**DATA PROCESSING AGREEMENT (DPA)** *Last updated: 02/04/2026*

This Data Processing Agreement ("**DPA**") forms part of the Terms of Service ("**Agreement**") between **SecureSpells OÜ**, a company incorporated in Estonia with registry code **17318386** ("**Processor**" or "**SecureSpells**"), and the user or entity acting as the Data Controller ("**Controller**" or "**Customer**").

# 1. DEFINITIONS

- **"Services"** means the GDPR compliance auditing, website scanning, and risk scoring services provided by SecureSpells.
- **"Personal Data"** means any information relating to an identified or identifiable natural person processed by SecureSpells on behalf of the Controller.
- **"Sub-processor"** means any third party appointed by SecureSpells to process Personal Data (e.g., Postmark, Stripe).
- **"Data Protection Laws"** means the EU General Data Protection Regulation (GDPR) 2016/679 and any applicable national implementing laws.

# 2. SCOPE AND ROLES

2.1 Roles. The parties acknowledge that regarding the processing of Personal Data associated with Website Scans and Agency Member management, Customer is the Controller and SecureSpells is the Processor.
2.2 Scope. This DPA applies to the processing of Personal Data extracted from URLs submitted for scanning and Agency Member details managed within the SecureSpells platform.

# 3. PROCESSING OF PERSONAL DATA

3.1 Instructions. SecureSpells shall process Personal Data only on the documented instructions of the Controller, which are constituted by the Controller's use of the API, Dashboard, and scanning tools, unless required to do so by Union or Member State law.
3.2 Confidentiality. SecureSpells ensures that persons authorized to process the Personal Data (staff/contractors) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

# 4. SECURITY MEASURES

4.1 Technical and Organizational Measures. SecureSpells shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including encryption of personal data at rest and in transit, as detailed in Annex II.
4.2 Review. SecureSpells regularly tests, assesses, and evaluates the effectiveness of technical and organizational measures for ensuring the security of the processing.

# 5. SUB-PROCESSING

5.1 Authorized Sub-processors. The Controller generally authorizes SecureSpells to engage the Sub-processors listed in Annex III to provide specific functionalities (Email, Billing, Infrastructure).
5.2 Changes. SecureSpells will inform the Controller of any intended changes concerning the addition or replacement of other processors via email or dashboard notification, giving the Controller the opportunity to object.
5.3 Liability. SecureSpells remains fully liable to the Controller for the performance of the Sub-processor's obligations.

# 6. DATA SUBJECT RIGHTS

6.1 Assistance. Taking into account the nature of the processing, SecureSpells assists the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller's obligation to respond to requests for exercising the data subject's rights (e.g., access, rectification, erasure).
6.2 Technical Capabilities. SecureSpells provides automated tools for:

- **Data Export:** JSON and CSV exports of user data and scan history.
- **Deletion:** API endpoints and interface options for account deletion.

# 7. PERSONAL DATA BREACH

7.1 Notification. SecureSpells shall notify the Controller without undue delay after becoming aware of a Personal Data breach affecting the Controller's data.
7.2 Content. Such notification shall describe the nature of the breach, the categories of data involved, and measures taken or proposed to mitigate the breach.

# 8. DELETION AND RETURN OF DATA

8.1 Term. Upon termination of the Services or upon request, SecureSpells shall delete or return all Personal Data to the Controller, unless Union or Member State law requires storage of the Personal Data.
8.2 Retention Schedules. SecureSpells enforces the following automated retention policies:

- **Registered Account Scan Results:** Retained for up to **90 days**, after which they are automatically deleted or anonymized.
- **Public Scan Results:** Retained for **14 days**.
- **Deleted Accounts:** Subject to a **30-day "soft delete" grace period** to allow for recovery, after which all account data is permanently erased.

# 9. INTERNATIONAL TRANSFERS

9.1 Location. SecureSpells' primary infrastructure is located in Germany (EU).
9.2 Transfers. Any transfer of Personal Data to a third country (non-EU/EEA) shall be subject to appropriate safeguards, such as the Standard Contractual Clauses (SCCs). The Controller acknowledges that specific Sub-processors (listed in Annex III) are located in the United States and agrees to these transfers underpinned by SCCs.

# 10. AUDIT RIGHTS

SecureSpells shall make available to the Controller all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Such audits shall be conducted during normal business hours and subject to reasonable notice.

---

**ANNEX I: DETAILS OF PROCESSING**

A. Subject Matter
The subject matter of the processing is the execution of automated compliance audits on websites submitted by the Controller and the management of the Controller's agency workspace.
B. Duration
The processing will continue for the duration of the Controller's subscription to the Services, plus the applicable retention periods defined in Section 8.2 of the DPA.
**C. Nature and Purpose**

- Scanning websites to detect cookies, trackers, and data transfers.
- Generating risk scores and compliance reports.
- Managing agency subscriptions and role-based access.

**D. Categories of Data**

- **Account Data:** Name, Email Address, Billing Email, User ID, Username, OAuth Provider Data.
- **Scan Data:** Website URLs, IP Addresses (ephemeral during scan), Cookies, Trackers, Detected Domains.
- **Financial Data:** Stripe Customer ID, Subscription status (Card data is NOT stored).

**E. Categories of Data Subjects**

- Employees/Members of the Controller's agency.
- Visitors of the websites scanned by the Controller (if personal data is captured in the scan results).

---

**ANNEX II: TECHNICAL AND ORGANIZATIONAL MEASURES (SECURITY)**

SecureSpells implements the following measures to ensure the security of processing:

**1. Encryption & Pseudonymization**

- **PII at Rest:** Personal data (Name, Email) is encrypted using Fernet (AES-128-CBC + HMAC).
- **E2EE Exports:** Data exports are encrypted using AES-GCM with client-derived keys.
- **Hashing:** Email addresses are hashed (SHA-256 + pepper) for secure lookups without decryption.

**2. Access Control**

- **Authentication:** Session management via Redis with HTTP-only, SameSite=Strict cookies.
- **Role-Based Access:** Strict separation of roles (AGENCY OWNER, ADMIN, MEMBER) enforced at the database level.
- **Internal Access:** Production secrets are managed via environment variables and restricted to relevant services.

**3. Availability & Integrity**

- **Isolation:** Background jobs are isolated via Kafka and separate Worker services.
- **Rate Limiting:** Redis-based rate limiting protects against Denial of Service attacks.
- **Backup:** Regular automated backups of the database are performed.

**4. Data Minimization**

- **IP Addresses:** User IP addresses are used for rate limiting but are **not stored** permanently.
- **Auto-Purge:** Scan results are automatically purged after 90 days (registered) or 14 days (public).

---

**ANNEX III: LIST OF SUB-PROCESSORS**

The Controller authorizes the engagement of the following Sub-processors:

| **Sub-processor** | **Purpose** | **Location** | **Data Transferred** | **Transfer Mechanism** |
|---|---|---|---|---|
| **Hetzner Online GmbH** | Hosting & Database Infrastructure | **Germany (EU)** | All encrypted application data | Intra-EU (No Transfer) |
| **Postmark** (Wildbit, LLC) | Transactional Email Delivery | **USA** | Email Address, Name, Email Content | **SCCs** (Inc. in Terms) |
| **Stripe, Inc.** | Payment Processing | **USA** & Global | Customer ID, Billing Email | **SCCs** |
| **Google / LinkedIn / GitHub / Apple** | OAuth Authentication | **USA** & Global | Email, Name, Avatar (only for auth) | **SCCs** |