SMAPLY DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is entered into between Smaply GmbH ("Smaply" or "Processor") and the entity identified as the Customer ("Customer" or "Controller") and is legally to be seen as either part of:

– (i) Smaply's General Terms and Conditions (as applicable) or

– (ii) other electronic or written agreements incorporating this DPA govern the Customer's access and use of Smaply and related services (the "Agreement"). The parties agree that this DPA shall be incorporated into and form part of the Agreement and is subject to the provisions therein.

Definitions

– "Applicable Privacy Law," "Applicable Privacy Laws," or "Data Privacy Laws" means all data protection as well as privacy laws and regulations applicable to the Parties.

– "GDPR" means 2016/679 General Data Protection Regulation.

– "Service" or "Services" means the subscription software-as-a-service offering provided by Smaply.

– "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

– The terms "Controller," "Data Subject," "Personal Data," "Personal Data Breach," "Processing," and "Processor" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

– "Subprocessor" means any person or entity appointed by or on behalf of Processor to process Personal Data on behalf of the Customer in connection with the Agreement.

Smaply will process Personal Data solely to fulfill its contractual obligations to Customer under the Agreement, in particular to the following instructions or authorization of Customer, and in compliance with applicable Data Privacy Laws, as follows:

1. Description and Scope of Processing

Purpose:

– Processing will take place to provide Smaply to the Customer.

– Processing will take place to provide assistance services, such as responding to customer inquiries.

Duration:

– Smaply adheres to data minimization and storage limitations under GDPR, ensuring that personal data is retained only as long as necessary for its intended purposes. Personal data will be deleted or anonymized when it is no longer required for processing, which typically aligns with the duration of the Agreement, plus any additional period necessary to comply with applicable legal retention obligations or to account for data present in Smaply's backup systems. (Typically 1 year after the end of the agreement) For more information on Smaply's standard data retention policies and procedures, please contact us at privacy@smaply.com.

– The customer is free to withdraw the consent to the processing at any point in time in accordance with the GDPR.

Types of Personal Data:

– Names and email addresses (for authentication purposes)

– IP addresses and device information (for usage enhancements, spam protection, and server monitoring)

2. Personnel

Smaply shall take reasonable steps to ensure the trustworthiness of any employee, agent, or contractor of any contracted Processor who may have access to Customer Personal Data, making sure that access is strictly limited in each case to those individuals who need to know/access the relevant Customer Personal Data, as strictly necessary for the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, guaranteeing that all such personnel is subject to confidentiality, may it be professional, statutory or contractual.

3. Security

Smaply shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing. Such measures shall be designed to protect Personal Data from (i) accidental or unlawful destruction, (ii) loss, alteration, unauthorized disclosure of, or access to the Personal Data. Smaply shall implement these measures by default to ensure that, by default, only personal data necessary for each specific purpose is processed.

At a minimum, such measures shall include the security measures identified in Annex 1.

4. Return and Destruction of Personal Data

Except to the extent required otherwise by applicable Data Privacy Laws, Smaply will, at your choice and upon your written request, return to you or securely destroy all Personal Data upon such request or at termination or expiration of the Agreement. If no request to return Customer's Personal Data is received, Smaply will securely destroy your Personal Data at termination or expiration of the Agreement.

5. Subprocessing

The customer grants Smaply general authorization to subcontract the processing of Customer Personal Data to a Subprocessor.

If Smaply engages a new or replacement Subprocessor, Smaply will:

- Update the Subprocessor List,
- Inform the Customer in electronic form about the Subprocessor,
- Impose substantially the same data protection terms on any Subprocessor it engages as contained in this DPA (including data transfer provisions, where applicable); and
- Remain liable to Customer for any breach of this DPA caused by an act, error, or omission of such Subprocessor.

