POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Teo Support Admin

Entreprise individuelle Dernière mise à jour: décembre 2025 Entrée en vigueur: 1er janvier 2026

TABLE DES MATIÈRES

POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS 1
- TABLE DES MATIÈRES 1
- 1. INTRODUCTION ET PRINCIPES 3
- 2. IDENTIFICATION DE L'ORGANISATION 4
- 3. RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 4
- 4. FINS DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS 5
- 5. CONSENTEMENT 6
- 6. TYPES DE RENSEIGNEMENTS COLLECTÉS 8
- 7. MOYENS DE COLLECTE 10
- 8. COMMUNICATION DES RENSEIGNEMENTS À DES TIERS 13
- 9. SOUS-TRAITANTS ET FOURNISSEURS DE SERVICES 14
- 10. TRANSFERTS TRANSFRONTALIERS DE DONNÉES 17
- 11. DURÉE DE CONSERVATION 19
- 12. MESURES DE SÉCURITÉ 20
- 13. DROITS DES PERSONNES CONCERNÉES 23
- 14. GESTION DES INCIDENTS DE CONFIDENTIALITÉ 26
- 15. MODIFICATIONS DE LA POLITIQUE 30
- 16. COORDONNÉES POUR QUESTIONS OU RÉCLAMATIONS 31
- CONCLUSION 32
- ANNEXE A: GLOSSAIRE 32
- ANNEXE B: FORMULAIRE DE CONSENTEMENT 33

---

1. INTRODUCTION ET PRINCIPES

Teo Support Admin (ci-après « l'Entreprise ») s'engage à protéger les renseignements

personnels qu'elle collecte, utilise et conserve, conformément à la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « Loi 25 »).

Cette politique décrit nos pratiques en matière de protection des renseignements personnels et les droits dont disposent les personnes concernées. Elle s'applique à tous les renseignements personnels traités par l'Entreprise, qu'ils soient collectés directement auprès des personnes concernées ou auprès de tiers.

L'Entreprise adhère aux principes suivants:

- **Légitimité**: Les renseignements ne sont collectés que pour des fins déterminées, explicites et légales.
- **Consentement**: Le consentement est obtenu de manière claire, libre, éclairée et spécifique pour chaque fin de collecte.
- **Transparence**: Les personnes sont informées de la nature, de l'étendue et de l'utilisation de leurs renseignements.
- **Sécurité**: Des mesures appropriées sont mises en place pour protéger les renseignements contre l'accès non autorisé, la perte ou la divulgation.
- **Responsabilité**: L'Entreprise assume la responsabilité de ses pratiques en matière de protection des renseignements.

---

2. IDENTIFICATION DE L'ORGANISATION

Nom légal: Teo Support Admin

Type d'entité: Entreprise individuelle

Adresse: 1055 rue de la Gauchetière, App 110, Montréal, H2L0E5, CA

Province/Territoire: Québec, Canada

Numéro d'entreprise du Québec (NEQ): 2281639775

Secteur d'activité: Services de conseil et soutien en amélioration des processus administratifs et opérationnels

Description des activités: L'Entreprise offre des services de conseil et de soutien administratif aux organisations, notamment des conseils en matière de processus opérationnels, d'organisation administrative, de mise en place de solutions numériques et de gestion de données. L'Entreprise aide ses clients à optimiser leurs opérations en utilisant diverses solutions logicielles et plateformes.

---

3. RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Conformément à la Loi 25, l'Entreprise a désigné une personne responsable de la protection des renseignements personnels (ci-après « RPRP »).

Responsable désigné:

- **Nom:** Teo Blanc
- **Titre/Fonction:** Propriétaire - Responsable Protection Données
- **Adresse:** 1055 rue de la Gauchetière, App 110, Montréal, H2L0E5, CA
- **Téléphone:** (438) 596-2000
- **Courriel:** rprp@teo.support

Le RPRP est responsable de:

- Assurer la conformité aux dispositions de la Loi 25
- Répondre aux questions concernant la protection des renseignements personnels
- Traiter les demandes d'accès, de rectification et de suppression
- Gérer les incidents de confidentialité
- Mener des évaluations des facteurs relatifs à la vie privée (EFVP) selon les besoins
- Mettre en place les mesures de sécurité appropriées

Les personnes concernées peuvent communiquer avec le RPRP à tout moment pour toute question ou préoccupation relative à cette politique ou à la protection de leurs renseignements personnels.

---

4. FINS DE LA COLLECTE DES RENSEIGNEMENTS PERSONNELS

L'Entreprise collecte et traite les renseignements personnels pour les fins suivantes:

4.1 Fins Principales

4.1.1 Exécution des Services de Conseil et Soutien Administratif

- Fournir les services de conseil et de soutien aux clients
- Analyser les processus administratifs et opérationnels du client

- Élaborer et mettre en œuvre des recommandations d'amélioration
- Préparer les rapports et documentations relatifs aux services
- Communiquer avec les représentants du client concernant l'exécution des services
- Cette fin inclut l'accès aux données opérationnelles du client, lesquelles peuvent contenir les renseignements personnels des employés, clients ou bénéficiaires du client

4.1.2 Gestion Administrative et Opérationnelle

- Tenir des dossiers clients et de projets
- Facturation et gestion des paiements
- Correspondance administrative
- Archivage et tenue de registres

4.1.3 Conformité Légale et Réglementaire

- Respecter les obligations légales applicables
- Conserver les renseignements pour fins de preuve
- Répondre aux demandes d'autorités compétentes

4.1.4 Analyse et Amélioration des Services

- Évaluer la qualité des services fournis
- Identifier les domaines d'amélioration
- Adapter les services aux besoins des clients (à condition de l'anonymisation des données)

4.2 Fins Secondaires

4.2.1 Communications de Marketing et Promotion

- Informer les clients actuels et potentiels des nouveaux services
- Envoyer des mises à jour concernant l'Entreprise
- **Important:** Aucune communication de marketing ne sera envoyée sans consentement distinct et explicite.

4.2.2 Suivi Analytique du Site Web

- Analyser l'utilisation du site internet
- Améliorer l'expérience utilisateur
- Compiler des statistiques d'accès (anonymisées lorsque possible)
- **Important:** Voir section 7.3 concernant les cookies et le consentement.

