POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Teo Support
Entreprise individuelle
Dernière mise à jour: janvier 2026
Entrée en vigueur: 1er janvier 2026

TABLE DES MATIÈRES

---

1. INTRODUCTION ET PRINCIPES

Teo Support (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.

Portée géographique et réglementaire
Cette politique est principalement fondée sur la Loi 25 applicable au Québec. Lorsque l'Entreprise traite des renseignements personnels de personnes situées dans d'autres provinces canadiennes, elle s'efforce également de respecter la Loi fédérale sur la protection des renseignements personnels et les documents électroniques (PIPEDA). L'Entreprise respecte également les obligations de la Loi canadienne anti-pourriel (LCAP) pour toute communication électronique commerciale.

Principes Directeurs

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 et proportionnées 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

Élément	**Information**
Nom légal	Teo Support
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

Élément	Information
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

Responsabilités du RPRP

Le RPRP est responsable de :

- Assurer la conformité aux dispositions de la Loi 25 et de la LCAP
- Répondre aux questions concernant la protection des renseignements personnels
- Traiter les demandes d'accès, de rectification, de suppression et de portabilité
- Gérer les incidents de confidentialité et assurer la notification en cas de risque

de préjudice sérieux
- Mener des Évaluations des Facteurs Relatifs à la Vie Privée (EFVP) selon les besoins
- Mettre en place et superviser les mesures de sécurité appropriées
- Tenir un registre des incidents de confidentialité

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

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
- **Note importante** : Cette fin inclut l'accès aux données opérationnelles du client, lesquelles peuvent contenir les renseignements personnels des employés, clients ou bénéficiaires du client. Ces données ne sont traitées que strictement aux fins du mandat convenu et selon les instructions 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
- Documentation des services rendus

4.1.3 Conformité Légale et Réglementaire

- Respecter les obligations légales applicables
- Conserver les renseignements pour fins de preuve et de comptabilité

- 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 complète 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
- Partager des contenus ou ressources pertinents aux services

Important : Aucune communication de marketing ne sera envoyée sans consentement distinct et explicite. Le droit de se désabonner sera fourni dans chaque communication et respecté dans les 10 jours ouvrables conformément à la LCAP.

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 requis.

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

Principes clés : 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

5.2.1 Demandes Écrites

- La demande de consentement 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, de suppression et de portabilité
- Le droit de retirer son consentement

5.4 Retrait du Consentement

Une personne peut retirer son consentement à tout moment. Le retrait s'applique uniquement 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 du client.

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

Plateforme Principale : Google Workspace Business Premium

L'Entreprise utilise **Google Workspace Business Premium** comme plateforme centrale de gestion administrative et de traitement des renseignements personnels. Cette plateforme comprend :

- **Gmail** : Stockage et gestion de la correspondance avec les clients et les contacts
- **Google Drive** : Stockage sécurisé des documents clients et données administratives
- **Google Sheets et Google Docs** : Création et gestion collaborative de données opérationnelles
- **Google Contacts** : Gestion des répertoires de contacts clients
- **Google Calendar** : Planification et gestion des rendez-vous

Tous les renseignements personnels traités via Google Workspace bénéficient des mesures de sécurité avancées décrites à la section 12.

Autres Outils de Gestion Administrative

- **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

- **Cloudflare WARP** : VPN sécurisé pour tout accès à distance aux outils contenant des renseignements personnels
- **1Password** : Gestionnaire de mots de passe professionnel pour sécurisation de l'accès à tous les comptes critiques

- **KeePassXC** : Gestion locale et sécurisée des mots de passe pour accès d'urgence (local uniquement, aucun stockage cloud)

Traitement des Paiements

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

Infrastructure de Sécurité Web

- **Cloudflare** : Service DNS, sécurité web et protection contre les attaques DDoS

7.3 Cookies et Suivi Analytique du Site Web

7.3.1 Types de Cookies Utilisés

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

7.3.5 Synchronisation avec la Politique

Les dispositions décrites ci-dessus concernant les cookies reflètent exactement ce qui est implémenté sur le site via le panneau de consentement. Toute modification du fonctionnement technique des cookies entraînera une mise à jour correspondante de la présente politique.

---

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 explicite 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 (Google, Airtable, etc.)
- Prestataires de services techniques (Stripe pour paiements, Zapier pour intégration)
- Services de sécurité (Cloudflare pour protection web)

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 Business Premium (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 Business Premium + Addenda relatif au traitement de données disponible à https://cloud.google.com/terms/data-processing-addendum
- **Mesures de Sécurité Google Workspace** :
    - Authentification multi-facteurs obligatoire
    - Chiffrage automatique en transit (TLS 1.2+) et au repos (AES 256-bit)
    - Contrôles d'accès granulaires basés sur les rôles
    - Audit trails détaillés de toutes les activités
    - Conformité SOC 2 Type II, ISO 27001, HIPAA
    - Protection avancée contre les menaces (Advanced Protection, Titan Security Keys support)
    - Chiffrage de bout en bout pour Docs, Sheets, Drive (optionnel)
    - DLP (Data Loss Prevention) intégré
    - Sauvegardes automatiques et versioning