The customer may object to Smaply's appointment of any new or replacement Subprocessor promptly in electronic form within thirty (30) days after receipt of notice and on reasonable grounds related to the Subprocessor's ability to comply with Applicable Privacy Law(s). In such a case, the parties shall discuss the Customer's concerns in good faith to achieve a commercially reasonable resolution. If the parties cannot reach such a resolution, Smaply shall have the right, at its sole discretion, to either not appoint the disputed Subprocessor or permit Customer to suspend or terminate the applicable order and/or the Agreement. Under no circumstances will the appointed Subprocessor process the Customer's data in the event of an objection by the Customer. These procedures are the Customer's exclusive remedy and Smaply's entire liability for resolving the Customer's objections to Smaply's appointment of Subprocessor under this DPA.

6. Additional Safeguards

To the extent that Smaply processes the Personal Data of Data Subjects located in or subject to the applicable Data Protection Laws of the European Economic Area, Switzerland, the United Kingdom, California, or Brazil,

Smaply has implemented a variety of additional safeguards regarding the transfer of such Personal Data from these jurisdictions. Smaply maintains transfer impact assessment materials, which are considered Smaply's Confidential Information. We will provide these materials to customers located in these jurisdictions upon written request from privacy@smaply.com. TIA may be accessible for requests from supervisory authorities.

7. Data Breaches

In the event of a Data Breach, Smaply shall inform Customer without undue delay and will provide written details of the Data Breach to Customer, including the type of data affected and the identity of the affected person(s), once such information becomes known or available to Smaply. Smaply shall, to the extent possible, provide timely information and cooperation to Customer to allow Customer to fulfill its Data Breach reporting obligations under Applicable Privacy Law(s) and shall take reasonable steps to remedy or mitigate the effects of the Data Breach. The obligations herein shall not apply to Data Breaches that are caused by the Customer or its users.

8. Data Subject Rights

Taking into account the nature of the Processing, Smaply shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Controller obligations, as reasonably understood by the Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

9. Cooperation

Smaply shall reasonably cooperate with Customer to enable Customer to respond to any requests, complaints, or other communications from data subjects and regulatory or judicial bodies relating to the processing of Customer Personal Data, including requests from data subjects seeking to exercise their rights under Applicable Privacy Law(s). If any such request, complaint, or communication is made directly to Smaply, Smaply shall, once it has identified the request is from or related to a data subject for whom the Customer is responsible, pass this onto Customer and shall not respond to such communication without Customer's express authorization (unless required to do so to comply with applicable law(s)).

To the extent Smaply is required under Applicable Privacy Law(s), Smaply will assist the Customer in conducting a data protection impact assessment and, where legally required, consult with applicable data protection authorities in respect of any proposed processing activity that presents a high risk to data subjects.

10. Assistance & Audits

- Smaply will assist the Customer in ensuring compliance with its obligations under articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Smaply.

- Smaply shall make available to the Customer the information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and, if needed, allow audits to be conducted by the Customer that is not a competitor of Smaply.

11. Survival

The provisions of this DPA survive the termination or expiration of the Agreement for so long as Smaply or its Subprocessors process the Personal Data.

12. Governing Law and Jurisdiction

This DPA is governed by Austrian law.

Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the regional court of Innsbruck.

ANNEX 1: TECHNICAL AND ORGANIZATIONAL MEASURES

This Annex 1 forms part of the DPA.

Smaply operates as a remote organization and does not maintain its own offices or data centers for the processing of Customer Personal Data. Production infrastructure is hosted by Smaply's cloud infrastructure subprocessor, Google Cloud Platform (GCP), which are responsible for the physical and environmental security of the underlying facilities. Smaply reviews the relevant subprocessor attestation reports and performs a risk analysis at least annually. The measures set out below are further evidenced by Smaply's ISO/IEC 27001 certification and SOC 2 Type II report, which are available via the Trust Center at https://trust.smaply.app.