4.3 Absence d'Autres Fins

Sauf indication contraire dans un contrat spécifique avec le client, l'Entreprise n'utilisera pas les renseignements collectés à des fins autres que celles énumérées ci-dessus. Toute utilisation additionnelle nécessitera un consentement distinct et explicite.

---

5. CONSENTEMENT

5.1 Principes Généraux du Consentement

Conformément à la Loi 25, le consentement doit être:

- **Manifeste:** Exprimé par le biais d'une déclaration, d'une action positive ou d'une signature
- **Libre:** Donné sans contrainte, pression ou influence
- **Éclairé:** Basé sur une information claire et complète
- **Spécifique:** Donné pour chacune des fins de traitement identifiées

Le consentement n'est PAS obtenu par défaut. L'absence de réaction (« opt-out ») ne constitue pas un consentement valide. Un consentement explicite (« opt-in ») est requis.

5.2 Demande de Consentement

Le consentement est obtenu de la manière suivante:

5.2.1 Demandes Écrites

- Lorsque le consentement est demandé par écrit, la demande est présentée **distinctement** de toute autre information ou condition
- Le consentement est clairement identifié dans le document
- Le langage utilisé est clair, simple et compréhensible
- La personne peut refuser sans conséquence négative

5.2.2 Moyens de Consentement

- Signature (papier ou électronique)
- Cocher une case dédiée
- Cliquer un bouton de confirmation sur le site web
- Envoyer un courriel de confirmation
- Autres méthodes clairement explicites

5.2.3 Consentement Distinct par Fin

Pour les fins suivantes, le consentement est demandé **séparément et distinctement**:

1. Services de conseil (consentement implicite par engagement de service)
2. Communications de marketing
3. Analyse du site web via cookies
4. Partage de données avec des tiers spécifiques
5. Collecte de données sensibles (le cas échéant)

5.3 Renseignements à Fournir Avant Consentement

Avant de demander le consentement, l'Entreprise informe la personne concernée de:

- Les fins précises de la collecte
- Les moyens de collecte
- L'identité du tiers pour qui la collecte est réalisée (le cas échéant)
- L'identité des tiers à qui les renseignements seront communiqués
- La durée de conservation des renseignements
- Les droits d'accès, de rectification et de suppression
- Le droit de retirer son consentement

5.4 Retrait du Consentement

Une personne peut retirer son consentement à tout moment. Le retrait ne s'applique qu'à la collecte future et n'annule pas les traitements effectués avant le retrait, pour autant que le traitement antérieur était légal.

Pour retirer son consentement, la personne communique avec le RPRP aux coordonnées fournies à la section 16.

5.5 Personnes Mineures

En cas de collecte de renseignements concernant une personne de moins de 14 ans, le consentement de la personne titulaire de l'autorité parentale ou du tuteur légal est obligatoire. L'Entreprise identifiera à l'avance toute collecte pouvant concerner des mineurs et prendra les mesures appropriées.

---

6. TYPES DE RENSEIGNEMENTS COLLECTÉS

6.1 Renseignements Fournis Directement par la Personne

L'Entreprise collecte les types de renseignements suivants directement auprès des personnes:

Renseignements d'Identification de Base:

- Prénom et nom
- Adresse courriel professionnelle ou personnelle
- Numéro de téléphone (téléphone fixe ou mobile)
- Adresse postale complète
- Titre/fonction professionnelle

Renseignements Professionnels et Opérationnels:

- Nom de l'organisation pour laquelle travaille la personne
- Description du rôle et des responsabilités
- Historique de communication avec l'Entreprise
- Détails des projets et mandats
- Observations et préférences concernant les services

Renseignements Relatifs aux Paiements:

- Informations de facturation
- Adresse de facturation
- **IMPORTANT:** L'Entreprise NE collecte PAS directement les numéros de carte de crédit ou autres données bancaires sensibles (voir section 9 concernant Stripe)

Renseignements Accessoires:

- Informations d'authentification (identifiant, mot de passe haché) pour accès aux services en ligne
- Date de naissance (si fournie volontairement)
- Langue préférée de communication

6.2 Renseignements Obtenus Auprès de Clients

Dans le cours de l'exécution de ses services, l'Entreprise a accès à et traite les renseignements personnels des clients du client, notamment:

- Noms et coordonnées des employés du client
- Listes de membres, bénéficiaires ou clients du client
- Renseignements opérationnels concernant les individus (ex. : rôle, historique, interactions)
- Données relatives à la paie (salaires) - si applicable à l'analyse des processus
- Données de communication (courriels, messages)

Note Importante: L'Entreprise obtient l'accès à ces renseignements strictement pour les fins de fourniture des services de conseil au client. L'Entreprise ne peut pas utiliser

ces données à d'autres fins sans consentement additionnel.

6.3 Renseignements Collectés Automatiquement via le Site Web

Via Formulaires Web:

- Informations soumises via formulaires de contact
- Demandes d'information
- Inscriptions aux infolettres

Via Cookies et Suivi Analytique:

- Adresse IP
- Type de navigateur et système d'exploitation
- Pages visitées et temps passé
- Source du trafic (référents)
- Interactions sur le site (clics, défilements)
- Données démographiques approximatives (localisation géographique générale)

Note importante: Un consentement explicite aux cookies est requis via le panneau de consentement du site. Voir section 7.3.

6.4 Renseignements NON Collectés Intentionnellement

L'Entreprise ne collecte PAS intentionnellement:

- Numéros de carte d'identité ou permis de conduire
- Numéros d'assurance sociale
- Renseignements de santé ou données médicales
- Données génétiques
- Données biométriques
- Renseignements relatifs aux casiers judiciaires
- Convictions criminelles
- Autres données sensibles sans consentement explicite et justification

Si ces renseignements sont fournis accidentellement, ils seront supprimés immédiatement.

6.5 Renseignements Inférés ou Dérivés

L'Entreprise peut, à partir des données collectées, créer des renseignements inférés ou dérivés à des fins analytiques internes, notamment:

- Profils d'utilisation ou modèles de comportement (anonymisés)
- Segments de clients pour amélioration des services

- Analyses statistiques

Ces données inférées sont conservées uniquement sous forme anonymisée ou agrégée et ne permettent pas d'identifier des individus spécifiques.