- Recovery options (restauration de documents supprimés jusqu'à 30 jours)

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, SOC 2 Type II, authentification multi-facteurs

9.2.3 Zapier Inc.

- **Finalité** : Automatisation et intégration des flux de données entre applications
- **Type de données** : Données transmises entre applications intégrées (varié selon les flux)
- **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, SOC 2 Type II

9.2.4 Softr Inc.

- **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, chiffrage en transit et au repos

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 (norme la plus stricte)
    - Chiffrage de bout en bout des données de paiement
    - Audit réguliers par tiers indépendants
    - Tokenization des données de paiement
    - Fraud detection et prevention automatisés

9.2.6 Cloudflare Inc.

- **Finalité** : Service de DNS, sécurité web, protection contre les attaques, VPN WARP pour accès sécurisé à distance
- **Type de données** : Métadonnées de requêtes web (adresses IP, URLs, temps de réponse, informations de connexion VPN)
- **Localisation du traitement** : États-Unis
- **Contrat** : Conditions de service Cloudflare
- **Mesures de Sécurité** :
    - Filtrage DDoS automatique
    - WAF (Web Application Firewall)
    - DNSSEC pour sécurité DNS
    - VPN WARP avec chiffrage Wireguard
    - Protection contre les bots et attaques zero-day
    - Sauvegardes et redondance globale

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, conformité GDPR

9.2.8 1Password (Agile Bits Inc.)

- **Finalité** : Gestion professionnelle et sécurisée des mots de passe et des secrets
- **Type de données** : Mots de passe hachés, clés de sécurité, informations d'authentification
- **Localisation du traitement** : Serveurs cloud avec sièges aux États-Unis et au Canada
- **Contrat** : Conditions de service 1Password
- **Mesures de Sécurité** :
    - Chiffrage end-to-end militaire (AES 256-bit)
    - Zéro-knowledge architecture (1Password n'a jamais accès aux données

non chiffrées)
- Deux facteurs d'authentification obligatoires
- Audit trails de tous les accès aux secrets
- SOC 2 Type II et ISO 27001 certifiés
- Aucun stockage de mots de passe localement sauf sur décision explicite

9.2.9 KeePassXC (Logiciel Open-Source)

- **Finalité** : Gestion locale et sécurisée des mots de passe pour accès d'urgence uniquement (pas de synchronisation cloud)
- **Type de données** : Mots de passe hachés, identifiants
- **Localisation du traitement** : Appareil local uniquement
- **Mesures de Sécurité** : Chiffrage local fort (AES 256-bit), aucun accès en ligne, aucune transmission de données

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 et certifications (SOC 2, ISO 27001, conformité PIPEDA/GDPR)
3. Confirme que des contrats appropriés (DPA - Data Processing Agreement) sont en place
4. Documente l'EFVP si le traitement se fait hors Québec
5. Assure que le sous-traitant s'engage à limiter le traitement aux fins convenues

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
- Les lois d'accès gouvernemental de la juridiction concernée

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 à la personne concernée
- 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. Infrastructure de Sécurité Renforcée

VPN WARP de Cloudflare

- L'Entreprise utilise **Cloudflare WARP** pour tout accès à distance aux outils contenant des renseignements personnels
- WARP fournit un tunnel VPN chiffré (protocole Wireguard) qui isole le trafic de l'Entreprise
- Aucun accès direct aux outils sensibles sans passage par ce VPN
- IP masquée et trafic chiffré de bout en bout

Authentification Renouvelée Toutes les 4 Heures

- L'Entreprise n'utilise **jamais de sessions Google Workspace persistantes**
- Chaque accès à Google Workspace (Gmail, Drive, Sheets, Docs) exige une réauthentification toutes les 4 heures maximum
- Cela empêche qu'une session compromise reste active au-delà de cette période
- Mise en œuvre via les paramètres de session Google Workspace et des policies de déconnexion automatique

Gestion des Mots de Passe via 1Password

- TOUS les mots de passe professionnels sont stockés et gérés via **1Password Business Account** (Agile Bits Inc.)
- 1Password offre un chiffrage de bout en bout militaire (AES 256-bit) avec architecture zéro-knowledge
- Aucun mot de passe n'est stocké en local, en cloud sans chiffrage, ou dans un navigateur
- Chaque mot de passe est généré avec une complexité maximale et unique par service
- Authentification multi-facteurs requise pour tout accès à 1Password
- Audit trail complet de qui a accédé à quel secret, quand et pourquoi

2. Minimisation et Anonymisation des Données

- Transmission uniquement des données essentielles à la fourniture des services
- Anonymisation ou pseudo-anonymisation lorsque possible
- Suppression rapide des données sensibles inutiles
- Aucun transfert de données sensibles au-delà de ce qui est nécessaire au mandat

