Auftragsverarbeitungs-vereinbarung nach Art. 28 DSGVO

Version 2026-11-23

Data Processing Agreement pursuant to Art. 28 GDPR

Version 2026-11-23

I. Parteien und Anwendungsbereich

1.1 Auftragnehmer

Auftragnehmer ist die Klardaten GmbH („Klardaten“).

1.2 Auftraggeber

Auftraggeber ist der Kunde, der in dem jeweiligen Bestellformular, Angebot, Checkout, Kundenkonto oder sonstigen Bestelldokument bezeichnet ist und diese AVV akzeptiert hat.

1.3 Rolle der Parteien

Klardaten ist Auftragsverarbeiter des Verantwortlichen oder, wenn der Auftraggeber selbst im Auftrag handelt, weiterer Auftragsverarbeiter (siehe Anlage 4). Im zweiten Fall stellt der Auftraggeber vorab die erforderliche schriftliche Genehmigung des Verantwortlichen für Klardaten und deren Unterauftragsverarbeiter sicher. Er leitet die dokumentierten Weisungen weiter und legt Klardaten die einschlägigen Datenschutzpflichten vertraglich auf.

1.4 Bestandteil des Vertrags

Diese AVV ist Bestandteil des Vertrags über die Nutzung der Klardaten-Dienste.

1.5. Sprache

Nur der deutsche Text ist relevant. Die englische Fassung dient nur der Information. Im Falle von Abweichungen gilt daher nur die deutsche Fassung.

I. Parties and Scope of Application

1.1 Processor

The processor is Klardaten GmbH (“Klardaten”).

1.2 Client

The client is the Customer identified in the respective order form, offer, checkout, customer account, or other order document and who has accepted this DPA.

1.3 Role of the Parties

Klardaten acts as the controller’s processor or, where the Client itself acts as a processor, as a subprocessor (see Annex 4). In the latter case, the Client ensures that the controller’s required prior written authorisation covers Klardaten and its subprocessors. The Client forwards the documented instructions and contractually imposes the applicable data protection obligations on Klardaten.

1.4 Part of the Agreement

This DPA forms part of the agreement governing the use of the Klardaten Services.

1.5 Language

Only the German text is legally relevant. The English version is provided for information purposes only. In the event of any discrepancies, only the German version shall prevail.

II. Dauer der Vereinbarung

(1) Diese AVV gilt ab Wirksamwerden des Vertrags und bleibt so lange in Kraft, wie Klardaten personenbezogene Daten im Auftrag des Kunden verarbeitet, einschließlich Verarbeitung in Backups, Protokollen sowie Lösch- und Rückgabeprozessen.

(2) Eine isolierte ordentliche Kündigung dieser AVV ist ausgeschlossen, solange der Vertrag über die Klardaten-Dienste fortbesteht und Klardaten personenbezogene Daten im Auftrag des Kunden verarbeitet.

II. Duration of the agreement

(1) This DPA applies from the effective date of the Agreement and remains in force for as long as Klardaten processes personal data on behalf of the Customer, including processing in backups, logs, and deletion and return processes.

(2) A separate ordinary termination of this DPA is excluded for as long as the agreement for the Klardaten services remains in force and Klardaten processes personal data on behalf of the Customer.

III. Pflichten des Dienstleisters

(1) Der Dienstleister und jede dem Dienstleister unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, verarbeiten personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn er ist oder sie sind nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Erhält der Dienstleister einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

(2) Der Dienstleister erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

(3) Der Dienstleister erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 2 zu entnehmen).

(4) Der Dienstleister ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.

III. Obligations of the service provider

(1) The service provider and any person acting under its authority who has legitimate access to personal data shall process such data only on the basis of documented instructions from the client, including the authorizations granted in this contract, unless they are required to do so under Union law or the law of a Member State. If the service provider receives an official order to disclose the client's data, it shall — insofar as legally permissible — inform the client immediately and refer the authority to the client.

(2) The service provider shall declare in a legally binding manner that it has obligated all persons commissioned with data processing to maintain confidentiality before commencing their activities or that they are subject to an appropriate statutory confidentiality obligation.

(3) The service provider declares in a legally binding manner that it has taken all necessary measures to ensure the security of processing in accordance with Art 32 GDPR (details can be found in Annex 2).