---

7. MOYENS DE COLLECTE

7.1 Collecte Directe via Formulaires et Communications

L'Entreprise collecte les renseignements directement auprès des personnes par les moyens suivants:

- **Formulaires Web:** Les personnes soumettent volontairement des informations via les formulaires du site internet (ex. formulaire de contact, demande de services)
- **Courriels:** Communications directes avec les clients et prospects
- **Appels Téléphoniques:** Discussions verbales et prise de rendez-vous
- **Rencontres en Personne:** Lors de consultations ou présentations
- **Documents Signés:** Contrats de service, ententes de confidentialité, confirmations écrites

7.2 Collecte via Outils et Plateformes

L'Entreprise utilise les plateformes et logiciels suivants pour collecter, stocker et traiter les renseignements personnels:

Outils de Gestion Administrative:

- **Google Workspace** (Gmail, Google Drive, Google Sheets, Google Docs): Stockage et gestion de la correspondance, documents clients, données administratives
- **Airtable:** Base de données pour gestion des clients, projets, contacts, données opérationnelles du client
- **Softr:** Création de portails et interfaces web pour collecte et affichage de données
- **Zapier:** Automatisation et intégration entre différents outils

Outils de Communication et Collecte:

- **JotForm:** Création de formulaires web pour collecte de données
- **Google Meet:** Réunions en ligne (enregistrements audio/vidéo avec consentement)

Outils de Sécurité et Accès:

- **KeePassXC:** Gestion sécurisée des mots de passe (local)
- **Cloudflare:** Service DNS et sécurité web

Traitement de Paiements:

- **Stripe:** Traitement sécurisé des paiements (l'Entreprise ne reçoit jamais directement les données bancaires)

7.3 Cookies et Suivi Analytique du Site Web

7.3.1 Types de Cookies Utilisés

Le site internet de l'Entreprise utilise les cookies suivants:

Cookies Strictement Nécessaires (sans consentement requis):

- Cookies de session pour maintenir la connexion
- Cookies de sécurité pour prévention des fraudes
- Cookies techniques pour fonctionnement du site

Cookies Analytiques (consentement requis):

- **Google Analytics:** Analyse du trafic du site, comportement utilisateur, démographie approximative
- Suivi des pages visitées, durée des sessions, taux de rebond

Cookies de Marketing (consentement requis):

- Pixels de tracking pour publicités réorientées
- Suivi des conversions

7.3.2 Gestion du Consentement aux Cookies

À la première visite du site, un **panneau de consentement** s'affiche demandant explicitement à l'utilisateur de consentir ou refuser:

- Cookies analytiques
- Cookies de marketing
- Autres technologies de tracking

L'utilisateur peut:

- **Accepter tous:** Accepter tous les cookies
- **Refuser tout:** Rejeter les cookies non nécessaires

- **Gérer les préférences:** Choisir finement quels types de cookies accepter

Le consentement est enregistré et l'utilisateur peut modifier ses préférences à tout moment via un lien accessible au pied de page du site.

7.3.3 Durée de Conservation des Cookies

- Cookies strictement nécessaires: Durée de la session ou jusqu'à max. 1 an
- Cookies analytiques: Maximum 2 ans
- Cookies de marketing: Maximum 1 an

7.3.4 Renseignements Google Analytics

Google Analytics est utilisé pour analyser l'utilisation du site. Les données sont envoyées à Google selon les conditions d'utilisation de Google Analytics. L'Entreprise a configuré Google Analytics pour:

- Anonymiser les adresses IP (masquage du dernier octet)
- Supprimer automatiquement les données après 26 mois
- Respecter le droit au consentement

Pour plus d'informations sur la protection des données par Google Analytics, consulter: https://policies.google.com/privacy

7.4 Intégrations et Partenaires Tiers

Lors du processus de collecte, les données sont souvent transmises à des plateformes tierces. Voir la section 8 et 9 pour les détails sur les tiers.

---

8. COMMUNICATION DES RENSEIGNEMENTS À DES TIERS

8.1 Principes Généraux

L'Entreprise communique les renseignements personnels à des tiers UNIQUEMENT:

1. Avec le consentement explicit de la personne concernée, OU
2. Lorsque la loi l'exige, OU
3. Lorsqu'il s'agit d'un sous-traitant mandaté pour traiter les données au nom de l'Entreprise

Pour les communications sans consentement (exceptions légales), l'Entreprise mènera

une **Évaluation des Facteurs Relatifs à la Vie Privée (EFVP)** avant la communication.

8.2 Tiers Auxquels les Données Peuvent Être Communiquées

À titre de Sous-traitants (données traitées au nom de l'Entreprise):

- Partenaires cloud pour stockage sécurisé
- Prestataires de services techniques

Avec Consentement Explicite:

- Autres organisations de conseil ou prestataires de services externes
- Auditeurs externes (si requis légalement)

Cas Spécifique - Données de Clients du Client: Lorsque l'Entreprise traite les renseignements des clients du client (ex.: employés, membres), ces données ne sont communiquées à d'autres tiers QUE:

- Avec l'autorisation du client principal, OU
- Lorsque le client principal l'exige dans le cadre du mandat (ex.: exporter les données vers une nouvelle plateforme)

8.3 Communication NON Réalisée

L'Entreprise NE communique PAS les renseignements à:

- Des fins de marketing ou prospection sans consentement
- Des tiers pour vente ou location de listes de contacts
- À des fins publicitaires ciblées sans consentement
- Des tiers externes non essentiels à la fourniture des services

8.4 Obligations Envers les Personnes Communiquées

Lorsque l'Entreprise communique des renseignements à un tiers sans consentement de la personne (via exception légale), elle doit:

- Informer la personne de la communication envisagée
- Identifier le tiers ou la catégorie de tiers
- Expliquer la raison de la communication
- Donner à la personne la possibilité de s'opposer (sauf exception)

---

9. SOUS-TRAITANTS ET FOURNISSEURS DE SERVICES

9.1 Définition et Responsabilités

Un **sous-traitant** est une personne ou une organisation qui traite les renseignements personnels pour le compte de l'Entreprise (responsable du traitement), selon les instructions de cette dernière.