3. Chiffrage Fourni par Google Workspace

- L'Entreprise utilise **Google Workspace Business Premium** qui fournit :
    - Chiffrage automatique en transit (TLS 1.2+) et au repos (AES 256-bit)
    - Option de chiffrage de bout en bout pour Docs, Sheets, Drive si traitement de données très sensibles
    - DLP (Data Loss Prevention) pour détecter et prévenir les fuites
    - Conformité Google aux standards internationaux (SOC 2 Type II, ISO 27001, HIPAA)
- **Clarification** : Le chiffrage est fourni par Google Workspace. L'Entreprise n'effectue pas elle-même le chiffrage direct, mais utilise toutes les meilleures technologies et mesures de sécurité mises à disposition par Google Workspace Business Premium

4. Contrats Protecteurs

- Addenda de traitement de données (DPA) avec chaque sous-traitant (Google, Airtable, Zapier, Softr, Stripe, JotForm, Cloudflare)
- Clauses explicites exigeant que les sous-traitants notifient l'Entreprise en cas d'accès gouvernemental
- Obligations de limitation d'accès et de respect des instructions
- Audit rights pour vérification de conformité

- Durée de contrat alignée avec la période de conservation des données

5. Durée Minimale de Conservation

- Conservation limitée à la période nécessaire pour fournir les services (maximum 5 ans après fin de mandat)
- Destruction sécurisée après la période (données physiquement irrécupérables)
- Procédures documentées de suppression

6. Audit et Surveillance Continues

- Examens périodiques (annuels) de la sécurité et de la conformité
- Monitoring des accès aux données sensibles
- Registre des activités sensibles tenues dans l'Infrastructure de sécurité de Google Workspace
- Analyse régulière de la conformité EFVP

10.3 Transferts vers le Canada

Statut

Certaines données peuvent également être traitées sur des serveurs canadiens (ex. Google Workspace, Cloudflare offrent des options de localisation Canada).

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 que les États-Unis
- Risques réduits comparé aux États-Unis
- Mesures de sécurité similaires toujours appliquées
- Droit québécois et fédéral applicable et plus protecteur

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 des personnes concernées serait obtenu.

10.5 Information aux Personnes Concernées

Lors de la collecte ou du traitement de leurs données, les personnes sont informées que :

- Leurs renseignements peuvent être traités aux États-Unis et au Canada par nos

sous-traitants
- Des mesures de protection appropriées et disproportionnées sont mises en place (VPN, réauthentification, chiffrage Google, contrats DPA)
- Elles ont le droit de s'opposer à ce transfert (bien que cela puisse limiter la fourniture des services)
- En cas de question, elles peuvent contacter le RPRP

---

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, anonymisés ou archivés de manière sécurisée.

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 des services

Renseignements de Clients Anciens et Données de Mandats Complétés

- Conservés pendant **5 ans après la fin de la relation commerciale**

- Justification : Obligations légales et comptables, potentiels litiges, références futures

- **Processus d'anonymisation spéciale à fin de mandat** :

  Tous les dossiers clients sont anonymisés à la fin du mandat selon la procédure suivante :

  1. **Codification** : Tous les noms de clients, noms d'employés, données sensibles et renseignements à caractère confidentiel sont remplacés par des codes alphanumériques uniques
  2. **Clés de Décodage** : Les clés permettant de déchiffrer les codes sont conservées dans un **dossier sécurisé distinct** isolé des données anonymisées
  3. **Accès Restreint** : **Seul Teo Blanc** (RPRP) a accès au dossier contenant les clés de décodage
  4. **Protection du Dossier des Clés** : Le dossier contenant les clés est protégé

par **1Password** avec authentification multi-facteurs requise

5. **Finalité** : Ces données anonymisées peuvent servir à des fins d'analyse, amélioration des processus, ou formation, mais elles ne permettent plus d'identifier les individus concernés
6. **Conservation Sécurisée** : Les données anonymisées et les clés sont conservées séparément, sécurisées et chiffrées

Données Transactionnelles (Paiements et Facturation)

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

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 ou de consentement renouvelé 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 (Données de Clients du Client)

- 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 documentée

Registres d'Incidents et de Sécurité

- Conservés pendant **3 ans** pour fins de conformité et audit
- Après 3 ans, anonymisation ou suppression sécurisée

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 via un processus documenté
2. Une vérification est effectuée pour confirmer aucune obligation légale de rétention
3. Les données sont supprimées de manière sécurisée (suppression permanente, irrécupérable) via les outils utilisés (Google Drive, Airtable, etc.)
4. Les sauvegardes contenant les données sont également supprimées après la période de rétention des backups (généralement 6 mois après suppression primaire)
5. Un registre de suppression est tenu et documenté

---

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
- Les standards de l'industrie pour les PME de services de conseil

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

12.2 Mesures Techniques de Sécurité

12.2.1 Chiffrage et Encryptage

Chiffrage en Transit

- Chiffrage TLS 1.2+ pour toutes les communications en ligne (site web, courriels, accès aux outils)

- Certificats SSL/TLS valides pour tous les services web
- Tous les transferts de données utilisent le protocole HTTPS sécurisé

Chiffrage au Repos

- Chiffrage à repos pour données stockées dans Google Workspace (AES 256-bit automatique par Google)
- Chiffrage à repos pour données dans Airtable, Stripe, et autres outils cloud (standard de chaque fournisseur)
- Chiffrage local pour données sur appareils personnels (KeePassXC pour les accès d'urgence)
- **Clarification** : Le chiffrage au repos n'est PAS effectué directement par l'Entreprise. L'Entreprise utilise les meilleures technologies de chiffrage **fournies par Google Workspace Business Premium et nos autres sous-traitants**, qui appliquent le chiffrage de bout en bout selon leurs standards de sécurité.