(4) The service provider shall take the technical and organizational measures to ensure that the client can fulfill the rights of the data subjects under Chapter III of the GDPR (information, access, rectification and erasure, data portability, objection and automated decision-making in individual cases) at any time within the statutory time limits and shall provide the client with all necessary information.

(5) Der Dienstleister unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(6) Der Dienstleister wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht der Einsichtnahme und Kontrolle eingeräumt. Die Kontrolle erfolgt vorrangig durch Dokumentenprüfung. Der Dienstleister verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(5) The service provider shall support the client in complying with the obligations set out in Art. 32 to 36 GDPR (data security measures, notification of personal data breaches to the supervisory authority, notification of the person affected by a personal data breach, data protection impact assessment, prior consultation).

(6) The service provider is advised that it must draw up a processing directory in accordance with Art. 30 GDPR for the present order processing.

(7) The Client shall be granted the right to inspect and control the processing of the data provided by it. The review is carried out primarily by means of a documentation review. The Service Provider undertakes to provide the Client with the information necessary to monitor compliance with the obligations set out in this Agreement.

(8) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Beauftragung – hat der Dienstleister sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(8) Copies or duplicates of the data shall not be created without the knowledge of the client. Exceptions apply to backup copies, insofar as they are necessary to ensure proper data processing, as well as data that must be retained to comply with statutory retention obligations.
After completion of the contractually agreed work, or earlier upon request by the client—but no later than upon termination of the engagement—the service provider shall hand over to the client all documents, processing and usage results, and data sets obtained in connection with the contractual relationship, or, with the prior consent of the client, securely destroy them in compliance with data protection requirements.
The same applies to test and discarded material. A record of the deletion must be provided upon request.

(9) Der Dienstleister hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

(9) The Service Provider shall inform the Client immediately if it believes that an instruction of the Client violates data protection regulations of the Union or the Member States.

(10) Der Dienstleister verpflichtet sich, seine technisch-organisatorischen Maßnahmen mindestens einmal jährlich zu überprüfen und in angemessenem Umfang dem Stand der Technik anzupassen.

(11) Sofern gesetzlich zulässig, informiert der Dienstleister den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sich diese auf diesen Auftrag beziehen.

(12) Der Dienstleister verpflichtet sich dazu, seine beauftragten Subunternehmer in angemessenen Zeitabständen und angemessenem Umfang daraufhin zu überprüfen, ob diese im Sinne der DSGVO als geeignete Dienstleister einzustufen sind.

(13) Der Dienstleister meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

(10) The service provider undertakes to review its technical and organizational measures at least once a year and to adapt them to the state of the art to an appropriate extent.

(11) To the extent permitted by law, the service provider shall inform the client immediately of any inspection activities and measures taken by the supervisory authority, insofar as these relate to this order.

(12) The Service Provider undertakes to review its commissioned subcontractors at appropriate intervals and to an appropriate extent to determine whether they are to be classified as suitable service providers within the meaning of the GDPR.

(13) The service provider shall report personal data breaches to the client without undue delay in such a manner that the client can fulfill its legal obligations, in particular those under Articles 33 and 34 of the GDPR. The service provider shall prepare documentation of the entire process and make it available to the client for further action.

IV. Ort der Durchführung der Datenverarbeitung

(1) Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

IV. Place where data processing is carried out

(1) Data processing activities are carried out exclusively within the EU or the EEA.

V. Sub-Auftragsverarbeiter

(1) Der Kunde genehmigt den Einsatz der in der jeweils aktuellen Unterauftragsverarbeiterliste genannten Unterauftragsverarbeiter. Klardaten stellt die Liste mit Name, Zweck der Verarbeitung, Sitz, Verarbeitungsort und etwaigen Drittlandübermittlungen bereit.

(2) Klardaten informiert den Kunden mindestens 30 Tage vor dem Einsatz neuer oder wesentlich geänderter Unterauftragsverarbeiter. Handelt der Kunde selbst im Auftrag, leitet er die Mitteilung so rechtzeitig weiter, dass der Verantwortliche vor dem Einsatz widersprechen kann. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund widersprechen; findet sich keine angemessene Lösung, kann der Kunde den betroffenen Dienst kündigen.

(3) Klardaten verpflichtet Unterauftragsverarbeiter nach Art. 28 Abs. 4 DSGVO mindestens in dem Umfang, in dem Klardaten gegenüber dem Kunden verpflichtet ist.