Les sous-traitants de l'Entreprise sont tenus de:

- Traiter les renseignements UNIQUEMENT selon les instructions de l'Entreprise
- Assurer la confidentialité des renseignements
- Mettre en place des mesures de sécurité appropriées
- Notifier l'Entreprise en cas d'incident de confidentialité
- Permettre à l'Entreprise de procéder à des audits et vérifications
- Ne pas communiquer les renseignements à d'autres tiers sans autorisation

9.2 Liste des Sous-traitants Actuels

9.2.1 Google Workspace (Google Canada Corp.)

- **Finalité:** Stockage et gestion des courriels professionnels, documents, feuilles de calcul, gestion des contacts, calendrier
- **Type de données:** Renseignements clients, données opérationnelles, communications
- **Localisation du traitement:** Serveurs Google (États-Unis et Canada - configurable)
- **Contrat:** Conditions de service Google Workspace + Addenda relatif au traitement de données disponible à https://cloud.google.com/terms/data-processing-addendum
- **Mesures de Sécurité:** Chiffrage en transit et au repos, authentification multi-facteurs, contrôles d'accès

9.2.2 Airtable Inc.

- **Finalité:** Base de données pour gestion des clients, projets, contacts, données administratives
- **Type de données:** Données opérationnelles, contacts clients, informations de projets
- **Localisation du traitement:** États-Unis
- **Contrat:** Conditions d'utilisation d'Airtable + Addenda de traitement de données disponible sur demande
- **Mesures de Sécurité:** Chiffrage, contrôles d'accès basés sur les rôles, journalisation des activités

9.2.3 Zapier Inc.

- **Finalité:** Automatisation et intégration des flux de données entre applications

- **Type de données:** Données transmises entre applications intégrées (varié)
- **Localisation du traitement:** États-Unis
- **Contrat:** Conditions d'utilisation de Zapier + Addenda disponible à https://zapier.com/legal
- **Mesures de Sécurité:** Chiffrage TLS, authentification API, audit trails

9.2.4 Softr Inc. (Softr)

- **Finalité:** Création et hébergement de portails web, interfaces de gestion de données
- **Type de données:** Données affichées ou collectées via les portails Softr
- **Localisation du traitement:** États-Unis
- **Contrat:** Conditions d'utilisation de Softr
- **Mesures de Sécurité:** Hébergement cloud sécurisé, contrôles d'accès utilisateur

9.2.5 Stripe Inc.

- **Finalité:** Traitement sécurisé des paiements en ligne
- **Type de données:** Informations de facturation (nom, adresse, montant)
- **Important:** Stripe NE reçoit jamais directement les numéros de carte de crédit en raison du chiffrage côté client
- **Localisation du traitement:** États-Unis (conforme PCI-DSS)
- **Contrat:** Conditions de service Stripe + Data Processing Addendum
- **Mesures de Sécurité:** Conformité PCI-DSS niveau 1, chiffrage, audit réguliers

9.2.6 Cloudflare Inc.

- **Finalité:** Service de DNS, sécurité web, protection contre les attaques
- **Type de données:** Métadonnées de requêtes web (adresses IP, URLs, temps de réponse)
- **Localisation du traitement:** États-Unis
- **Contrat:** Conditions de service Cloudflare
- **Mesures de Sécurité:** Filtrage DDoS, WAF (Web Application Firewall), DNSSEC

9.2.7 JotForm Inc.

- **Finalité:** Création et hébergement de formulaires web pour collecte de données
- **Type de données:** Données soumises via les formulaires (contacts, demandes d'information)
- **Localisation du traitement:** États-Unis
- **Contrat:** Conditions d'utilisation de JotForm
- **Mesures de Sécurité:** Chiffrage SSL, sauvegardes régulières, contrôles d'accès

9.2.8 KeePassXC (Logiciel Open-Source)

- **Finalité:** Gestion locale et sécurisée des mots de passe (aucune transmission cloud)
- **Type de données:** Mots de passe hachés, identifiants
- **Localisation du traitement:** Appareil local uniquement
- **Mesures de Sécurité:** Chiffrage local fort, aucun accès en ligne

9.3 Évaluation des Sous-traitants

Avant d'engager un sous-traitant, l'Entreprise:

1. Évalue sa capacité à protéger les renseignements conformément à la Loi 25
2. Vérifie ses mesures de sécurité
3. Confirm que des contrats appropriés sont en place
4. Documente l'EFVP si le traitement se fait hors Québec

9.4 Modification de la Liste des Sous-traitants

Si l'Entreprise ajoute ou retire un sous-traitant, elle informera les personnes concernées de cette modification, particulièrement si cela affecte le traitement de leurs renseignements personnels.

---

10. TRANSFERTS TRANSFRONTALIERS DE DONNÉES

10.1 Obligation d'Évaluation des Facteurs Relatifs à la Vie Privée (EFVP)

Conformément à la Loi 25, avant de communiquer ou permettre qu'un sous-traitant traite les renseignements personnels en dehors du Québec, l'Entreprise doit conduire une **Évaluation des Facteurs Relatifs à la Vie Privée (EFVP)**.

Cette évaluation considère:

- La nature et la sensibilité des renseignements
- La quantité et la répartition des renseignements
- Les risques associés à la juridiction de destination
- Les mesures de protection mises en place
- Le régime juridique applicable

10.2 Transferts vers les États-Unis

Statut: L'Entreprise transfère des renseignements personnels aux États-Unis via les sous-traitants suivants: Google Workspace, Airtable, Zapier, Softr, Stripe, JotForm,

Cloudflare.

