POWERHANDWERK · EINE MARKE DER KETESO GMBH

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Anlage 2a zum Auftragsverarbeitungsvertrag (AVV, Anlage 2) · Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

PH-TOM v1.1 · Stand 07.07.2026 · Status: Freigegeben zur Verwendung

VORBEMERKUNG

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die KETESO nach Art. 32 DSGVO getroffen hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Berücksichtigt werden der Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung und die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Die operative Verarbeitung erfolgt innerhalb der von KETESO kontrollierten Systeme. Die zugrunde liegende Cloud-Infrastruktur wird über den Unter-Auftragsverarbeiter Amazon Web Services bereitgestellt (AWS-Konto der KETESO GmbH, Konto-Nr. 603433800788, Region eu-central-1, Frankfurt am Main); insoweit gelten zusätzlich dessen zertifizierte Maßnahmen (siehe § 7).

Das AWS-Konto wird derzeit ausschließlich für die KI-gestützte Verarbeitung über Amazon Bedrock genutzt (§ 1.5, § 3.1). Eine dauerhafte Speicherung personenbezogener Auftragsdaten in AWS-Speicher- oder Datenbankdiensten findet zum Stand dieser Fassung nicht statt; werden solche Datenbestände in Betrieb genommen, gelten die in § 3 und § 6 festgelegten Backup- und Löschregeln ab Inbetriebnahme.

§ 1 VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

1.1 Zutrittskontrolle (Schutz vor unbefugtem physischem Zutritt)

Ziel: Unbefugten ist der physische Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

- Die produktive Datenverarbeitung erfolgt nicht in eigenen Räumlichkeiten der KETESO, sondern in den Rechenzentren des Unter-Auftragsverarbeiters AWS (Region eu-central-1). Dort gelten dessen zertifizierte Zutrittskontrollen (u. a. mehrstufige Zugangskontrolle, Videoüberwachung, 24/7-Bewachung; vgl. AWS-Zertifizierungen ISO 27001, SOC 2, C5). Nachweis über AWS-Compliance-Berichte (siehe § 7).
- Arbeitsplätze, an denen auf Verarbeitungssysteme zugegriffen wird: Die Arbeitsplätze befinden sich in abschließbaren Geschäfts- bzw. Arbeitsräumen ohne Publikumsverkehr am Sitz der KETESO und der mit der Leistungserbringung befassten Personen. Zutritt nur für berechtigte Personen; Besucher halten sich nicht unbeaufsichtigt in Räumen mit Zugriff auf Verarbeitungssysteme auf.
- Sperrung der Arbeitsplätze bei Verlassen (automatische Bildschirmsperre, siehe § 1.2); keine offene Ablage von Zugangsdaten oder personenbezogenen Unterlagen (Clean-Desk-Grundsatz).

1.2 Zugangskontrolle (Schutz vor unbefugter Systemnutzung)

Ziel: Verhinderung, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Persönliche, individuelle Benutzerkonten für alle Beschäftigten und eingesetzten Personen; keine geteilten Sammelkonten. Im AWS-Konto: individuelle IAM-Identitäten, keine Nutzung des Root-Kontos im Tagesbetrieb.
- Das Root-Konto des AWS-Kontos ist mit Multi-Faktor-Authentifizierung (MFA) gesichert. Für Konsolenzugänge gilt eine kontoweite Passwortrichtlinie (Mindestlänge 14 Zeichen, Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen, Wiederverwendungssperre der letzten 5 Passwörter).
- Zwei-Faktor-Authentifizierung (2FA/MFA) für den Zugang zu Verwaltungs- und Cloud-Konsolen sowie zum Google-Unternehmensprofil-Manager (Google-Konten mit 2FA).
- Zugangsdaten werden in einem Passwortmanager mit individuellen Zugängen verwaltet; keine Klartext-Ablage von Passwörtern.
- Automatische Bildschirmsperre nach Inaktivität; vollverschlüsselte Endgeräte (Festplattenvollverschlüsselung, macOS FileVault bzw. Windows BitLocker) mit automatischen Sicherheitsupdates.
- Sperrung von Zugängen bei Ausscheiden oder Wegfall der Berechtigung unverzüglich.