Option Chiffrage Renforcé (Google Workspace)

- Pour données particulièrement sensibles, utilisation du chiffrage de bout en bout natif de Google (client-side encryption pour Docs, Sheets, Drive)
- Les clés de chiffrage restent sous le contrôle de l'Entreprise

12.2.2 Authentification et Gestion des Accès

Authentification Multi-Facteurs (MFA)

- Authentification multi-facteurs (2FA/MFA) **obligatoire** pour tous les comptes critiques :
    - Compte Google Workspace Business Premium
    - Compte 1Password
    - Compte Airtable
    - Compte Stripe
    - Compte Cloudflare
    - Tout compte accédant à des renseignements personnels

Mots de Passe Forts

- Tous les mots de passe professionnels respectent une politique de complexité stricte :
    - Minimum 16 caractères
    - Mix obligatoire : majuscules, minuscules, chiffres, caractères spéciaux
    - Pas de mots du dictionnaire
    - Pas de réutilisation entre services
- **Aucun mot de passe n'est partagé entre services différents**

- **Tous les mots de passe sont gérés via 1Password** (pas de sauvegarde locale en texte clair)

Réauthentification Obligatoire Toutes les 4 Heures

- **Sessions Google Workspace : Durée maximale 4 heures**
    - Aucune session persistante sur Google Workspace
    - Déconnexion automatique après 4 heures d'inactivité/d'accès
    - Réauthentification obligatoire pour continuer le travail
    - Cela prévient qu'une session compromise reste active au-delà de ce laps de temps
- Cette mesure s'ajoute à la présence du **Cloudflare WARP VPN** qui isole le trafic en amont

Gestion Sécurisée des Mots de Passe

- Utilisation de **1Password Business Premium** pour tous les mots de passe professionnels
- Chiffrage end-to-end militaire (AES 256-bit)
- Zéro-knowledge : 1Password n'a jamais accès aux données non chiffrées
- Audit trails complets de tous les accès
- Authentification multi-facteurs requise pour accéder à 1Password
- Partage sécurisé de secrets selon le besoin (future délégation si croissance)

KeePassXC pour Accès d'Urgence

- Gestionnaire de mots de passe local pour accès d'urgence uniquement
- Chiffrage fort local, aucune transmission cloud
- Utilisé uniquement si 1Password devient indisponible
- Stocké et sécurisé sur appareil personnel uniquement

12.2.3 Contrôle d'Accès et Audit

Principe du Moindre Privilège

- Accès accordé uniquement selon le principe du « moindre privilège »
- Seul accès nécessaire à chaque rôle / fonction
- Révocation immédiate d'accès en cas de cessation de service (actuellement N/A pour entreprise individuelle)

Rôles Utilisateur dans Google Workspace

- Administrateur (contrôle complet) : Teo Blanc uniquement
- Éditeur (modification de documents) : Restreint

- Visualisateur (lecture seule) : Pour consultants externes si applicable
- Lecteur seul : Pour accès en lecture aux documents partagés

Audit Trails

- Tous les accès aux outils contenant des renseignements personnels sont tracés :
    - Google Workspace Audit Logs
    - Airtable Activity History
    - Stripe Logs
    - Cloudflare Logs
- Consultation régulière des audit trails pour détecter les activités anormales

12.2.4 Sécurité Réseau

VPN Cloudflare WARP Obligatoire

- **Utilisation obligatoire du VPN Cloudflare WARP pour tout accès à distance** aux outils contenant des renseignements personnels
- WARP fournit :
    - Tunnel VPN chiffré (Wireguard Protocol)
    - Masquage de l'adresse IP réelle
    - Chiffrage de bout en bout du trafic
    - Protection contre les écoutes et interceptions
    - Routage sécurisé via les serveurs Cloudflare mondiaux
- **Aucun accès sans VPN** depuis réseau domestique, Wi-Fi public ou réseau tiers

Restrictions d'Accès Réseau

- Aucun accès direct depuis réseaux Wi-Fi publics sans VPN (bibliothèques, cafés, aéroports, etc.)
- Connexion par réseau Wi-Fi privée sécurisé (WPA3 si possible) ou connexion filaire
- Utilisation de VPN WARP même sur réseau Wi-Fi privé pour couche de sécurité additionnelle

