Data Processing Agreement (DPA)

DATA PROCESSING AGREEMENT (DPA)

Between:

Customer (Data Controller) - The legal entity purchasing services under the Main Agreement.

Supplier / Data Processor ("Shopspray") – Shopsprayed AB , org. no.: 559174-4890 Hyllie Boulevard 40, 215 15, Malmö, SWEDEN, including any current or future parent companies, subsidiaries, or other affiliated companies within the Shopspray group involved in delivering the Services.

This Data Processing Agreement ("DPA") forms an integral part of the Main Agreement between the Parties and governs Shopspray's processing of personal data on behalf of the Customer in accordance with GDPR and applicable EU and Swedish data protection law.

1. DEFINITIONS

Data Processor: Shopspray.

Data Controller: The Customer.

Personal Data: Any information described in Appendix 1 and processed as part of the services.

Services: All services delivered under the Main Agreement.

Subprocessor: A third party engaged by the Data Processor to process personal data.

GDPR: Regulation (EU) 2016/679.

2. PURPOSE AND SCOPE

The DPA regulates the Data Processor's processing of personal data strictly for purposes defined by the Data Controller and as necessary to deliver the Services. Processing shall only occur based on documented instructions from the Data Controller, including:

- Performance of the Services under the Main Agreement.
- Support, troubleshooting, maintenance, and updates.
- Improving the Services through anonymized and aggregated data.

Any new or changed purposes must be agreed in writing..

3. CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS

Defined in Appendix 1, structured per service.

4. DATA CONTROLLER RESPONSIBILITIES

The Data Controller is responsible for ensuring lawful grounds for processing, accuracy, and compliance with GDPR. The Controller must notify the Processor if instructions appear non-compliant.

5. DATA PROCESSOR RESPONSIBILITIES

The Data Processor shall:

- Process personal data only according to documented instructions.
- Ensure confidentiality for all personnel with access to personal data.
- Implement appropriate technical and organizational measures under GDPR Art. 32.
- Assist the Controller with data subject rights fulfilment.
- Assist the Controller with DPIAs, breach notifications, and regulatory inquiries.
- Maintain records of processing activities under GDPR Art. 30(2).
- Notify the Controller without undue delay regarding data breaches.
- Notify the Controller if an instruction is believed to violate privacy laws.

6. USE OF SUBPROCESSORS

- The Customer grants a general authorization for subprocessors.
- The Processor must notify the Customer before adding or replacing subprocessors.
- Subprocessors shall be subject to the same obligations as the Processor.
- The Processor remains fully liable for subprocessor performance.
- Subprocessor list is detailed in Appendix 1.

7. SECURITY MEASURES

Shopspray shall maintain administrative, physical, and technical safeguards ensuring a security level appropriate to the risk, in accordance with GDPR Article 32.

Security measures applicable to the Services are detailed in Appendix 2.

Shopspray may update or improve its security measures from time to time, provided that such updates do not reduce the overall level of security.

Documentation of current security measures shall be made available to the Data Controller upon request.

8. AUDITS AND INSPECTIONS

The Data Controller may audit the Processor's processing at reasonable intervals. The Processor shall assist and provide all necessary information to demonstrate compliance.

9. DATA BREACHES

The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach, including information required under GDPR Art. 33.

10. INTERNATIONAL TRANSFERS

Personal data shall only be transferred outside the EEA if:

- The Data Controller has provided prior written approval.
- The transfer complies with Chapter V of the GDPR (e.g., SCCs, adequacy decision).

11. DURATION AND TERMINATION

This DPA remains in force as long as the Processor processes personal data on behalf of the Controller.

Upon termination:

- The Controller may choose deletion or return of personal data.
- Deletion shall include backups unless legally required retention applies.
- The Processor shall document the completed deletion.

12. GOVERNING LAW AND VENUE

This DPA is governed by Swedish law. Disputes shall be resolved at Stockholm District Court.

Data Processing Agreement (DPA)

APPENDIX 1: DESCRIPTION OF PROCESSING PER SERVICE INCLUDING SUB-PROCESSORS

The Data Processor shall deliver services in accordance with the Main Agreement. The Data Controller determines the purposes for which personal data is processed.

Service	Purpose	Processing Activities	Personal Data Categories	Subprocessors Location
Microsoft	Hosting / Infrastructure; Communication, Identity	Cloud hosting, data storage, email communication and identity management.	Identification data (name, phone, email), employee identifiers (where provided).	EU
Freshworks Inc.	Support	Freshdesk is used for customer support requests, case logging and support ticket handling.	Identification data (name, phone, email), employee identifiers (where provided).	EU
Sand Dune Mail Ltd.	Communication	SMTP2GO is used to send automatic emails from our systems.	Identification data (name, phone, email), employee identifiers (where provided).	EU / US / AUS
Functional Software, Inc.	Monitoring / Logging	Sentry.io is used as our application logging and error monitoring tool.	N/A	EU
Vercel Inc.	Hosting / Infrastructure	For hosting of our demo applications.	N/A	US
Netlify Inc.	Hosting / Infrastructure	For hosting of our demo applications.	N/A	EU
Hubspot inc.	CRM	Customer relationship management	Identification data (company, name, phone, email), employee identifiers.	US / EU

APPENDIX 2: SECURITY MEASURES

Security Governance

- A defined Information Security Management System (ISMS) aligned with ISO/IEC 27001.
- A documented and maintained Information Security Policy and Privacy Policy approved by management and communicated to all relevant personnel.
- Clearly assigned roles and responsibilities for information security.

Access Control

- Access granted strictly on a need-to-know basis following least-privilege principles.
- Mandatory multi-factor authentication (MFA) for privileged and remote access.
- Logging of both authorised access and attempted unauthorised access.
- Access logs retained for a minimum of three months, or longer where required by law, contractual requirements, or security necessity.
- Physical access controls for buildings, facilities, and equipment used for processing personal data.

Protection Against Threats

- Use of anti-malware, spam filtering, firewalls, and other appropriate protective technologies.
- Regular vulnerability assessments and timely installation of security patches.
- Logging of critical system operations essential for security monitoring and forensic readiness.

Incident Management

- Documented incident management processes including detection, reporting, containment, and mitigation.
- All incidents involving personal data shall be logged and documented.
- Incident documentation retained as required under applicable data protection legislation.
- Timely provision of information to enable the Controller's GDPR Articles 33 and 34 obligations.

Business Continuity

- Backup procedures for all critical systems, including regular backups and secure storage.
- Encryption of backups where technically feasible.
- Recovery procedures and periodic recovery testing to ensure business continuity and data availability.

Personnel Security

- Mandatory information security and data protection training for all personnel with access to systems or personal data.
- Regular refresher training aligned with Shopspray's training program.
- Background checks conducted where legally permissible and relevant to assigned duties.

Encryption

- Encryption of communications and data transmissions using industry-standard algorithms and protocols.
- Special Category Personal Data always encrypted during transfer and, where applicable, at rest.