Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR, between the SmoovOps customer ("Controller") and Northwood UG (haftungsbeschränkt) ("Processor")

Preamble

This Data Processing Agreement ("Agreement" or "DPA") specifies the parties' data protection obligations in connection with the use of SmoovOps and supplements the Terms and Conditions between the parties. It applies to all processing of personal data carried out by the Processor on behalf of the Controller in the course of providing SmoovOps.

In the event of any conflict between this DPA and the Terms and Conditions, the provisions of this DPA prevail with respect to the processing of personal data.

§ 1 Subject Matter and Duration

(1) The subject matter of this Agreement is the processing of personal data by the Processor on behalf of the Controller in connection with providing the SmoovOps application, in particular the Partners (CRM), Product Catalogue, Contracts, Documents (including invoices, offers, delivery notes, letters, and receipts), Notes, Payments, and Dashboard modules.

(2) Details on the nature, scope, and purpose of the processing, the type of personal data, and the categories of data subjects are set out in **Annex 1**.

(3) The term of this Agreement corresponds to the term of the main agreement between the parties (the SmoovOps usage agreement under the Terms and Conditions). It automatically ends upon termination of the main agreement, subject to the obligations continuing under § 10.

§ 2 Controller's Right to Issue Instructions

(1) The Processor processes personal data only on documented instructions from the Controller, unless required to do so by European Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless the law in question prohibits such notification on important grounds of public interest.

(2) Use of SmoovOps in accordance with the contractually agreed features, as well as the configurations and data entries made by the Controller via the user interface, constitute instructions within the meaning of this Agreement. Any further instructions must be given in text form (e.g. email to info@northwood.de).

(3) If the Processor considers an instruction from the Controller to be unlawful, it shall inform the Controller without delay. The Processor is entitled to suspend implementation of such an instruction until it is confirmed or amended by the Controller.

§ 3 Confidentiality

The Processor ensures that persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of confidentiality, and that such persons have access to the relevant personal data only to the extent necessary.

§ 4 Technical and Organizational Measures

(1) The Processor implements the technical and organizational measures (TOMs) described in **Annex 2** to ensure a level of protection appropriate to the risk in accordance with Art. 32 GDPR.

(2) The Processor is entitled to adapt the TOMs, provided the originally agreed level of protection is not undercut. Material changes will be communicated to the Controller.

§ 5 Processor's Obligations

Taking into account the nature of the processing, the Processor undertakes to assist the Controller, insofar as possible, by appropriate technical and organizational measures, in fulfilling the Controller's obligation to respond to requests for the exercise of the data subject's rights set out in Chapter III GDPR (Art. 28(3)(e) GDPR). If the Processor receives such a request directly from a data subject, it will forward it to the Controller without delay without responding to it itself, unless the Controller instructs otherwise.

The Processor assists the Controller, taking into account the nature of the processing and the information available to the Processor, in complying with the obligations set out in Art. 32 to 36 GDPR (including security of processing, notification of personal data breaches, and data protection impact assessments).

§ 6 Notification of Data Protection Breaches

(1) The Processor notifies the Controller of any personal data breach within the meaning of Art. 4 No. 12 GDPR that comes to its attention without undue delay, and in any case within **48 hours** of becoming aware of it.

(2) The notification includes, to the extent known to the Processor, at least the information required under Art. 33(3) GDPR, and is sent to the address stored in the customer account.

(3) The Controller remains solely responsible for assessing whether an obligation to notify the supervisory authority under Art. 33 GDPR or to notify data subjects under Art. 34 GDPR exists, and for carrying out any such notification.

§ 7 Sub-processing

(1) The Controller grants the Processor a general authorization to engage sub-processors within the meaning of Art. 28(2) GDPR. The sub-processors engaged as of the date of this Agreement are listed in **Annex 3**.

(2) The Processor will inform the Controller of the engagement or replacement of sub-processors at least 14 days before the planned change, e.g. by email or via the customer account or a corresponding status page. The Controller may object to the change within this period for a legitimate, objectively verifiable reason. If no objection is raised, the change is deemed approved.

(3) The Processor contractually obligates sub-processors to data protection duties equivalent to those agreed in this Agreement, in particular with regard to appropriate technical and organizational measures.

(4) Where sub-processors process data outside the EU/EEA, the Processor ensures that appropriate safeguards within the meaning of Art. 44 et seq. GDPR are in place (e.g. an adequacy decision by the European Commission or EU Standard Contractual Clauses).

§ 8 Controller's Audit Rights

(1) The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allows for and contributes to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

(2) Evidence may, to the extent sufficient, also be provided by submitting current certifications, attestations, or audit reports from independent auditors (e.g. relating to hosting providers used by the Processor), provided these allow an assessment of compliance with the obligations agreed in this Agreement.

(3) On-site inspections must be announced in writing with reasonable advance notice (at least 2 weeks) and take place during normal business hours without unreasonably disrupting the Processor's operations. The Controller bears the costs of such an inspection, unless it was prompted by a finding of a material breach of this Agreement by the Processor.