Firewall et Protection Web

- Cloudflare fournit :
    - Filtrage DDoS automatique
    - WAF (Web Application Firewall) pour protection contre attaques web courantes
    - Blocage de trafic malveillant en amont
    - Protection des points de terminaison

12.2.5 Sauvegarde et Récupération

Sauvegardes Automatiques

- Google Workspace effectue des sauvegardes automatiques et continues (built-in)
- Données accessibles jusqu'à 30 jours après suppression
- Airtable inclut des sauvegardes et versions d'historique
- Tests périodiques de restauration effectués annuellement

Stockage de Sauvegarde Redondant

- Sauvegardes stockées en local et en cloud
- Redondance géographique via infrastructures Google et Cloudflare
- Récupération possible même en cas de défaillance matérielle

Plan de Continuité et de Récupération

- Documenté pour accès à services critiques en cas de sinistre
- Procédures pour restauration de données de clients
- Tests annuels de plan de continuité

12.3 Mesures Organisationnelles de Sécurité

12.3.1 Politiques et Procédures

Politique d'Utilisation Acceptable

- Ressources informatiques utilisées uniquement à des fins professionnelles légitimes
- Pas d'utilisation personnelle excessive
- Pas de stockage de données personnelles ou non liées à l'entreprise sur les outils

Procédures d'Onboarding et Offboarding

- À l'onboarding : Création de comptes, attribution d'accès, formation sécurité
- À l'offboarding : Révocation immédiate d'accès, récupération de matériel, archivage de données

Procédures de Gestion des Incidents de Confidentialité

- Documentées et testées régulièrement
- Processus de notification aux personnes affectées et à la CAI
- Voir section 14 pour détails complets

Procédures de Suppression de Données

- Suppression complète et irréversible après période de conservation
- Audit de suppression documenté
- Notification au client (si applicable) que les données ont été supprimées

12.3.2 Formation et Sensibilisation

Formation Annuelle

- Formation annuelle obligatoire en protection des données et sécurité informatique
- Contenu : Risques de phishing, ingénierie sociale, meilleures pratiques de mots de passe, gestion des secrets, incident reporting
- Documentation de participation

Sensibilisation Continue

- Rappels réguliers sur les bonnes pratiques de sécurité
- Alertes en cas de menace détectée
- Mise à jour de la politique quand changements majeurs

Protocols en Cas d'Incident

- Procédure claire de rapportage interne
- Escalade automatique si gravité élevée
- Communication rapide aux personnes affectées

12.3.3 Limitation de l'Accès aux Données Sensibles

Principe de Localisation

- **Aucune donnée sensible ou renseignements personnels n'est stockée localement** sur l'appareil personnel
- Stockage exclusif en cloud : Google Workspace, Airtable, Softr, etc.
- Téléchargement temporaire autorisé UNIQUEMENT pour travail immédiat et avec chiffrage

Partage de Données Sécurisé

- Partage via liens sécurisés avec expiration de validité
- Pas de copie locale des documents sensibles
- Permissions granulaires : lecture seule, édition restreinte, etc.

Documenter les Accès

- Registre tenu à jour de toute personne ayant accès à données sensibles
- Justification documentée pour chaque accès
- Révocation immédiate quand accès n'est plus nécessaire

12.3.4 Évaluation et Audit

Évaluations Périodiques (Annuelles)

- Audit annuel de conformité à cette politique
- Vérification que mesures de sécurité sont réellement implémentées
- Évaluation des Facteurs Relatifs à la Vie Privée (EFVP) pour nouveaux outils / traitements

Vérifications de Sécurité Informatique

- Contrôles de sécurité : firewall, antivirus, patches, certificats SSL
- Monitoring actif des audit trails
- Alertes configurées pour activités suspectes

Tests de Pénétration (si applicable)

- Envisagés si expansion et volumes de données croissent significativement
- Actuellement non prioritaires pour entreprise individuelle

Audits de Conformité Loi 25

- Audit annuel de conformité aux dispositions de la Loi 25
- Vérification du registre d'incidents
- Vérification de l'applicabilité des EFVP

12.4 Mesures Spécifiques par Type de Données

Données Hautement Sensibles (ex. numéros bancaires, assurance sociale, données médicales)

- Chiffrage fort (AES 256-bit)
- Accès très limité (uniquement si strictement nécessaire au mandat)
- Audit trail détaillé de tout accès
- Suppression rapide dès que inutile

Données Sensibles (ex. noms, adresses, numéros de téléphone, adresses courriel)

- Chiffrage standard (TLS en transit, AES au repos)
- Contrôle d'accès basé sur les rôles

- Audit trail de tous les accès
- Conservation selon la durée prévue

Données Non Sensibles (ex. informations publiques, données anonymisées)

- Sécurité de base (HTTPS, authentification)
- Audit occasionnel
- Destruction selon calendrier

12.5 Appareils et Travail à Distance

Sécurité des Appareils Personnels

- Antivirus et firewall personnel **obligatoires** et à jour
- Mises à jour de sécurité système effectuées régulièrement (OS patches)
- Verrouillage automatique après 15 minutes d'inactivité (password + face/empreinte si possible)
- Chiffrage du disque dur complet (BitLocker, FileVault, ou équivalent)

