# Data Processing Addendum — Unsigned Template

**Effective:** November 8, 2026 • **Version:** 2026-11-08 • **Service:** SpendLeak

*This unsigned template becomes binding only after the identified parties complete and validly execute it. The live Terms and Privacy Policy do not automatically execute this addendum.*

## Contents

1. Status and contracting parties
2. Roles and processing scope
3. Data subjects and categories
4. Instructions and confidentiality
5. Security measures
6. Subprocessors and transfers
7. Assistance and breach notification
8. Return, deletion and retention
9. Audits, liability and signature

## 1. Status and contracting parties

This Data Processing Addendum (“DPA”) is an unsigned negotiation template, not a contract automatically accepted by viewing a website. The parties must identify the Customer, the actual SpendLeak legal operator, effective date, applicable main agreement and any jurisdiction-specific terms before signature. Posting this DPA does not represent certification of compliance with any foreign law.

## 2. Roles and processing scope

For Customer-controlled invoices, contracts and related records, the Customer determines the processing purposes and SpendLeak generally acts as a service provider or processor subject to documented instructions, depending on applicable law. SpendLeak may act independently for account administration, security and legal compliance purposes. Processing may involve hosting, import validation, billing discrepancy analysis, reports and user-requested AI assistance.

## 3. Data subjects and categories

Data subjects may include Customer staff, supplier contacts, sole proprietors and individuals incidentally named in records. Categories may include names, business contact details, invoice references, compensation or payment-related details, contract records and review notes. Special-category or highly sensitive datasets are outside the standard intended use unless separately reviewed and agreed.

## 4. Instructions and confidentiality

The processor shall process Customer Data only for documented authorized purposes, except when required by applicable law, and shall limit access to persons subject to appropriate confidentiality duties. If an instruction appears unlawful or outside the agreed scope, the parties should address it before processing where practical. Neither party may use this DPA to eliminate legal rights of affected individuals.

## 5. Security measures

The parties must attach a factual schedule of deployed organizational and technical safeguards, including authentication, authorization, encryption, logging, backup and incident handling. Controls listed as planned are not binding representations of implemented safeguards unless expressly agreed. Each party retains responsibility for the security obligations applicable to its role.

## 6. Subprocessors and transfers

The parties should agree a current subprocessor list covering hosting, database, identity and any AI provider, with relevant services and processing locations. Contractual mechanisms for cross-border transfers must be evaluated by jurisdiction. A provider region alone is not a comprehensive data-residency guarantee. Material subprocessor changes should follow the notice and objection process agreed by the parties.

## 7. Assistance and breach notification

The processor should reasonably assist the Customer with lawful access, correction and deletion requests, security incident assessments and information needed to meet applicable obligations, subject to agreed scope and technical feasibility. The parties must negotiate concrete breach notification times and contact routes; none is fabricated by this template. Mandatory statutory deadlines remain applicable.

## 8. Return, deletion and retention

At termination, the parties should establish a secure process for export, return and deletion of eligible Customer Data, addressing copies, backups, legal holds and provider retention limits. A deletion certificate or detailed service-level commitment should only be promised if a verified procedure exists. The Customer remains responsible for retaining its legally required source records outside the Service.

## 9. Audits, liability and signature

Any audit rights, evidence access, remediation procedure, fees, confidentiality restrictions and liability allocations should be negotiated in the main agreement or signed DPA. Applicable law and mandatory privacy rights prevail. This template becomes effective only when accepted by authorized representatives through a legally sufficient process and with completed identification and schedules.