(4) Klardaten überprüft Unterauftragsverarbeiter risikobasiert und stellt dem Kunden auf Anfrage angemessene Nachweise zur Verfügung, soweit verfügbar. Ein unmittelbares Audit- oder Zutrittsrecht des Kunden gegenüber Unterauftragsverarbeitern besteht nur, soweit der jeweilige Unterauftragsverarbeiter dies ermöglicht.

V. Sub-processors

(1) The Customer approves the use of the subprocessors named in the current list of subprocessors. Klardaten shall provide the list, including the name, purpose of processing, registered office, place of processing, and any third-country transfers.

(2) Klardaten shall inform the Customer at least 30 days before engaging new subprocessors or making material changes to existing subprocessors. Where the Customer itself acts as a processor, it forwards the notice in time for the controller to object before the change takes effect. The Customer may object on important data protection grounds; if no appropriate solution can be found, the Customer may terminate the affected service.

(3) Klardaten shall contractually bind subprocessors pursuant to Art. 28(4) GDPR at least to the same extent as Klardaten is bound towards the Customer.

(4) Klardaten shall review subprocessors on a risk-based basis and provide the Customer with appropriate evidence upon request, to the extent available. The Customer shall have a direct audit or access right against subprocessors only to the extent that the respective subprocessor permits this.

VI. Geheimhaltungs-verpflichtung

(1) Sämtliche Informationen, Dokumente, Mitteilungen, Auskünfte und Daten, die der Dienstleister vom Auftraggeber sowie seinen Bevollmächtigten oder sonstigen Personen zur Erfüllung der Dienstleistung erhält, werden vom Dienstleister streng vertraulich behandelt und geheim gehalten.

VI Confidentiality obligation

(1) All information, documents, notifications, information and data that the service provider receives from the client and its authorized representatives or other persons for the performance of the service shall be treated as strictly confidential and kept secret by the service provider.

Anlage 1: Gegenstand der Dienstleistung

(1) Der Dienstleister stellt dem Auftraggeber eine Schnittstelle zu DATEV zur Verfügung.

(2) Abhängig von den freigeschalteten DATEV-Modulen und den vom Auftraggeber angewiesenen Verarbeitungsvorgängen kann der Dienstleister die folgenden Kategorien personenbezogener Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und nur insoweit verarbeiten, wie dies zur Erbringung der vereinbarten Dienste erforderlich ist:
Stamm- und Kontaktdaten (z. B. Name, Anschrift, E-Mail-Adresse und Telefonnummer); Mandanten-, Berater- und Benutzerkennungen; Metadaten zu Mandaten und Berechtigungen; Abrechnungs-, Buchhaltungs- und Lohn- und Gehaltsdaten, einschließlich Buchungssätzen, Konten, Vergütungs- und Entgeltbestandteilen, Sozialversicherungsnummern, steuerlichen Identifikationsnummern, Religionszugehörigkeit und Abwesenheitsdaten einschließlich der Gründe für Abwesenheiten, soweit diese erfasst werden; in Dokumenten und Anhängen enthaltene Daten, die über die Dienste bereitgestellt werden, einschließlich Dokumentinhalten und Metadaten; sowie technische Kommunikations- und Protokolldaten (z. B. Zeitstempel, Request-IDs und Fehlercodes).
Die Daten können besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 DSGVO umfassen, insbesondere Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen, einschließlich der Religionszugehörigkeit, sowie Gesundheitsdaten, soweit diese in Abwesenheitsdaten oder Dokumentinhalten enthalten sind.

Annex 1: Object of the service

(1) The Service Provider shall provide the Client with an interface to DATEV.

(2) Depending on the DATEV modules enabled and the processing operations instructed by the Controller, the Service Provider may process the following categories of personal data, solely on the Controller's documented instructions and to the extent necessary to provide the agreed Services:

Master data and contact details (e.g., name, address, email address and telephone number); client, advisor and user identifiers; mandate and permission metadata; billing, accounting and payroll data, including posting records, accounts, remuneration and compensation components, social security numbers, tax identification numbers, religious affiliation and absence records, including reasons for absence where recorded; data contained in documents and attachments made available through the Services, including document contents and metadata; and technical communication and log data (e.g., timestamps, request IDs and error codes).

The data may include special categories of personal data within the meaning of Article 9(1) GDPR, in particular data revealing religious or philosophical beliefs, including religious affiliation, and health data where included in absence records or document contents.

