Data Processing Agreement with Schedules

Draft for approval. Do not use for binding orders or approved customer deliveries. Complete open fields before use; legal and commercial review is required.

1. Parties, subject matter and effectiveness

Controller: organisation, address and contact [____]. Processor: Inceptum Business Solutions GmbH, Erich-Nörrenberg-Straße 7, 58636 Iserlohn, Germany, info@inceptumgroup.de. This agreement applies only to processing on behalf of the controller specifically described in Schedule A under Article 28 GDPR. It becomes binding upon valid agreement by the parties and completion of Schedules A to C. Software licensing alone does not establish processing on behalf of a controller.

Schedule A defines the subject matter, nature, purpose, data types, categories of data subjects, duration, processing locations and deletion process. The controller determines purposes and essential means, ensures a legal basis, informs data subjects and is responsible for the lawfulness of its instructions. This does not affect Inceptum's duties as processor.

2. Instructions and confidentiality

Inceptum processes personal data only on documented instructions from the controller, including transfers to third countries, unless processing is required by law. In that case Inceptum informs the controller of the requirement beforehand unless the law prohibits this on important public interest grounds. Schedule A identifies authorised instruction-givers and recipients. Urgent oral instructions are documented without undue delay.

If Inceptum considers an instruction to infringe data protection law, it promptly informs the controller and suspends the affected processing pending clarification where necessary. Persons with access are bound by confidentiality commitments or an appropriate statutory duty of confidentiality. Access is granted only to the extent necessary.

3. Security of processing

Inceptum implements technical and organisational measures appropriate to the risk under Article 32 GDPR. Schedule B must specifically document the measures actually agreed and their evidence. Protection needs, confidentiality, integrity, availability, resilience, recovery and regular effectiveness reviews must be considered. Changes may not reduce the agreed protection level; material changes are documented and communicated.

An empty measures list or a product security description does not demonstrate implemented operational safeguards. Before production remote access or hosting, measures must be reviewed, access methods defined and necessary approvals recorded.

4. Subprocessors and third countries

Subprocessors named in Schedule C with their services and processing locations are specifically authorised on conclusion. Any later addition or replacement requires the controller's separate prior authorisation in text form. An empty schedule provides no blanket authorisation. Inceptum contractually imposes the same data protection obligations on these organisations and remains responsible to the controller for their performance.

Processing outside the EEA requires, in addition to instructions and authorisation, a lawful basis under Chapter V GDPR, including necessary safeguards, transfer assessment and supplementary measures. This agreement is not itself a third-country transfer instrument. Hosting the shop at Mittwald does not automatically make Mittwald a subprocessor for all CRM customer data.

5. Assistance and personal data breaches

Taking account of the nature of processing, Inceptum assists the controller through appropriate measures in responding to data subject rights. Requests received directly are promptly forwarded and not answered independently without instructions unless legally required. Inceptum also assists with security, supervisory authority notifications, communication to data subjects, data protection impact assessments and prior consultation to the extent required by law, considering the information available.

Inceptum notifies the controller of a personal data breach without undue delay after becoming aware of it. Where available, the notification describes its nature and scope, affected data and individuals, contact point, likely consequences and measures taken or proposed; missing information is provided in stages. Inceptum preserves necessary evidence and assists containment. The controller's statutory notification deadline is not a waiting period for Inceptum.

6. Evidence and audits

Inceptum makes available all information necessary to demonstrate compliance with Article 28 GDPR and allows and contributes to audits, including inspections, by the controller or its appointed auditor. Audits are coordinated where appropriate and protect other customers' confidential information. Notice or cost arrangements must not obstruct urgency, specific incidents or statutory audit rights. Any fees for additional services are agreed transparently; statutory cooperation is not made dependent on unresolved fees.

7. End of processing, return and deletion

After the services end, Inceptum returns or deletes the data, including existing copies, at the controller's choice unless law requires retention. Schedule A defines the format, timing and treatment of backups. Data subject to legal retention is restricted, processed only for that purpose and deleted when the period ends. Completion is evidenced on request. Confidentiality obligations survive termination.

Schedule A: Specific processing

Complete and agree before access: main agreement/service order [____]; exact activity and purpose [____]; start/end [____]; data types [____]; categories of data subjects [____]; special-category data or exclusion of such data [____]; systems and processing locations [____]; authorised instruction-givers and emergency contacts for both parties [____]; return format and timing [____]; deletion/backups and evidence [____]. Include only data actually required; do not enter production passwords in this schedule.

Schedule B: Technical and organisational measures

For each measure record implementation, owner and evidence: identities/roles/MFA [____]; premises and device access [____]; transport/storage encryption and key management [____]; tenant separation [____]; logged, approved remote support [____]; backups and tested restoration [____]; patch and vulnerability management [____]; confidentiality/training [____]; deletion and media [____]; incident response [____]; regular effectiveness review [____]. This list identifies review areas and does not claim that measures have already been implemented.

Schedule C: Subprocessors and execution

For each organisation: legal name/address [____]; specific service [____]; data/data subjects [____]; processing and access locations [____]; authorisation [____]; for third-country involvement, transfer instrument and assessment [____]. If no subprocessors are used, this must be expressly confirmed. Execution: controller, name/role, date and signature or evidenced electronic acceptance [____]; Inceptum, name/role, date and acceptance [____].