1.3 Zugriffskontrolle (Berechtigungskonzept)

Ziel: Gewährleistung, dass die zur Nutzung Berechtigten ausschließlich auf die ihrer Berechtigung unterliegenden Daten zugreifen können.

- Rollen- und rechtebasiertes Berechtigungskonzept nach dem Prinzip der geringsten Rechte (least privilege) und dem Need-to-know-Prinzip.
- Trennung von administrativen und operativen Rechten; restriktive Vergabe administrativer Berechtigungen.
- Regionsbindung auf Infrastrukturebene: Im AWS-Konto ist eine verbindliche IAM-Richtlinie (“DenyOutsideFrankfurt”) hinterlegt, die sämtliche Dienst-Aktionen außerhalb der Region eu-central-1 technisch verweigert. Ausnahmen bestehen nur für globale Verwaltungsdienste (wie IAM und Abrechnung) sowie für den Aufruf der KI-Inferenz über Amazon Bedrock, der durch ein eigenes Richtlinien-Statement auf die EU-Regionen des EU-Inferenzprofils beschränkt ist (§ 1.5); jede Verarbeitung außerhalb der EU bleibt technisch verweigert. Die Richtlinie ist allen IAM-Identitäten und der Administratorengruppe zugewiesen.
- Protokollierung sicherheitsrelevanter Zugriffe und administrativer Tätigkeiten: Sämtliche Verwaltungsaktionen im AWS-Konto werden über AWS CloudTrail (Management Events, Region eu-central-1) revisionssicher protokolliert (Log-Datei-Validierung aktiviert); Aufbewahrung der Protokolle 365 Tage (siehe § 2.2).
- Regelmäßige Überprüfung und Aktualisierung der Berechtigungen (Turnus siehe § 4).
- Verbot der lokalen, KETESO-fremden Speicherung personenbezogener Auftragsdaten; Verarbeitung ausschließlich innerhalb der KETESO-kontrollierten Systeme.

1.4 Trennungskontrolle (Mandantentrennung)

Ziel: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken bzw. für unterschiedliche Kunden erhoben wurden.

- Logische Trennung der Daten unterschiedlicher Kunden (Mandantentrennung) auf System- bzw. Datenbankebene.
- Trennung von Produktiv-, Test- und Entwicklungsumgebungen; in Test-/Entwicklungsumgebungen werden keine echten personenbezogenen Produktivdaten verwendet, soweit nicht unvermeidbar; ggf. Pseudonymisierung/Anonymisierung.
- Zweckbindung der Verarbeitung gemäß Weisung des Verantwortlichen.

1.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Verschlüsselung der Datenübertragung über öffentliche Netze (TLS/HTTPS).
- Verschlüsselung gespeicherter Daten (Encryption at rest): AWS-Speicherdienste werden mit serverseitiger Verschlüsselung betrieben. Blockspeicher (EBS) ist kontoweit standardmäßig verschlüsselt (Encryption-by-default); Objektspeicher (S3) mit serverseitiger Verschlüsselung (SSE, AES-256).

- Schlüsselmanagement: Die Verschlüsselung erfolgt über von AWS verwaltete Schlüssel des AWS Key Management Service (AWS-managed KMS-Keys) mit automatischer, von AWS durchgeführter jährlicher Schlüsselrotation. Kundenspezifische Schlüssel (Customer-managed Keys) werden ergänzt, sobald Datenbestände dies erfordern.
- KI-gestützte Verarbeitung: Die KI-Verarbeitung erfolgt über Amazon Bedrock unter Verwendung von EU-Inferenzprofilen (Modellzugriff ausschließlich über EU-Regionen). Amazon Bedrock speichert die übermittelten Ein- und Ausgaben nicht dauerhaft und verwendet sie nicht zum Training von Modellen; die Verarbeitung ist insoweit zustandslos.
- Verschlüsselung der Endgeräte (Festplattenvollverschlüsselung, siehe § 1.2).
- Pseudonymisierung, soweit für den jeweiligen Verarbeitungszweck möglich und sinnvoll (z. B. in Auswertungs-/Berichtsdaten).