§ 9 Persons Authorized to Issue/Receive Instructions

The Controller's authorized contact is the person specified during registration or on file in the customer account. The Processor's contact is:

Northwood UG (haftungsbeschränkt) Attn: Thorsten Szutzkus Email: info@northwood.de

§ 10 Deletion and Return of Personal Data

(1) After termination of the main agreement, the Processor deletes all personal data processed on behalf of the Controller, or returns it at the Controller's choice, unless Union or Member State law requires storage of the personal data.

(2) For this purpose, the Controller is given access to the export functionality described in the Terms and Conditions (§ 8) for a period of 30 days after termination. After this period, the Processor deletes the remaining data, unless statutory retention obligations apply (e.g. for invoice data under Sec. 147 of the German Fiscal Code (AO) or Sec. 257 of the German Commercial Code (HGB)).

§ 11 Liability

(1) The statutory liability provisions of Art. 82, 28(10), and Art. 83 GDPR apply.

(2) In all other respects, the limitations of liability agreed in the Terms and Conditions apply accordingly, insofar as this does not conflict with mandatory statutory provisions of the GDPR.

§ 12 Final Provisions

(1) Amendments and supplements to this Agreement and all its components — including any assurances given by the Processor — require a written or electronically documented agreement.

(2) In the event of conflicts between this DPA and provisions of other agreements between the parties, in particular the Terms and Conditions, the provisions of this DPA prevail with respect to data protection matters.

(3) Should individual provisions of this Agreement be or become invalid, the validity of the remaining provisions remains unaffected.

(4) This Agreement is governed by the law of the Federal Republic of Germany.

Annex 1: Subject Matter, Nature, and Purpose of Processing

Subject Matter and Duration of Processing

Provision of the SmoovOps application as a software-as-a-service solution for the term of the main agreement.

Nature and Purpose of Processing

Collection, storage, organization, display, modification, export, and deletion of personal data entered or uploaded by the Controller in the course of using the following SmoovOps modules:

- **Partners (CRM):** management of contact and business relationship data

- **Product Catalogue:** management of product/service details (generally no personal data, unless contact persons or similar are recorded)
- **Contracts:** creation, storage, and management of contract documents
- **Documents:** creation, storage, upload, and management of documents of the types contract, invoice, offer, delivery note, letter, and receipt, including support for the XRechnung/ZUGFeRD invoice formats and data automatically extracted from uploaded documents (text recognition/IDP)
- **Notes:** recording of notes and comments relating to partners, contracts, payments, and products
- **Payments:** recording and tracking of payment transactions related to invoices
- **Dashboard:** aggregated analyses of the above data

Type of Personal Data

- First and last name
- Company name, address
- Contact details (email address, phone number)
- Invoice and payment data (invoice amounts, payment status, bank details, where entered by the Controller)
- Contract data and content, where personal in nature
- Note and comment content relating to partners, contracts, payments, and products (Notes module)
- Content of uploaded or generated documents and data automatically extracted from them (Documents module, e.g. text recognition/IDP of invoices and receipts)
- Photos, where added by the Controller to partner or product records

Categories of Data Subjects

- Business partners, customers, and contact persons of the Controller
- Employees of the Controller, where recorded in connection with contracts/invoices

---

Annex 2: Technical and Organizational Measures (TOMs) under Art. 32 GDPR

1. Confidentiality

- **Physical access control:** physical access control is handled by hosting provider AWS at its data centers in accordance with its certifications
- **System access control:** access to systems only via individual credentials
- **Data access control:** role- and permission-based concept restricting access to personal data to what is necessary for the respective task (need-to-know principle)
- **Separation control:** logical separation of different customers' data at the application level (multi-tenancy)

2. Integrity

- **Transmission control:** encrypted data transmission (TLS) for communication between client and server
- **Input control:** logging of security-relevant events and changes into audit logs

3. Availability and Resilience

- Regular data backups every 7 days
- Redundant infrastructure across the availability zones provided by the hosting provider
- Disaster recovery plan for restoring availability after a physical or technical incident

4. Procedures for Regular Testing, Assessment, and Evaluation

- Regular review of the security measures in place (semi-annual)
- Data Processing Agreements with all sub-processors engaged (see Annex 3)
- Software updates and security patches after review in a staging environment

---

Annex 3: Approved Sub-processors

Sub-processor	Service	Location of processing	Safeguard for third-country transfer
Amazon Web Services (AWS)	Hosting, infrastructure (incl. AWS Lambda, DynamoDB, S3) and content delivery/attack protection (CloudFront, WAF)	eu-central-1 (Frankfurt); WAF WebACL managed in us-east-1 (Northern Virginia) for technical reasons, processing only request metadata there	EU-US Data Privacy Framework (certification), with EU Standard Contractual Clauses as a fallback mechanism
Stripe Payments Europe, Ltd. (with possible involvement of its affiliate Stripe, Inc., USA)	Payment processing	Dublin, Ireland (Stripe, Inc.: USA)	EU Standard Contractual Clauses under Art. 46(2)(c) GDPR
Amazon Web Services (AWS SES)	Sending of transactional emails	eu-central-1 (Frankfurt)	not applicable (EU region)

Last updated: 29.07.2026