(3) Von der Verarbeitung der Daten betroffen sind:

Mandanten des Auftraggebers (Unternehmen und deren Ansprechpartner), Mitarbeiter der Mandanten oder Auftraggeber, ggf. Kunden/Lieferanten der Mandanten sowie Nutzer des DATEV-Systems (z. B. Kanzlei-/Mandanten-User).

(3) The following are affected by the processing of the data:

The Controller's clients (companies and their contact persons), employees of the clients or the Controller, where applicable the clients' customers/suppliers, as well as users of the DATEV system (e.g., firm/client users).

Anlage 2: Technisch-organisatorische Maßnahmen (TOM)

Die Verarbeitung erfolgt in einer bei Unterauftragnehmern (z. B. AWS, Hetzner) gehosteten Cloud-Umgebung. Physische Rechenzentrumssicherheit erfolgt durch den Unterauftragnehmer; Zugriffe auf die Klardaten-Anwendung werden durch Klardaten geregelt.

Klardaten speichert keine fachlichen Kundendaten (z. B. Buchhaltungs-/Steuerdaten) dauerhaft. Technisch erforderliche Daten können temporär verarbeitet werden (z. B. zur Übertragung/Störungsbehebung) sowie Protokolldaten (Logs) zur Sicherheit und Nachvollziehbarkeit, jeweils nach dem Prinzip der Datenminimierung und soweit möglich ohne Inhaltsdaten.

Annex 2: Technical and Organizational Measures (TOM)

Processing takes place in a cloud environment hosted by sub-processors (e.g., AWS, Hetzner). Physical data center security is provided by the sub-processor; access to the Klardaten application is governed by Klardaten.

Klardaten does not store substantive customer data (e.g., accounting/tax data) on a permanent basis. Technically necessary data may be processed temporarily (e.g., for transmission/incident resolution) as well as log data for security and traceability, in each case in accordance with the principle of data minimization and, where possible, without content data.

I. Grundsätze

(1) Keine Verarbeitung auf lokalen Systemen
Mitarbeitende der Klardaten GmbH speichern oder verarbeiten personenbezogene Daten nicht lokal. Auf Endgeräten werden keine Daten dauerhaft abgelegt. Zugriffe erfolgen ausschließlich über gesicherte, verschlüsselte Verbindungen in die gehostete Cloud-Umgebung.

(2) Technischer Stand
Alle beschriebenen Maßnahmen entsprechen dem aktuellen Stand der Technik und werden regelmäßig überprüft und angepasst (Art. 32 DSGVO).

I. Principles

(1) No Processing on Local Systems
Employees of Klardaten GmbH neither store nor process personal data locally. No data are permanently stored on end devices. Access occurs solely via secure, encrypted connections to the hosted cloud environment.

(2) Technical State of the Art
All measures described correspond to the current state of the art and are reviewed and adjusted regularly in accordance with Art. 32 GDPR.

II. Technisch-organisatorische Maßnahmen

1. Vertraulichkeit

(1) Zutrittskontrolle
Physischer Zutritt zu Datenverarbeitungsanlagen erfolgt ausschließlich in den Rechenzentren der Unterauftragnehmer (AWS, Hetzner) mit mehrstufigen Zutrittskontrollen (biometrisch, Zugangskarten, Videoüberwachung).

(2) Zugangskontrolle
Systemzugriffe auf produktive Systeme erfolgen ausschließlich über personalisierte Konten mit Mehrfaktor-Authentifizierung (MFA).
Zugänge sind rollenbasiert, protokolliert und werden regelmäßig überprüft.

(3) Zugriffskontrolle
Administrativer Zugriff erfolgt über gesicherte VPN- und SSH-Verbindungen mit Public/Private-Key-Authentifizierung.
Administrative Aktionen werden in angemessenem Umfang protokolliert und gegen unbefugte Veränderung geschützt.

(4) Pseudonymisierung und Verschlüsselung
Sämtliche gespeicherten Daten werden sowohl bei Übertragung (TLS 1.2+) als auch im Ruhezustand (AES-256) verschlüsselt.
Pseudonymisierung oder Anonymisierung erfolgt, soweit technisch sinnvoll und vertraglich vereinbart.

II. Technical and Organizational Measures

1. Confidentiality

(1) Physical Access Control
Physical access to data processing facilities is restricted to the subcontractors' data centers (AWS, Hetzner) and protected by multi-level controls (biometric identification, access cards, video surveillance).