Risques Identifiés Relatifs à la Juridiction Américaine:

- Régime FISA (Foreign Intelligence Surveillance Act) permettant aux autorités américaines d'accéder à certaines données
- Patriot Act et capacité du gouvernement américain à demander accès à données sans notification
- Absence d'équivalence de protection avec la Loi 25 québécoise
- Potentiels droits d'accès gouvernementaux sans contrôle approprié

Mesures de Protection Mises en Place:

1. **Chiffrage de Bout en Bout:**
    - Les données sensibles ou personnelles sont chiffrées avant transmission vers les serveurs américains
    - Clés de chiffrage conservées au Québec/Canada avec accès contrôlé
    - Impossibilité pour les prestataires d'accéder aux données déchiffrées sans autorisation
2. **Accès Restreint:**
    - Limitation du nombre de personnes ayant accès aux données
    - Authentification multi-facteurs obligatoire
    - Révocation immédiate des accès en cas de cessation de services
3. **Minimisation des Données:**
    - Transmission uniquement des données essentielles
    - Anonymisation ou pseudo-anonymisation lorsque possible
    - Suppression des données sensibles inutiles
4. **Contrats Protecteurs:**
    - Addenda de traitement de données (DPA) avec chaque sous-traitant
    - Clauses de restriction d'accès gouvernemental
    - Obligations de notification en cas de demande légale
    - Audit rights pour vérification de conformité
5. **Durée Minimale:**
    - Conservation limitée à la période nécessaire (5 ans maximum)
    - Destruction sécurisée après la période
    - Procédures documentées de suppression
6. **Audit et Surveillance:**
    - Examens périodiques de la sécurité
    - Monitorage des accès aux données

- Registre des activités sensibles

10.3 Transferts vers le Canada

Statut: Certaines données peuvent également être traitées sur des serveurs canadiens (ex. Google Workspace, Cloudflare).

Considérations:

- Le Canada est assujetti à la PIPEDA (Loi fédérale) et à la Loi 25 (Québec)
- Le régime juridique est plus favorable pour la protection des données
- Risques réduits comparé aux États-Unis
- Mesures de sécurité similaires toujours appliquées

10.4 Aucun Transfert vers Autres Juridictions

L'Entreprise ne transfère pas intentionnellement les renseignements personnels vers d'autres pays (Chine, Russie, Inde, etc.). Si une situation exceptionnelle se présentait, une EFVP supplémentaire serait conduite et le consentement explicite serait obtenu.

10.5 Information aux Personnes Concernées

Lors de la collecte, les personnes sont informées que:

- Leurs renseignements peuvent être traités aux États-Unis et au Canada
- Des mesures de protection appropriées sont mises en place
- Elles ont le droit de s'opposer à ce transfert (bien que cela puisse limiter la fourniture des services)

---

11. DURÉE DE CONSERVATION

11.1 Principe de Conservation Minimale

L'Entreprise conserve les renseignements personnels que le temps nécessaire pour atteindre les fins pour lesquelles ils ont été collectés. Au-delà de cette période, les renseignements sont supprimés ou anonymisés.

11.2 Durées de Conservation par Catégorie

Renseignements de Clients Actuels (pendant la relation):

- Conservés pendant la durée du contrat de service
- Accès et modification possibles tant que le client a besoin

Renseignements de Clients Anciens:

- Conservés pendant **5 ans** après la fin de la relation commerciale
- Justification: Obligations légales et comptables, potentiels litiges, références futures

Données Transactionnelles (Paiements):

- Conservées pendant **7 ans** conformément aux obligations comptables québécoises et fédérales
- Minimum requis par Revenu Québec et Revenu Canada

Données de Prospects (Contactés Mais Non Convertis):

- Conservées pendant **2 ans** maximum
- Possibilité de suppression plus rapide si la personne le demande
- Suppression automatique si pas d'engagement pendant 2 ans

Données du Site Web (Cookies et Analytics):

- Google Analytics: Données conservées 26 mois maximum, puis suppression automatique
- Cookies de session: Supprimés à la fin de la session
- Cookies de marketing: Conservés 12 mois maximum

Renseignements de Tiers Partagés:

- Durée déterminée par le contrat avec le client principal
- Suppression ou retour à la fin du mandat
- Aucune conservation au-delà de 5 ans sans justification spécifique

Registres d'Incidents:

- Conservés pendant **3 ans** pour fins de conformité et audit
- Ensuite anonymisés ou supprimés

11.3 Exceptions à la Durée de Conservation

L'Entreprise peut conserver les renseignements au-delà des délais normaux si:

- La loi l'exige (ex. obligations comptables/fiscales)
- Un litige est en cours ou prévisible
- La personne concernée a donné un consentement spécifique à conservation prolongée
- Les renseignements sont anonymisés ou dépersonnalisés

- Contrat spécifique avec le client prévoit une durée différente

11.4 Procédure de Suppression

À la fin de la période de conservation:

1. Les données sont identifiées comme candidates à suppression
2. Une vérification est effectuée pour confirmer aucune obligation légale de rétention
3. Les données sont supprimées de manière sécurisée (suppression impossible à récupérer)
4. Les sauvegardes contenant les données sont également supprimées après période de rétention des backups (généralement 6 mois)
5. Un registre de suppression est tenu

---

12. MESURES DE SÉCURITÉ

12.1 Principes de Sécurité

L'Entreprise met en place des mesures de sécurité appropriées et proportionnées à:

- La sensibilité des renseignements traités
- Les risques d'accès non autorisé, de perte ou de divulgation
- L'état des technologies disponibles
- La nature du traitement

L'Entreprise reconnaît qu'aucun système n'est 100% sécurisé. Ces mesures visent à atténuer les risques à un niveau raisonnablement acceptable.

