Security Policy — Sotagle

Sotagle implements reasonable technical and organizational security measures to protect user data and third-party platform integrations.

Credential and Token Protection

- API keys, access tokens, and third-party platform credentials are stored securely
- Credentials are not stored in public repositories
- Tokens for each user and store are logically separated

Encryption and Transport Security

- Data communication uses encrypted connections (HTTPS/TLS)
- Sensitive data is protected using appropriate encryption methods when required

Access Control

- System access is restricted to authorized personnel only
- Role-based access controls are applied where available

Logging and Monitoring

- System activities are logged for auditing and security purposes
- Sensitive data is not displayed in logs

Use of Third-Party Tools

Sotagle may use third-party tools for analytics, market research, AI processing, or system monitoring. Data access through these tools:

- Is limited to functional requirements
- Does not include irrelevant access
- Follows the security and privacy policies of the respective providers

Incident Handling

In the event of a security incident:

- We will conduct an internal investigation
- Access or tokens may be rotated
- Users will be notified if necessary

Data Minimization

We only collect and process data that is relevant to providing the services.