à jour sera datée et prendra effet dès sa publication.

Contact

Si vous avez des questions ou des préoccupations concernant cette politique de confidentialité, ou si vous souhaitez exercer vos droits en matière de renseignements personnels, veuillez contacter l’ICRC à l'adresse suivante :

Initiative Communautaire de Renforcement des Capacités (ICRC)
info@ccbi.ca
1988 Sainte catherine est #201, Montréal, Qc H2K 2H7

Conclusion

l’ICRC demeure engagée à protéger la vie privée et les informations personnelles des individu.e.s interagissant avec l'organisation. Cette politique de confidentialité constitue un pilier de cet engagement, énonçant les principes et les procédures que nous suivons pour assurer une gestion responsable et éthique des données.

Votre confiance est essentielle à notre mission, et nous nous engageons à respecter les normes les plus élevées en matière de protection des données et de confidentialité dans toutes nos activités.

Annexes

Annexe 1 : Procédure en cas de violation de la sécurité des données

l'ICRC prend très au sérieux les incidents de sécurité des données et suit une procédure définie pour les traiter :

1. **Identification** : Les employé..e.s ou les sous-traitant.e.s doivent signaler immédiatement toute violation suspectée ou confirmée de données à la direction.
2. **Confinement** : Des actions immédiates seront entreprises pour prévenir tout accès non autorisé ou dommage supplémentaire, comme la désactivation des comptes compromis ou l'isolement des systèmes affectés.
3. **Enquête** : Une revue approfondie sera menée pour déterminer l'ampleur et la cause de la violation.
4. **Notification** : Si des informations personnelles sont concernées, les individu.e.s affecté.e.s et les autorités compétentes seront informé.e.s conformément à la législation applicable.
5. **Atténuation** : Des actions correctives seront mises en place pour prévenir de futurs incidents, telles que la révision des protocoles ou le renforcement des mesures de sécurité.

Annexe 2 : Procédures de gestion de la collecte et de la destruction des données

1. **Informations relatives aux déclarations fiscales**
   Données collectées : Revenu, dépenses, états financiers, crédits, déductions, documents justificatifs et autres détails financiers requis pour la préparation des déclarations fiscales.
   Méthodes de collecte : Directement auprès des client.e.s via des formulaires d'admission, des entrevues et des soumissions de documents électroniques.
   Stockage : Bases de données sécurisées et cryptées, avec un accès limité au personnel autorisé.
   Destruction : Aucun document papier n'est accepté, les dossiers électroniques sont supprimés de manière sécurisée après les périodes de conservation légales.
2. **Participants aux programmes et évaluations de l'impact**
   Données collectées : Détails d'inscription des participant.e.s, données démographiques, retours sur les programmes et données d'évaluation de l'impact.
   Méthodes de collecte : Formulaires d'inscription en ligne, enquêtes, entrevues et groupes de discussion.
   Stockage : Bases de données à accès restreint, organisées par programme pour faciliter l'anonymisation lors de l'analyse.
   Destruction : Les données sont anonymisées ou supprimées de manière sécurisée lorsqu'elles ne sont plus nécessaires pour l'évaluation ou la production de rapports.
3. **Inscription des membres et mises à jour**
   Données collectées : Informations d'inscription des membres, données démographiques, préférences, mises à jour et détails de participation aux offres/événements spéciaux.
   Méthodes de collecte : Formulaires d'inscription des membres soumis en ligne.
   Stockage : Bases de données sécurisées des membres avec des contrôles d'accès à plusieurs niveaux.
   Destruction : Les données des membres sont supprimées de manière sécurisée ou anonymisées après l'annulation de l'adhésion ou après une période prolongée d'inactivité, conformément aux politiques organisationnelles.
4. **Fournisseurs**
   Données collectées : Contrats de fournisseur, coordonnées et informations fiscales (par exemple, NAS pour l'émission de T4A).
   Méthodes de collecte : Formulaires d'inscription des fournisseurs et accords contractuels.

Stockage : Systèmes financiers et annuaires d'équipe avec accès administratif uniquement.
Destruction : Les archives sont soit archivées, soit supprimées de manière sécurisée après l'exécution des obligations contractuelles et réglementaires.

5. **Employés et membres du conseil d'administration**
   Données collectées : Contrats de travail, numéros d'assurance sociale (NAS), accords de partenariat, registres de gouvernance et autres documents juridiques.
   Méthodes de collecte : Processus d'intégration, formulaires et candidatures.
   Stockage : Systèmes sécurisés des ressources humaines.
   Destruction : Les dossiers sont détruits de manière sécurisée après la période de conservation légale conformément aux lois du travail.
6. **Contributions financières et gestion des dossiers**
   Données collectées : Montants des dons et parrainages, informations de contact des donateurs et parrains.
   Méthodes de collecte : Formulaires de don, systèmes de paiement en ligne ou plateformes tierces.
   Stockage : Systèmes de gestion sécurisés conformes aux régulations applicables.
   Destruction : Les données sont supprimées de manière sécurisée après les périodes de conservation légales.
7. **Partenaires et collaborateurs**
   Données collectées : Coordonnées, accords de partenariat et ressources partagées.
   Méthodes de collecte : Accords de partenariat et bases de données partagées.
   Stockage : Systèmes de gestion documentaire avec accès partagé mais restreint.
   Destruction : Les informations sont supprimées des systèmes partagés et supprimées de manière sécurisée après la fin du partenariat.