12.2 Mesures Techniques de Sécurité

12.2.1 Chiffrage et Encryptage

- Chiffrage TLS 1.2+ pour toutes les communications en ligne
- Chiffrage à repos pour données stockées en cloud (Google Workspace, Airtable, etc.)
- Chiffrage local pour données sur appareils personnels (KeePassXC)
- Certificats SSL valides pour tous les services web

12.2.2 Authentification

- Authentification multi-facteurs (2FA/MFA) obligatoire pour tous les comptes critiques
- Mots de passe forts (minimum 12 caractères, mix de caractères)

- Pas de partage de mots de passe entre services
- Utilisation de gestionnaire de mots de passe (KeePassXC)

12.2.3 Contrôle d'Accès

- Accès selon le principe du « moindre privilège »
- Rôles utilisateur définis (administrateur, éditeur, visualisateur, lecteur seul)
- Révocation immédiate d'accès en cas de cessation de service
- Audit trails pour tracer les accès et modifications

12.2.4 Sécurité Réseau

- Utilisation obligatoire de VPN pour accès distants
- Firewall et protection DDoS (Cloudflare)
- Filtrage du trafic malveillant
- Pas d'accès direct depuis réseaux Wi-Fi publics sans VPN

12.2.5 Sauvegarde et Récupération

- Sauvegardes régulières de données critiques
- Sauvegardes stockées en local et en cloud (redondance)
- Tests périodiques de restauration
- Plans de récupération en cas de sinistre

12.3 Mesures Organisationnelles de Sécurité

12.3.1 Politiques et Procédures

- Politique d'utilisation acceptable des ressources informatiques
- Procédures d'onboarding/offboarding des utilisateurs
- Procédures de gestion des incidents de confidentialité
- Procédures de suppression de données

12.3.2 Formation et Sensibilisation

- Formation annuelle en protection des données et sécurité informatique
- Sensibilisation aux risques de phishing et ingénierie sociale
- Bonnes pratiques en matière de gestion des mots de passe
- Protocoles en cas d'incident

12.3.3 Limitation de l'Accès

- Accès restreint aux données sensibles
- Données sensibles stockées en cloud uniquement, jamais localement
- Partage de données via liens sécurisés avec expiration, pas en copie locale

- Documenter toute personne ayant accès à données sensibles

12.3.4 Évaluation et Audit

- Évaluations périodiques (annuelles) des facteurs relatifs à la vie privée
- Vérifications de sécurité informatique
- Tests de pénétration si applicable
- Audits de conformité Loi 25

12.4 Mesures Spécifiques par Type de Données

Données Hautement Sensibles:

- Données bancaires, numéros d'assurance sociale, données médicales
- Méthode: Chiffrage fort, accès très limité, audit trail détaillé

Données Sensibles:

- Noms, adresses, numéros de téléphone, adresses courriel
- Méthode: Chiffrage, contrôle d'accès, audit trail

Données Non Sensibles:

- Informations publiques, données anonymisées
- Méthode: Sécurité de base, audit occasionnel

12.5 Appareils et Travail à Distance

Sécurité des Appareils Personnels:

- Antivirus et firewall personnels obligatoires
- Mises à jour de sécurité régulières
- Verrouillage automatique après inactivité
- Chiffrage du disque dur

Aucun Stockage Local de Données Sensibles:

- Données sensibles/confidentielles JAMAIS stockées localement
- Stockage exclusivement en cloud (Google Drive, Airtable, etc.)
- Téléchargement temporaire autorisé seulement avec chiffrage
- Suppression immédiate après utilisation

Travail à Distance:

- VPN obligatoire si accès depuis domicile ou lieux publics
- Connexion Wi-Fi privée (wifi publics interdits sans VPN)
- Écran de veille avec mot de passe (30 min inactivité)

- Pas de partage d'écran avec données sensibles visibles

12.6 Accès des Sous-traitants

L'Entreprise s'assure que chaque sous-traitant:

- Met en place des mesures de sécurité appropriées
- Restreint l'accès aux données
- Notifie en cas d'incident
- Permet les audits de sécurité
- Respecte les instructions de l'Entreprise

---

13. DROITS DES PERSONNES CONCERNÉES

13.1 Droits Reconnus par la Loi 25

Les personnes dont l'Entreprise détient des renseignements personnels disposent des droits suivants:

13.2 Droit d'Accès

La personne a le droit de demander l'accès à tout renseignement personnel la concernant que détient l'Entreprise.

Comment exercer ce droit:

1. Envoyer une demande écrite au RPRP à l'adresse fournie à la section 16
2. Inclure suffisamment d'information pour identifier la demande (nom, adresses, période, projet, etc.)
3. L'Entreprise dispose de **30 jours** pour répondre
4. La communication sera faite de manière sécurisée (lien sécurisé, mot de passe, ou remise en personne)
5. Aucuns frais applicables sauf si la demande est manifestement abusive ou exagérée

Contenu de la Réponse:

- Liste complète des renseignements personnels conservés
- Fins pour lesquelles les renseignements sont utilisés
- Catégories de personnes ayant accès
- Durée de conservation prévue
- Coordonnées du RPRP

13.3 Droit de Rectification

La personne peut demander la correction de tout renseignement personnel qui est inexact, incomplet ou équivoque.

Comment exercer ce droit:

1. Envoyer une demande écrite spécifiant les corrections demandées
2. Fournir des preuves ou justifications si pertinent
3. L'Entreprise corrigera les renseignements dans les **30 jours**
4. Les parties n'étant pas d'accord peuvent ajouter une note explicative au dossier

13.4 Droit de Suppression ou d'Anonymisation

La personne peut, dans certaines circonstances, demander la suppression ou l'anonymisation de ses renseignements.

Cas où la suppression est possible:

- Les renseignements ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés
- La durée de conservation légale a expiré
- La personne retire son consentement
- Les renseignements sont utilisés illégalement

Cas où la suppression peut être refusée:

- Les renseignements sont requis pour conformité légale
- Un litige est en cours et les données sont pertinentes
- Contrat avec client spécifie la rétention

Processus:

1. Demande écrite au RPRP
2. Évaluation de la demande dans les 30 jours
3. Suppression sécurisée si approuvée (impossible à récupérer)
4. Notification de completion

13.5 Droit à la Portabilité des Données (Nouveau)

Depuis le 22 septembre 2024, la personne a le droit de recevoir ses renseignements personnels informatisés dans un format technologique structuré et couramment utilisé.

Données Concernées:

- Renseignements informatisés recueillis directement auprès de la personne

- Doivent être dans un format technique standard (CSV, JSON, XML, etc.)

Données NON Concernées:

- Renseignements inférés ou dérivés par l'Entreprise
- Données créées par l'Entreprise (analyses, rapports)
- Renseignements obtenus auprès de tiers

Comment exercer ce droit:

1. Demande écrite au RPRP
2. Spécifier quelles données portabilité est demandée
3. L'Entreprise fournira les données dans les **30 jours** en format structuré
4. Possibilité de demander transmission directe à tiers autorisé
5. Aucuns frais

13.6 Droit de Retrait du Consentement

La personne peut retirer son consentement à tout moment.