(2) System Access Control
Access to production systems is restricted to personalized accounts with multi-factor authentication (MFA).
Access rights are role-based, logged, and reviewed regularly.

(3) Data Access Control
Administrative access occurs via secured VPN and SSH connections with public/private key authentication.
Administrative actions are logged to an appropriate extent and protected against unauthorized modification.

(4) Pseudonymization and Encryption
All data are encrypted during transmission (TLS 1.2+) and at rest (AES-256).
Pseudonymization or anonymization is applied when technically feasible and contractually agreed upon.

2. Integrität und Verfügbarkeit

(1) Verfügbarkeitskontrolle
Mehrstufige Backup-Strategie mit redundanter Speicherung in getrennten Verfügbarkeitszonen. Regelmäßige Tests zur Wiederherstellung.

(2) Systemhärtung und Patchmanagement
Betriebssysteme und Serverkomponenten werden kontinuierlich aktualisiert. Sicherheitsupdates werden zeitnah eingespielt.

(3) Monitoring und Logging
Zentrale Überwachung sämtlicher Systeme (CPU, Netzwerk, Fehler, Security Events). Ungewöhnliche Aktivitäten werden automatisiert erkannt und analysiert.

(4) Incident Response und Notfallmanagement
Es existieren dokumentierte Prozesse für Sicherheitsvorfälle, inklusive Eskalationsstufen, Dokumentation und Benachrichtigung des Auftraggebers gemäß Art. 33, 34 DSGVO.

2. Integrity and Availability

(1) Availability Control
A multi-tiered backup strategy with redundant storage across separate availability zones is implemented. Regular recovery tests are conducted.

(2) System Hardening and Patch Management
Operating systems and server components are continuously updated. Security patches are applied without undue delay.

(3) Monitoring and Logging
All systems (CPU, network, errors, and security events) are centrally monitored. Unusual activities are automatically detected and analyzed.

(4) Incident Response and Emergency Management
Documented processes exist for handling security incidents, including escalation levels, documentation, and notification of the client in accordance with Articles 33 and 34 GDPR.

3. Endgeräteschutz und Zugriffssicherheit

(1) Endgeräteverwaltung
Die Geräteverschlüsselung (z. B. FileVault, BitLocker) ist verpflichtend.

(2) Netzwerksicherheit
Verbindungen zu produktiven Systemen erfolgen ausschließlich über verschlüsselte Verbindungen.
Öffentliche oder ungesicherte Netzwerke sind untersagt.

(3) Datenträger- und Wechseldatenträgerkontrolle
Externe Speichermedien sind standardmäßig deaktiviert. Nutzung nur nach Freigabe und mit Verschlüsselung erlaubt.

(4) Sicherheitsrichtlinien
Starke Passwortvorgaben, automatische Bildschirmsperren nach Inaktivität, regelmäßige Sicherheitsüberprüfungen.

(5) Schulung und Sensibilisierung
Alle Mitarbeitenden werden regelmäßig zu Datenschutz, IT-Sicherheit und Umgang mit personenbezogenen Daten geschult.

3. Endpoint Protection and Access Security

(1) Device Management
Device encryption (e.g., FileVault, BitLocker) is mandatory.

(2) Network Security
Connections to production systems occur exclusively via encrypted connections.
Use of public or unsecured networks is prohibited.

(3) Removable Media Control
External storage media are disabled by default. Use is permitted only with explicit approval and encryption.

(4) Security Policies
Strong password requirements, automatic screen locks after inactivity, and regular security reviews are enforced.

(5) Training and Awareness
All employees receive regular training on data protection, IT security, and the proper handling of personal data.

4. Weitere organisatorische Maßnahmen

(1) Berechtigungsmanagement
Zugriffsrechte nach dem „Need-to-know"-Prinzip. Rollen werden dokumentiert, Änderungen nachvollziehbar versioniert.

(2) Audits und Überprüfungen
Jährliche interne Sicherheitsüberprüfungen, Dokumentation von Verbesserungsmaßnahmen, ggf. externe Penetrationstests.

(3) Vertraulichkeitsverpflichtung
Alle Mitarbeitenden der Klardaten GmbH sind vor Tätigkeitsaufnahme schriftlich auf Vertraulichkeit und Weisungsbindung verpflichtet (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO).
Soweit mitwirkende Personen Zugang zu Berufsgeheimnissen erhalten können, werden mitwirkende Personen zusätzlich nach § 203 StGB verpflichtet.