Aucun Stockage Local de Données Sensibles

- Données sensibles / confidentielles **JAMAIS** stockées localement en clair
- Stockage exclusif en cloud chiffré (Google Workspace, Airtable, Softr)
- Téléchargement temporaire autorisé seulement pour travail immédiat et avec chiffrage supplémentaire
- Suppression immédiate de l'appareil après utilisation (pas de résidu)
- Pas de fichiers de travail laissés sur le disque local

Travail à Distance et Sécurité du Réseau

- **VPN Cloudflare WARP obligatoire** si accès depuis domicile, établissements publics ou lieux externes
- Connexion Wi-Fi privée sécurisée (WPA3 si possible) - pas d'accès depuis Wi-Fi public sans VPN
- Écran de veille avec mot de passe obligatoire après 15–20 minutes d'inactivité
- Pas de partage d'écran avec données sensibles visibles (notamment en réunion vidéo publique)

12.6 Accès des Sous-traitants

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

- Met en place des mesures de sécurité appropriées (SOC 2 Type II, ISO 27001, ou équivalent)
- Restreint l'accès aux données strictement au nécessaire
- Notifie immédiatement l'Entreprise en cas d'incident

- Permet des audits de sécurité périodiques
- Respecte les instructions de l'Entreprise et les contrats DPA

12.7 Gouvernance Interne de la Sécurité

L'Entreprise s'est dotée de **procédures internes de gouvernance des renseignements personnels** :

- **Registre des incidents** tenu à jour selon les exigences de la Loi 25
- **Procédure EFVP** pour évaluation des risques avant l'introduction de nouveaux outils ou traitements
- **Procédure d'onboarding/offboarding** pour gestion des accès et suppression des données
- **Procédure de gestion des demandes de droits** (accès, rectification, suppression, portabilité, désindexation)
- **Procédure d'audit annuel** de conformité

Ces procédures peuvent être mises à disposition de la Commission d'accès à l'information (CAI) sur demande légale.

---

13. DROITS DES PERSONNES CONCERNÉES

13.1 Droits Reconnus par la Loi 25 et PIPEDA

Les personnes dont l'Entreprise détient des renseignements personnels disposent des droits suivants en vertu de la Loi 25 et, le cas échéant, de la PIPEDA.

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 ou par courriel fournie à la section 16
2. Inclure suffisamment d'information pour identifier la demande (nom, adresses courriel, période pertinente, projet, etc.)
3. L'Entreprise dispose de **30 jours** pour répondre (prolongeable de 60 jours en cas de complexité exceptionnelle)
4. La communication sera faite de manière sécurisée (lien sécurisé avec expiration, mot de passe, ou remise en personne)
5. **Aucun frais applicable** 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
- Droit de rectification, suppression, portabilité, désindexation

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. Si les parties ne s'accordent pas, une note explicative sera ajoutée 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 ou contreviennent à la loi

Cas où la Suppression Peut Être Refusée

- Les renseignements sont requis pour conformité légale (ex. comptabilité, litiges)
- Un litige est en cours et les données sont pertinentes
- Contrat avec client spécifie la rétention des données
- Obligations comptables ou fiscales exigent la conservation

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

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
- Format technique standard : CSV, JSON, XML, Excel ou autre format lisible

Données NON Concernées

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

Comment Exercer ce Droit

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

13.6 Droit à la Désindexation et à la Cessation de Diffusion

Conformément à l'article 28.1 de la Loi 25, une personne peut demander à l'Entreprise de :

- **Cesser de diffuser** un renseignement personnel la concernant
- **Désindexer** tout hyperlien rattaché à son nom donnant accès à ce renseignement
- **Cesser la réindexation** du renseignement

Ceci est applicable lorsque la diffusion du renseignement :

- Lui cause un préjudice grave (atteinte à réputation, privacy, dignité, bien-être)
- Contrevient à la loi ou à une ordonnance judiciaire
- N'est plus pertinent ou approprié dans le contexte actuel

Comment Exercer ce Droit

1. Demande écrite au RPRP décrivant le renseignement et le préjudice causé
2. L'Entreprise analysera la demande dans les **30 jours**
3. Si approuvée :
    - Cessation immédiate de la diffusion
    - Désindexation de tout lien associé au nom
    - Notification à la personne
4. Si refusée :
    - Justification écrite fournie à la personne
    - Droit de contester auprès de la CAI

13.7 Droit de Retrait du Consentement

Une 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**
4. Traitement immédiat (cessation des traitements affiliés)

13.8 Droit de S'Opposer

La personne peut s'opposer au traitement de ses renseignements pour certaines fins, notamment :

- Marketing direct et communications promotionnelles
- Profilage et analyse comportementale à des fins de marketing
- Utilisation pour fins secondaires non liées à la fin principale

Comment Exercer

1. Communiquer opposition au RPRP
2. Respecté immédiatement pour nouvelles communications de marketing
3. Cessation de l'envoi de messages promotionnels dans les **10 jours ouvrables** (conforme à LCAP)

13.9 Droit à l'Explication en Cas de Décisions Automatisées

Si l'Entreprise prenait des décisions basées exclusivement sur le traitement automatisé

(ex. algorithmes, scoring, profilage décisionnel), les personnes auraient le droit à une explication compréhensible.

