

Data Protection Policy

Les services Stelvar S.E.N.C.

Last updated: July 18, 2026

1. Purpose of the policy

Les services Stelvar S.E.N.C. ("Stelvar") recognizes the importance of protecting the information entrusted to it by its clients, partners and users.

This policy describes the measures and principles applied by Stelvar in order to ensure:

- the security of the information;
- the confidentiality of the data;
- the reduction of risks related to security incidents;
- the protection of information belonging to clients.

This policy aims to demonstrate Stelvar's commitment to responsible management of the information used in the course of its services.

2. Privacy by Design approach

Stelvar applies an approach to the protection of personal information that is integrated from the design stage of its services.

This approach is based, in particular, on the following principles:

Minimal data collection

Stelvar collects only the information necessary for the operation of its services.

The data is mainly used to:

- manage client accounts;
- provide access to the portal;
- calculate the statistics related to the NFC cards;
- ensure the operation of the service.

Limited access

Access to the data is limited to authorized persons who need it in the course of their responsibilities.

Reasonable retention

The data is retained only for the period necessary for the operation of the service and for compliance with the applicable obligations.

Built-in security

Security measures are built into Stelvar's technical architecture in order to protect the information against unauthorized access.

3. Data classification

In order to ensure appropriate management of the information, Stelvar categorizes the data it processes according to its nature.

3.1 Commercial data

This data concerns the client businesses.

It may include:

- business name;
- email address;
- city;
- information related to the plan;
- information required for account management.

3.2 Statistical data

This data allows clients to measure the performance of their NFC cards.

It may include:

- number of scans;
- dates of interactions;
- times of interactions;
- conversion rate;
- statistics related to card usage.

3.3 Google Business Profile data

When the client connects their Google Business profile, Stelvar may process certain information coming from the official Google Business Profile API.

This information may include:

- number of stars;
- number of reviews.

This information is used only to provide the statistical features of the portal.

3.4 Technical data

This data mainly concerns the operation and security of the platform.

It may include:

- technical logs;
- information required for security;
- data used for system administration.

This information is accessible only to authorized administrator accounts.

4. Access control

Stelvar applies a principle of access limitation.

The authorized persons who may access the data are currently:

- Justin Picard;
- Charles-Olivier Sarazin.

Access is used only for:

- administration of the service;
- client support;
- maintenance;
- resolution of technical problems;
- account management.

No unauthorized external person has access to client data.

5. Technical security

Stelvar uses various measures in order to protect its systems.

Protection of communications

Communications between users and the Stelvar services are protected by HTTPS.

Account protection

The measures include, in particular:

- secure storage of passwords in hashed form;
- control of user access;
- limitation of administrative access.

Administrator accounts currently use password authentication.

Data protection

The data stored in the Stelvar database is encrypted in order to reduce the risks of unauthorized access.

6. Infrastructure and external providers

In order to ensure the operation of its services, Stelvar uses certain technology providers.

Bluehost

Used for hosting the Stelvar infrastructure.

Cloudflare

Used for certain network protection and security functions.

Stripe

Used for payment processing.

Stelvar does not retain complete bank card information.

Google

Used notably for:

- Google Business Profile API;
- certain analytical features.

Titan Email

Used for electronic communications.

7. Backups and recovery

Stelvar performs manual backups of its data in order to enable recovery in the event of a technical problem.

The backups notably help reduce the risks related to:

- technical errors;
- accidental losses;
- infrastructure problems.

Stelvar may develop its backup practices according to the evolution of its operational needs.

8. Management of security incidents

In the event of an incident that could affect the security of the data, Stelvar applies a structured process comprising:

1. Detection

Identification of the incident or the vulnerability.

2. Analysis

Assessment of the nature of the problem and of the data potentially concerned.

3. Containment

Measures taken in order to limit the impacts.

4. Correction

Implementation of fixes in order to prevent the problem from recurring.

5. Assessment of obligations

Analysis of the applicable obligations concerning the notification of the persons concerned or of the competent authorities.

6. Communication

Communication when necessary according to the nature of the incident.

9. Data retention

Stelvar retains data for as long as necessary in order to:

- provide its services;
- maintain client accounts;
- comply with the applicable legal obligations;
- resolve disputes;
- enforce contractual agreements.

The retention period may vary according to the nature of the information concerned.

10. Data deletion

Clients may request the deletion of their personal information.

Any request will be handled according to the following process:

- 1. Receipt of the request.
- 2. Verification of the identity of the requester.
- 3. Analysis of the data that can be deleted.
- 4. Deletion when possible.

Certain data may need to be retained when this is necessary in order to:

- comply with a legal obligation;
- preserve administrative evidence;
- manage contractual obligations.

11. Internal responsibilities

Persons who have access to Stelvar data must:

- protect the confidentiality of the information;
- use the data only within a professional context;
- avoid any unnecessary access;

- comply with the established security measures.

Access is limited in order to reduce the risks of abusive use.

12. Revision of the policy

Stelvar may modify this policy in order to reflect:

- technological evolution;
- the improvement of internal practices;
- the evolution of the services;
- applicable legislative changes.

The most recent version of this policy represents Stelvar's current practices.

Contact

Les services Stelvar S.E.N.C.

Email:

contact@stelvar.ca