CONFIDENTIALITY

- **Physical access control:** Smaply does not operate its own offices or data centers for the processing of Customer Personal Data. Production servers are hosted by Smaply's cloud infrastructure subprocessor, Google Cloud Platform (GCP) which is responsible for the physical and environmental security of its data centers, including controlled facility access (for example, badge and/or biometric access controls), perimeter protection, and continuous monitoring. Smaply reviews the subprocessor's attestation reports and performs a risk analysis at least annually.
- **System access control:** Access to systems and applications requires unique user credentials, with password requirements enforced in accordance with Smaply's access-control policy. Multi-factor authentication (MFA) is required for privileged and production-system access and is available to end users through supported single sign-on (SSO) identity providers. Production systems are remotely accessible only by authorized personnel over encrypted connections.
- **User access control:** Access is granted on a least-privilege, need-to-know basis using role-based access control. Access provisioning and de-provisioning follow documented procedures, including approval and background checks prior to provisioning and revocation of access upon termination within defined timelines. Access rights are reviewed at least quarterly, and access events are logged.
- **Encryption:** Customer Personal Data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256. Access to encryption keys is restricted to authorized personnel with a business need.
- **Data classification:** Smaply maintains a data classification policy so that confidential data is identified, secured, and restricted to authorized personnel. Confidential or sensitive customer data is not used or stored in non-production environments.

INTEGRITY

- **Disclosure and transmission control:** Secure transmission protocols (TLS 1.2 or higher) protect Personal Data during electronic transmission; portable and removable media are encrypted where used.
- **Input control:** Security-relevant activity, including access, authentication, and configuration changes, is centrally logged and monitored. Changes to the application and infrastructure follow documented change-management and version-control procedures, with review and approval prior to deployment to production.

AVAILABILITY AND RESILIENCE

- **Availability control:** Production data is backed up on an automated basis, with backups encrypted and stored separately from the production system within the cloud provider's infrastructure. Databases are replicated to a secondary location, with alerting on replication failure. Edge protection (web application firewall and DDoS mitigation) and vulnerability scanning are applied, and Business Continuity and Disaster Recovery plans are maintained.
- **Rapid restorability:** Point-in-time recovery and automated failover support restoration within defined recovery objectives.

- **Deletion periods:** Formal retention and disposal procedures govern both data and metadata such as log files. Customer Personal Data is purged from the application environment when a customer leaves the service, and secure deletion (including cryptographic erasure) is applied at the cloud-infrastructure level.

PROCESS FOR REGULAR INSPECTION, ASSESSMENT, AND EVALUATION

- **Data protection management** within an Information Security Management System (ISO/IEC 27001), including regular employee security training and continuous control monitoring.
- **Incident response management,** including documented procedures for identifying, reporting, and responding to security and data-privacy incidents.
- **Data protection-friendly default settings** (privacy by design and by default).

ANNEX 2 – DATA PROTECTION CONTACTS & COMPANY INFORMATION

This Annex forms part of the DPA and sets out the Processor's data protection contacts and company information.

A. Data Protection Contacts

Data Protection Contacts	
Data Protection Officer	Bilgehan Arifoğlu — privacy@smaply.com
Company Representative	Marc Stickdorn — marc@smaply.com
Competent Supervisory Authority	Österreichische Datenschutzbehörde (DSB), Vienna, Austria
General Privacy Contact	privacy@smaply.com
Security & Compliance Portal	https://trust.smaply.app

B. About Smaply

Smaply is a software-as-a-service platform developed by Smaply GmbH, dedicated to customer journey mapping and journey management. It enables organizations to visualize and manage journey maps, personas, and stakeholder relationships as an organization-wide system for making customer-centric decisions.

Company Information	
Legal Name	Smaply GmbH
Registered Office	Kapuzinergasse 14, 6020 Innsbruck, Austria
Commercial Register	FN 421906 a (Austrian Commercial Register)
VAT ID	ATU69101223
Managing Director	Marc Stickdorn
Email	mail@smaply.com
Phone	+43 512385143
Website	https://smaply.app / https://smaply.com
Certifications	ISO/IEC 27001; SOC 2 Type II