(4) Datenschutzfreundliche Voreinstellungen Systeme sind standardmäßig so konfiguriert, dass nur erforderliche personenbezogene Daten verarbeitet werden (Privacy by Default).

4. Additional Organizational Measures

(1) Access Rights Management
Access rights are granted on a strict need-to-know basis. Roles are documented, and all changes are version-controlled.

(2) Audits and Reviews
Annual internal security audits are performed. Results and corrective actions are documented; external penetration tests are conducted when appropriate.

(3) Confidentiality Commitment
All employees of Klardaten GmbH are, prior to commencing their duties, contractually bound in writing to confidentiality and to processing only on documented instructions (Art. 28(3)(b), Art. 29, Art. 32(4) GDPR).
Where persons involved may gain access to professional secrets, any persons involved will additionally be bound under Section 203 of the German Criminal Code (StGB).

(4) Privacy by Default
Systems are configured by default to ensure that only necessary personal data are processed.

5. Löschung und Aufbewahrung

(1) Löschungsfristen
Personenbezogene Daten werden nach Vertragsende oder auf Weisung des Auftraggebers unverzüglich gelöscht, sofern keine gesetzlichen Aufbewahrungsfristen entgegenstehen.

Backups werden nicht gezielt wiederhergestellt, es sei denn, dies ist aus Sicherheits-, Nachweis- oder Wiederherstellungsgründen erforderlich. Personenbezogene Daten in Backups werden nach dem regulären Backup-Zyklus überschrieben oder gelöscht.

(2) Löschprotokolle
Löschvorgänge werden dokumentiert und auf Anforderung nachgewiesen.

5. Deletion and Retention

(1) Deletion Periods
Personal data are deleted immediately after termination of the contract or upon instruction from the client, unless legal retention requirements apply.

Backups shall not be selectively restored unless this is necessary for security, evidentiary, or recovery reasons. Personal data contained in backups shall be overwritten or deleted in accordance with the regular backup cycle.

(2) Deletion Records
Deletion procedures are documented and can be demonstrated upon request.

Anlage 3: Unterauftrags-verarbeiterliste

1. Amazon Web Services EMEA SARL
Zweck: Hosting, Infrastruktur
Sitz: Luxemburg
Verarbeitungsregion: Frankfurt / EU
Drittlandtransfer: nein, da EU-Region genutzt wird

2. Hetzner Online GmbH
Zweck: Hosting, Infrastruktur
Sitz: Deutschland
Verarbeitungsregion: Nürnberg / EU
Drittlandtransfer: nein

3. Microsoft Ireland Operations Limited
Zweck: Microsoft Azure, Azure OpenAI Services, ggf. KI-gestützte Verarbeitung
Sitz: Irland
Verarbeitungsregion: Deutschland / EU, ggf. Schweden oder Frankreich

Drittlandtransfer: nein, da EU-Region genutzt wird

Zusatz: German Data Secrecy Amendment / Zusatzvereinbarung für Berufsgeheimnisträger, soweit einschlägig

Annex 3: List of Subprocessors

1. Amazon Web Services EMEA SARL
Purpose: Hosting, infrastructure
Registered office: Luxembourg
Processing region: Frankfurt / EU
Third-country transfer: no, as an EU region is used

2. Hetzner Online GmbH
Purpose: Hosting, infrastructure
Registered office: Germany
Processing region: Nuremberg / EU
Third-country transfer: no

3. Microsoft Ireland Operations Limited
Purpose: Microsoft Azure, Azure OpenAI Services, and, where applicable, AI-supported processing
Registered office: Ireland
Processing region: Germany / EU, where applicable Sweden or France

Third-country transfer: no, as an EU region is used

Addendum: German Data Secrecy Amendment / Addendum for Professional Secrecy Obligations, where applicable

Anlage 4: Beauftragungskette

Leistung oder Installation

_____

Beteiligte in Reihenfolge der Beauftragung (Firma oder Name und Rolle je Stufe)

1. _____
2. _____
3. _____
4. _____

Weisungskontakt (Name oder Funktion und E-Mail)

_____

Annex 4: Chain of Engagement

Service or installation

_____

Parties in order of engagement (company or name and role at each stage)

1. _____
2. _____
3. _____
4. _____

Contact for instructions (name or role and email)

_____