

Politique de protection des données

Les services Stelvar S.E.N.C.

Dernière mise à jour : 18 juillet 2026

1. Objectif de la politique

Les services Stelvar S.E.N.C. (« Stelvar ») reconnaît l'importance de protéger les renseignements qui lui sont confiés par ses clients, partenaires et utilisateurs.

La présente politique décrit les mesures et les principes appliqués par Stelvar afin d'assurer :

- la sécurité des renseignements;
- la confidentialité des données;
- la réduction des risques liés aux incidents de sécurité;
- la protection des informations appartenant aux clients.

Cette politique vise à démontrer l'engagement de Stelvar envers une gestion responsable des renseignements utilisés dans le cadre de ses services.

2. Approche Privacy by Design

Stelvar applique une approche de protection des renseignements personnels intégrée dès la conception de ses services.

Cette approche repose notamment sur les principes suivants :

Collecte minimale des données

Stelvar collecte uniquement les renseignements nécessaires au fonctionnement de ses services.

Les données sont principalement utilisées pour :

- gérer les comptes clients;
- fournir l'accès au portail;
- calculer les statistiques liées aux cartes NFC;
- assurer le fonctionnement du service.

Accès limité

L'accès aux données est limité aux personnes autorisées qui en ont besoin dans le cadre de leurs responsabilités.

Conservation raisonnable

Les données sont conservées uniquement pendant la période nécessaire au fonctionnement du service et au respect des obligations applicables.

Sécurité intégrée

Des mesures de sécurité sont intégrées dans l'architecture technique de Stelvar afin de protéger les informations contre les accès non autorisés.

3. Classification des données

Afin d'assurer une gestion appropriée des renseignements, Stelvar catégorise les données traitées selon leur nature.

3.1 Données commerciales

Ces données concernent les entreprises clientes.

Elles peuvent inclure :

- nom de l'entreprise;
- adresse courriel;
- ville;
- informations liées au forfait;
- informations nécessaires à la gestion du compte.

3.2 Données statistiques

Ces données permettent aux clients de mesurer la performance de leurs cartes NFC.

Elles peuvent inclure :

- nombre de scans;
- dates des interactions;
- heures des interactions;
- taux de conversion;
- statistiques liées à l'utilisation des cartes.

3.3 Données Google Business Profile

Lorsque le client connecte son profil Google Business, Stelvar peut traiter certaines informations provenant de l'API officielle Google Business Profile.

Ces informations peuvent inclure :

- nombre d'étoiles;
- nombre d'avis.

Ces informations sont utilisées uniquement pour fournir les fonctionnalités statistiques du portail.

3.4 Données techniques

Ces données concernent principalement le fonctionnement et la sécurité de la plateforme.

Elles peuvent inclure :

- journaux techniques;
- informations nécessaires à la sécurité;
- données utilisées pour l'administration du système.

Ces informations sont accessibles uniquement aux comptes administrateurs autorisés.

4. Contrôle des accès

Stelvar applique un principe de limitation des accès.

Les personnes autorisées pouvant accéder aux données sont actuellement :

- Justin Picard;
- Charles-Olivier Sarazin.

Les accès sont utilisés uniquement pour :

- administration du service;
- soutien aux clients;
- maintenance;
- résolution de problèmes techniques;
- gestion des comptes.

Aucune personne externe non autorisée n'a accès aux données clients.

5. Sécurité technique

Stelvar utilise différentes mesures afin de protéger ses systèmes.

Protection des communications

Les communications entre les utilisateurs et les services Stelvar sont protégées par HTTPS.

Protection des comptes

Les mesures comprennent notamment :

- stockage sécurisé des mots de passe sous forme hachée;
- contrôle des accès utilisateurs;
- limitation de l'accès administratif.

Les comptes administrateurs utilisent actuellement une authentification par mot de passe.

Protection des données

Les données stockées dans la base de données Stelvar sont chiffrées afin de réduire les risques d'accès non autorisé.

6. Infrastructure et fournisseurs externes

Afin d'assurer le fonctionnement de ses services, Stelvar utilise certains fournisseurs technologiques.

Bluehost

Utilisé pour l'hébergement de l'infrastructure Stelvar.

Cloudflare

Utilisé pour certaines fonctions de protection réseau et de sécurité.

Stripe

Utilisé pour le traitement des paiements.

Stelvar ne conserve pas les informations complètes de cartes bancaires.

Google

Utilisé notamment pour :

- Google Business Profile API;
- certaines fonctionnalités analytiques.

Titan Email

Utilisé pour les communications électroniques.

7. Sauvegardes et récupération

Stelvar effectue des sauvegardes manuelles de ses données afin de permettre une récupération en cas de problème technique.

Les sauvegardes permettent notamment de réduire les risques liés :

- aux erreurs techniques;
- aux pertes accidentelles;
- aux problèmes d'infrastructure.

Stelvar pourra faire évoluer ses pratiques de sauvegarde selon l'évolution de ses besoins opérationnels.

8. Gestion des incidents de sécurité

Dans l'éventualité d'un incident pouvant affecter la sécurité des données, Stelvar applique une démarche structurée comprenant :

1. Détection

Identification de l'incident ou de la vulnérabilité.

2. Analyse

Évaluation de la nature du problème et des données potentiellement concernées.

3. Contention

Mesures prises afin de limiter les impacts.

4. Correction

Mise en place de correctifs afin d'éviter la répétition du problème.

5. Évaluation des obligations

Analyse des obligations applicables concernant la notification des personnes concernées ou des autorités compétentes.

6. Communication

Communication lorsque nécessaire selon la nature de l'incident.

9. Conservation des données

Stelvar conserve les données aussi longtemps que nécessaire pour :

- fournir ses services;
- maintenir les comptes clients;
- respecter les obligations légales applicables;
- résoudre les différends;
- appliquer les ententes contractuelles.

La durée de conservation peut varier selon la nature des informations concernées.

10. Suppression des données

Les clients peuvent demander la suppression de leurs renseignements personnels.

Toute demande sera traitée selon le processus suivant :

- 1. Réception de la demande.
- 2. Vérification de l'identité du demandeur.
- 3. Analyse des données pouvant être supprimées.
- 4. Suppression lorsque possible.

Certaines données peuvent devoir être conservées lorsque cela est nécessaire pour :

- respecter une obligation légale;
- conserver des preuves administratives;
- gérer des obligations contractuelles.

11. Responsabilités internes

Les personnes ayant accès aux données Stelvar doivent :

- protéger la confidentialité des informations;
- utiliser les données uniquement dans le cadre professionnel;

- éviter tout accès inutile;
- respecter les mesures de sécurité établies.

Les accès sont limités afin de réduire les risques d'utilisation abusive.

12. Révision de la politique

Stelvar peut modifier cette politique afin de refléter :

- l'évolution technologique;
- l'amélioration des pratiques internes;
- l'évolution des services;
- les changements législatifs applicables.

La version la plus récente de cette politique représente les pratiques actuelles de Stelvar.

Contact

Les services Stelvar S.E.N.C.

Courriel :

contact@stelvar.ca