Conséquences:

- S'applique uniquement aux traitements futurs
- N'annule pas les traitements antérieurs légaux
- Peut affecter la capacité de l'Entreprise à fournir certains services

Comment exercer:

1. Communiquer avec le RPRP par écrit
2. Spécifier quel consentement est retiré (marketing, cookies, partage tiers, etc.)
3. Confirmation dans les 7 jours

13.7 Droit de S'Opposer

La personne peut s'opposer au traitement de ses renseignements pour certaines fins (notamment marketing direct et profilage).

Comment exercer:

1. Communiquer opposition au RPRP
2. Respecté immédiatement pour nouvelles communications de marketing

13.8 Droit à l'Explication en Cas de Décisions Automatisées

Si l'Entreprise prenait des décisions basées exclusivement sur le traitement automatisé (ex. algorithmes), les personnes auraient le droit à une explication.

Note: À date, l'Entreprise ne prend pas de décisions importantes basées exclusivement sur traitement automatisé, mais cette disposition demeure pertinente si changement futur.

13.9 Exercice des Droits

Modalités:

- Droits exercés par demande écrite au RPRP
- Peuvent être exercés gratuitement sauf cas abusif
- Délais de réponse standard: **30 jours** (peut être prolongé de 60 jours si complexité)
- Pas de discrimination à l'encontre de la personne ayant exercé un droit

Identification:

- L'Entreprise peut demander une preuve d'identité raisonnables
- Protéger la confidentialité lors de la vérification

---

14. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

14.1 Définition d'un Incident de Confidentialité

Un **incident de confidentialité** est tout événement qui compromet ou pourrait compromettre la protection des renseignements personnels:

- 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
- Toute autre atteinte à la protection d'un tel renseignement

14.2 Évaluation du Risque de Préjudice Sérieux

Pour chaque incident, l'Entreprise doit évaluer s'il présente un **risque de préjudice sérieux** aux personnes concernées.

Facteurs Considérés:

- Nature et sensibilité des renseignements (données bancaires = plus grave que nom)
- Type de personne affectée (mineurs = considération spéciale)
- Probabilité d'utilisation malveillante
- Conséquences potentielles (identité, fraude, discrimination, atteinte réputation,

etc.)
- Mesures de protection en place

Exemples de Préjudice Sérieux:

- Vol d'identité ou fraude financière
- Discrimination ou stigmatisation
- Pertes financières
- Atteinte à réputation ou dignité
- Dommages émotionnels ou psychologiques significatifs

Exemples de NON Préjudice Sérieux:

- Accès accidentel non malveillant sans utilisation ultérieure
- Données déjà publiques
- Données anonymisées/dépersonnalisées
- Données non sensibles accessibles de manière limitée

14.3 Procédure d'Incident

14.3.1 Découverte et Signalement Interne

1. **Détection:** Tout incident détecté est signalé immédiatement au RPRP
2. **Documentation:** Informations initiales consignées (date, nature, portée approximative)
3. **Escalade:** Si incident critique, escalade immédiate

14.3.2 Investigation et Évaluation

1. **Analyse:** Déterminer la cause, la portée, les renseignements affectés
2. **Chronologie:** Établir les dates de l'incident et de sa découverte
3. **Nombre de personnes:** Identifier nombre de personnes potentiellement affectées
4. **Évaluation du Risque:** Déterminer s'il y a risque de préjudice sérieux (voir 14.2)
5. **Documentation:** Tout inscrit dans registre des incidents

14.3.3 Mesures de Mitigation

1. **Confinement:** Isoler la source et empêcher accès additionnel
2. **Remédiation:** Corriger la vulnérabilité ou le processus défaillant
3. **Vérification:** S'assurer qu'aucun accès additionnel n'a eu lieu
4. **Communication:** Préparer communications pour personnes et autorités si nécessaire

14.3.4 Notification à la CAI (Commission d'Accès à l'Information)

Obligation: Si l'incident présente un **risque de préjudice sérieux**, l'Entreprise doit notifier la CAI avec **diligence** (délai raisonnable, généralement 3-7 jours).

Notification Inclut:

- Formulaire officiel de la CAI (disponible à cai.gouv.qc.ca)
- Description complète de l'incident
- Nombre et type de personnes affectées
- Renseignements en cause
- Mesures prises pour mitigation
- Détails de notification aux personnes

Adresse CAI: Commission d'accès à l'information 525, boulevard René-Lévesque Est, bureau 2.36 Québec (QC) G1R 5S9 Téléphone: 418-528-7741 ou 1-888-528-7741 Courriel: cai.communications@cai.gouv.qc.ca

14.3.5 Notification aux Personnes Concernées

Obligation: Si l'incident présente un risque de préjudice sérieux, les personnes affectées doivent être avisées.

Délai: Aussi rapidement que possible après découverte

Contenu de l'Avis:

- Description claire et simple de l'incident
- Types de renseignements affectés
- Date approximative de l'incident
- Mesures que l'Entreprise a prises pour minimiser les dégâts
- Mesures que la personne peut prendre pour se protéger
- Coordonnées pour questions (RPRP)

Moyens de Notification:

- Courriel direct (si adresse disponible)
- Lettre par courrier (si adresse postale disponible)
- Avis public sur le site web (si impossible de rejoindre individuellement)
- Communication médiatique si ampleur importante

14.3.6 Documentation et Registre

Tous les incidents de confidentialité sont inscrits dans un **registre des incidents** qui

inclut:

- Date et heure découverte
- Nature et description de l'incident
- Cause présumée
- Renseignements affectés
- Nombre de personnes affectées
- Évaluation du risque de préjudice sérieux
- Mesures prises
- Date de notification à CAI et/ou personnes
- Date de résolution

Le registre est conservé pendant **3 ans** et peut être divulgué à la CAI sur demande.