Situation Actuelle : À date, l'Entreprise ne prend pas de décisions significatives basées exclusivement sur traitement automatisé. Cette disposition demeure pertinente si changement futur dans les services offerts.

13.10 Exercice des Droits — Modalités Générales

Modalités Générales

- Droits exercés par demande écrite au RPRP aux coordonnées fournies en section 16
- Peuvent être exercés **gratuitement** sauf cas manifestement abusif ou exagéré
- **Délais standard de réponse** : 30 jours (prolongeable de 60 jours si complexité ou volume)
- **Pas de discrimination** à l'encontre de la personne ayant exercé un droit

Identification et Vérification

- L'Entreprise peut demander une preuve d'identité raisonnable pour vérifier que la demande provient bien de la personne concernée
- Vérification effectuée de manière confidentielle et sécurisée
- Protéger la confidentialité des données personnelles lors de la vérification

Communication des Réponses

- Réponses fournies par écrit de manière sécurisée
- Utilisation de lien sécurisé avec expiration, mot de passe, ou remise en personne
- Confirmation écrite de la completion de la demande

---

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, notamment :

- 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 à un tiers
- Perte d'un renseignement personnel (suppression accidentelle, perte de matériel)
- Vol, destruction ou dommage à renseignements personnels

- Altération ou corruption de renseignements personnels
- Toute autre atteinte à la confidentialité, l'intégrité ou la disponibilité d'un renseignement

14.2 Procédure de Rapportage Interne

Dès la découverte d'un incident soupçonné :

1. **Rapportage immédiat** au RPRP (Teo Blanc)
2. **Documentation** :
    - Date et heure de découverte
    - Description détaillée de l'incident
    - Type de données impliquées
    - Nombre de personnes potentiellement affectées
    - Cause présumée (erreur, attaque, perte de matériel, etc.)
    - Mesures d'urgence prises immédiatement
3. **Isolement** de la source si possible pour prévenir propagation
4. **Notification aux sous-traitants** (si incident chez eux) pour vérification et confirmation

14.3 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 / financières = très grave
    - Données d'identité = grave
    - Données de contact = moins grave
    - Données anonymisées = pas de préjudice sérieux
- **Type de personne affectée** :
    - Mineurs = considération spéciale accrue
    - Personnes vulnérables = considération accrue
    - Adultes en général = évaluation standard
- **Étendue de l'incident** :
    - 1 personne = préjudice potentiel limité
    - Milliers de personnes = préjudice potentiel massif
- **Probabilité d'utilisation malveillante** :
    - Accès accidentel par employé (faible)
    - Vol de données (très élevé)
    - Attaque externe (très élevé)
- **Mesures de protection en place** :
    - Données chiffrées = réduction du risque

    - Données lisibles en clair = risque complet
- **Conséquences potentielles** :
    - Identité ou fraude financière = grave
    - Discrimination ou stigmatisation = grave
    - Pertes financières = grave
    - Atteinte à réputation ou dignité = grave
    - Dommages émotionnels ou psychologiques = grave
    - Inconvénience mineur = pas grave

14.4 Registre des Incidents Tenu Conforme à la Loi 25

L'Entreprise tient un **registre documenté des incidents de confidentialité** exactement comme l'exige la Loi 25, comprenant :

- **Date et heure** de découverte
- **Description détaillée** de l'incident
- **Type et sensibilité** des renseignements impliqués
- **Nombre de personnes** potentiellement affectées (ou estimation)
- **Cause probable** (erreur, attaque, perte, configuration, etc.)
- **Évaluation du risque** de préjudice sérieux
- **Mesures immédiates** prises (confinement, alertes, etc.)
- **Mesures de remédiation** appliquées
- **Notifications effectuées** (CAI, personnes, sous-traitants, etc.)
- **Date de fermeture** de l'incident
- **Observations** (améliorations recommandées)

Ce registre est **conservé pendant 3 ans** à partir de la date de fermeture de l'incident, puis anonymisé ou supprimé.

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

Si l'incident présente un **risque de préjudice sérieux**, l'Entreprise notifie la **Commission d'accès à l'information** du Québec dans les **délais impartis par la loi** (généralement rapidement, sauf circonstances exceptionnelles).

