

Data Processing Agreement (AVV) - Template

Article 28 GDPR template for a customer using Hide as processor. Complete all bracketed customer fields and obtain legal review before signature.

DRAFT FOR REVIEW

1. Parties and scope

Controller: [Customer legal name and address]. Processor: Clexa GmbH, Friedrich-Ebert-Strasse 31, 92421 Schwandorf, Germany (provider of Hide). This agreement covers personal data processed when the customer uses the Hide workspace, current-message add-ins, approved mailbox connections, payment checks, supplier records and audit exports.

2. Subject, duration and purpose

Hide processes submitted message and payment indicators to return a warning verdict, document verification steps and maintain the customer's selected history. Processing lasts for the service term plus the deletion and return period stated below.

3. Data and data subjects

Category	Description
Data subjects	Customer users, employees, contacts, suppliers and message senders whose data appears in an authorized check.
Data	Account data; sender and routing fields; domains; hashed IBAN and invoice identifiers; verdict, category, signal identifiers and timestamps; approved vendor contact data.
Special categories	Not intended. The customer must not submit special-category data unless separately agreed and necessary.

4. Controller instructions

The processor acts only on documented instructions in the service configuration and this agreement. An instruction that appears unlawful is escalated before execution, unless Union or Member State law prohibits notice.

5. Confidentiality and security

Authorized personnel are bound to confidentiality. The technical and organizational measures in the attached TOMs apply. Access is least-privilege, workspace-bound and logged.

6. Sub-processors

The processor maintains a public sub-processor list and gives customers advance notice of material additions. Equivalent Article 28 duties apply to each sub-processor. The customer may object on substantiated data-protection grounds within [14] days.

7. International transfers

The default architecture must keep processing and storage in the EU. Any exceptional third-country transfer requires an applicable Chapter V mechanism, documented assessment and customer notice.

8. Assistance

Hide provides reasonable assistance with data-subject requests, security incidents, DPIAs, prior consultation and evidence needed to demonstrate compliance, taking into account the nature of processing and information available to Hide.

9. Incidents

Hide notifies the customer without undue delay after becoming aware of a personal-data breach affecting customer data and supplies known facts, likely consequences and remediation. Notification is not an admission of fault.

10. Deletion and return

Raw message and image content is not retained by default. Extracted deduplication fields expire after 90 days. Personal check records default to 12 months; workspace records default to three years and must become configurable. On termination, customer data is deleted or returned as instructed, subject to mandatory retention.

11. Audit

Hide supplies current compliance information and permits proportionate audits. Parties first use existing reports and remote evidence. On-site access is limited to what is necessary, confidential and scheduled to avoid security or operational harm.

12. Signatures

For the controller: [name, role, date, signature]. For Clexa GmbH: [name, role, date, signature]. Electronic signature is permitted.