14.4 Types d'Incidents et Procédures Spécifiques

Cyberattaque / Ransomware:

- Isolation immédiate des systèmes affectés
- Engagement de professionnels en sécurité informatique si requis
- Évaluation de l'accès aux données
- Considération d'attente avant restauration backup (pour ransomware)

Perte ou Vol de Matériel:

- Identification des données stockées sur l'appareil
- Confirmations que données étaient chiffrées
- Tentatives de localisation
- Évaluation accès possible

Accès Non Autorisé / Violation de Sécurité:

- Identification du vecteur d'attaque
- Audit trails pour identifier données accédées
- Renforcement des contrôles d'accès
- Réinitialisation des mots de passe si compromission

Erreur Humaine (ex. Email mal adressé):

- Demande de retour/suppression au destinataire
- Évaluation si destinataire malveillant possible
- Renforcement procédures
- Évaluation si notification requise

Divulgation Accidentelle:

- Confidentiel divulgué à tiers non autorisé
- Évaluation du risque de divulgation ultérieure
- Confidentiel demandé au destinataire
- Accord de confidentialité si applicable

14.5 Prévention Future

Après chaque incident, l'Entreprise:

1. Identifie la cause fondamentale
2. Implémente des corrections pour éviter récurrence
3. Met à jour procédures/politiques si nécessaire
4. Forme le personnel concerné
5. Teste les mesures pour efficacité

---

15. MODIFICATIONS DE LA POLITIQUE

15.1 Droit de Modification

L'Entreprise se réserve le droit de modifier cette politique de protection des renseignements personnels à tout moment pour:

- Rester conforme aux changements légaux
- Refléter les nouvelles pratiques de l'Entreprise
- Améliorer la protection des renseignements
- Ajouter ou retirer des sous-traitants

15.2 Notification des Modifications

En cas de modification substantielle, les personnes concernées seront notifiées par:

- Courriel direct (si adresse disponible)
- Publication sur le site web
- Mention lors de prochaines interactions

Les modifications mineures (corrections typographiques, clarifications) peuvent être effectuées sans notification préalable.

15.3 Date d'Entrée en Vigueur

La version actuelle de cette politique est en vigueur depuis le 1er janvier 2026.

Les versions antérieures de la politique restent disponibles sur demande auprès du RPRP.

---

16. COORDONNÉES POUR QUESTIONS OU RÉCLAMATIONS

16.1 Personne Responsable de la Protection des Renseignements Personnels

Pour toute question, demande d'exercice de droits, ou signalement d'incident de confidentialité:

Responsable Protection Données:

- **Nom:** Teo Blanc
- **Fonction:** Propriétaire - Teo Support Admin
- **Adresse:** 1055 rue de la Gauchetière, App 110, Montréal, H2L0E5, CA
- **Téléphone:** (438) 596-2000
- **Courriel:** rprp@teo.support

Heures de réponse: Les demandes sont traitées dans les meilleurs délais, délai standard de réponse: **30 jours**.

16.2 Procédure de Réclamation

Si une personne estime que ses droits ont été violés:

1. **Étape 1 - Communication à l'Entreprise:**
    - Communiquer les préoccupations au RPRP en détail
    - Donner 30 jours pour résolution
2. **Étape 2 - Commission d'Accès à l'Information (CAI):**
    - Si insatisfait, présenter plainte à la CAI
    - Adresse: 525, René-Lévesque Est, bureau 2.36, Québec (QC) G1R 5S9
    - Téléphone: 1-888-528-7741
    - Site: https://www.cai.gouv.qc.ca
3. **Étape 3 - Recours Judiciaires:**
    - Actions en dommages-intérêts auprès des tribunaux québécois
    - Consultation d'avocat recommandée

16.3 Site Web et Ressources

- **Site de l'Entreprise:** https://teo.support/
- **Politique de Confidentialité Complète:** Disponible sur site et sur demande
- **Commission d'Accès à l'Information:** https://www.cai.gouv.qc.ca

- **Loi 25 - Informations:** https://www.cai.gouv.qc.ca/loi-25

CONCLUSION

L'Entreprise Teo Support Admin s'engage à protéger la vie privée et les renseignements personnels de tous les individus avec lesquels elle traite. Cette politique fournit un aperçu complet de nos pratiques.

Pour toute question ou clarification, veuillez communiquer avec le Responsable de la Protection des Renseignements Personnels.

Signature/Approbation: 

Nom: Teo Blanc

Fonction: Propriétaire - Teo Support Admin

Date: 2025/12/29

Version: 1.0 **Date d'entrée en vigueur:** 1er janvier 2026 **Prochaine révision prévue:** 1er janvier 2027

ANNEXE A: GLOSSAIRE

- **CAI:** Commission d'accès à l'information (autorité québécoise)
- **DPA:** Data Processing Agreement (accord de traitement de données)
- **EFVP:** Évaluation des Facteurs Relatifs à la Vie Privée
- **Incident de confidentialité:** Accès, utilisation, communication ou perte non autorisée de renseignements personnels
- **Loi 25:** Loi sur la protection des renseignements personnels dans le secteur privé (Québec)
- **PIPEDA:** Loi fédérale sur la protection des renseignements personnels
- **Renseignements personnels:** Toute information permettant d'identifier ou de contacter une personne

- **Responsable du traitement:** Organisation qui détermine les fins et moyens de traitement (Teo Support Admin)
- **RPRP:** Responsable de la Protection des Renseignements Personnels
- **Sous-traitant:** Organisation qui traite les renseignements pour le compte du responsable

---

ANNEXE B: FORMULAIRE DE CONSENTEMENT

[À adapter selon la situation]

Formulaire de Consentement à la Collecte et au Traitement de Renseignements Personnels

Je soussigné(e), _____, confirme que:

1. ☐ J'autorise Teo Support Admin à collecter et utiliser mes renseignements personnels pour la fourniture des services de conseil administratif.

2. ☐ J'autorise Teo Support Admin à m'envoyer des communications marketing et mises à jour concernant ses services.

3. ☐ J'autorise l'utilisation de cookies analytiques sur le site web pour amélioration des services.

4. ☐ J'ai lu et compris la Politique de Protection des Renseignements Personnels.

5. ☐ Je comprends que je peux retirer mon consentement à tout moment en communiquant avec le RPRP.

Signature: _____ Date: _____