Contenu de la Notification à la CAI

- Description de l'incident
- Type et sensibilité des renseignements
- Nombre de personnes affectées
- Évaluation du risque de préjudice sérieux
- Mesures correctives prises
- Mesures de prévention future

14.6 Notification aux Personnes Concernées

Si le risque de préjudice sérieux est confirmé, l'Entreprise notifie **directement les personnes concernées** de :

- La nature de l'incident
- Les renseignements impliqués
- Les risques potentiels
- Les mesures de prévention et de remédiation prises
- Les coordonnées du RPRP pour questions supplémentaires

Timing : Notification effectuée **sans délai injustifié** (généralement dans les 5–10 jours ouvrables après confirmation du risque).

Méthode : Notification par courriel sécurisé, courrier recommandé ou appel téléphonique selon la gravité et les coordonnées disponibles.

14.7 Amélioration Continue Post-Incident

Suite à tout incident, l'Entreprise :

1. Effectue une **analyse de cause racine** pour identifier pourquoi l'incident s'est produit
2. Identifie des **mesures préventives** pour éviter récurrence
3. Met à jour les **procédures de sécurité** si nécessaire
4. Assure une **formation additionnelle** si l'incident résultait d'une erreur humaine
5. Teste la mise en œuvre des corrections
6. Documente les leçons apprises

14.8 Incidents NON Critiques (Pas de Préjudice Sérieux)

Certains incidents peuvent ne pas présenter un risque de préjudice sérieux. Exemples :

- Accès accidentel non malveillant à renseignements par un employé interne
- Perte de données chiffrées (cryptage empêche usage)
- Données anonymisées perdues (pas d'identification possible)
- Incident de courte durée rapidement contenu et sans usage malveillant

Ces incidents sont :

- Documentés dans le registre
- Évalués mais classés comme « risque faible »
- NON notifiés à la CAI ou aux personnes (à moins que loi spécifique ne l'exige)
- Utilisés pour amélioration continue interne

---

15. MODIFICATIONS DE LA POLITIQUE

L'Entreprise se réserve le droit de modifier la présente politique en tout temps pour refléter :

- Changements dans les technologies utilisées
- Changements dans les exigences légales ou réglementaires
- Amélioration des pratiques de protection des données
- Feedback des personnes concernées

Notification des Modifications

- Les modifications majeures sont communiquées aux personnes concernées via le site ou par courriel
- Une notification claire indique la date d'entrée en vigueur
- Version antérieure reste accessible sur demande
- Entrée en vigueur de la nouvelle version : généralement 30 jours après publication

---

16. COORDONNÉES POUR QUESTIONS OU RÉCLAMATIONS

Toute personne ayant une question, préoccupation ou désir d'exercer ses droits peut communiquer avec :

Responsable de la Protection des Renseignements Personnels (RPRP)

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

Délais de Réponse : Réponse fournie dans les **10 jours ouvrables** pour questions générales, et dans les **30 jours** pour demandes formelles de droits (prolongeable à 60 jours si complexité).

Commission d'Accès à l'Information du Québec (CAI)

En cas de non-satisfaction avec la réponse de l'Entreprise, une personne peut soumettre une plainte à :

- **Commission d'accès à l'information du Québec (CAI)**
- Adresse : 1045, boulevard de la Chaudière, Québec (Québec) G1R 5E5

- Téléphone : 1-888-528-8668 (sans frais) ou (418) 528-7741
- Courriel : protectionrenseignements@cai.gouv.qc.ca
- Site web : https://www.cai.gouv.qc.ca

La CAI est l'organisme de régulation indépendant responsable de l'application de la Loi 25 au Québec.

CONCLUSION

Teo Support s'engage à respecter la présente politique et à protéger les renseignements personnels de ses clients, prospects et partenaires. La protection des données est une priorité et demeure au cœur de nos opérations.

Toute question relative à cette politique ou à la protection des renseignements personnels est bienvenue et sera traitée avec diligence.

Dernière mise à jour : janvier 2026

GLOSSAIRE

- **EFVP** : Évaluation des Facteurs Relatifs à la Vie Privée — document d'analyse des risques avant traitement transfrontalier
- **RPRP** : Responsable de la Protection des Renseignements Personnels
- **DPA** : Data Processing Addendum — contrat entre responsable et sous-traitant
- **PIPEDA** : Loi fédérale canadienne sur la protection des renseignements personnels et documents électroniques
- **LCAP** : Loi canadienne anti-pourriel
- **CAI** : Commission d'accès à l'information du Québec
- **SOC 2** : Service Organization Control 2 — certification de sécurité des services cloud
- **ISO 27001** : Norme internationale de gestion de la sécurité de l'information
- **TLS/SSL** : Protocole de chiffrage pour communications sécurisées
- **VPN** : Réseau privé virtuel
- **MFA/2FA** : Authentification multi-facteurs / double authentification
- **AES** : Advanced Encryption Standard — algorithme de chiffrage
- **Wireguard** : Protocole VPN léger et performant
- **DLP** : Data Loss Prevention — prévention des fuites de données
- **WAF** : Web Application Firewall — pare-feu applicatif
- **Chiffrage de bout en bout** : Chiffrage où les clés restent uniquement chez l'expéditeur et le destinataire

- **Zéro-knowledge** : Architecture où le fournisseur n'a jamais accès aux données non chiffrées