---

§ 2 INTEGRITÄT (ART. 32 ABS. 1 LIT. B DSGVO)

2.1 Weitergabekontrolle

Ziel: Gewährleistung, dass personenbezogene Daten bei elektronischer Übertragung oder während ihres Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Transportverschlüsselung (TLS) für sämtliche Datenübertragungen.
- Datenhaltung und Infrastruktur ausschließlich in der Region eu-central-1; die KI-Inferenz über EU-Inferenzprofile erfolgt ausschließlich in EU-Regionen. Keine standardmäßige Weitergabe in Drittländer (siehe AVV § 8 Abs. 2). Die Regionsbindung ist technisch erzwungen (IAM-Richtlinie “DenyOutsideFrankfurt”, § 1.3).
- Protokollierung von Datenübertragungen an Schnittstellen, soweit technisch vorgesehen.

2.2 Eingabekontrolle

Ziel: Nachvollziehbarkeit, ob und von wem personenbezogene Daten in Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung von Eingabe, Änderung und Löschung sicherheitsrelevanter Daten (Logging): Verwaltungsaktionen im AWS-Konto werden über AWS CloudTrail mit aktivierter Log-Datei-Validierung protokolliert; die Protokolle werden in einem zugriffsbeschränkten, verschlüsselten S3-Bucket abgelegt.
- Zuordnung der Verarbeitungsvorgänge zu individuellen Benutzerkonten (§ 1.2).
- Aufbewahrung der Protokolle: 365 Tage; danach automatische Löschung über eine S3-Lifecycle-Regel (Datensparsamkeit, Art. 5 Abs. 1 lit. e DSGVO).

---

§ 3 VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B UND C DSGVO)

3.1 Verfügbarkeitskontrolle

Ziel: Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust.

- Redundante Infrastruktur des Unter-Auftragsverarbeiters AWS (mehrere Verfügbarkeitszonen innerhalb der Region eu-central-1).
- Schutzmaßnahmen der Cloud-Infrastruktur gegen Stromausfall, Brand und Wasser (durch AWS-Rechenzentren gewährleistet).
- Backup-Konzept: Zum Stand dieser Fassung werden keine personenbezogenen Auftragsdaten dauerhaft in AWS-Speicher- oder Datenbankdiensten gehalten (die KI-Verarbeitung ist zustandslos, § 1.5); ein gesonderter Backup-

Bestand ist insoweit nicht erforderlich. Für produktive Datenbestände gilt ab deren Inbetriebnahme verbindlich: tägliche automatisierte Sicherungen, Aufbewahrung der Sicherungen 35 Tage, Ablage getrennt vom Produktivsystem (gesonderter Backup-Speicher innerhalb der Region eu-central-1), mindestens jährlicher Wiederherstellungstest mit Dokumentation.

- Einsatz von Schutzsoftware und Systemhärtung auf Endgeräten (aktuelle Betriebssystem-Sicherheitsmechanismen, automatische Updates, Firewall).

3.2 Wiederherstellbarkeit (Rasche Wiederherstellung)

Ziel: Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

- Wiederherstellungsverfahren aus Backups definiert; Zielwerte für produktive Datenbestände: Wiederanlaufzeit (RTO) höchstens 24 Stunden, maximaler Datenverlust (RPO) höchstens 24 Stunden (entsprechend dem täglichen Sicherungszyklus).
- Die Wiederherstellbarkeit wird im Rahmen des jährlichen Wiederherstellungstests (§ 3.1) überprüft und dokumentiert.

3.3 Belastbarkeit der Systeme

- Nutzung skalierbarer, belastbarer Cloud-Infrastruktur (AWS), die auf Lastschwankungen reagieren kann.
- Monitoring der Systeme auf Verfügbarkeit und Auffälligkeiten; Kosten- und Anomalie-Überwachung des AWS-Kontos über Budget-Alarme.

---

§ 4 VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DSGVO)

- Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen: mindestens jährlich sowie anlassbezogen (insbesondere bei wesentlichen Änderungen der Systeme oder nach Sicherheitsvorfällen). Verantwortlich: die Geschäftsführung der KETESO GmbH.
- Verpflichtung aller mit der Verarbeitung befassten Personen auf das Datengeheimnis bzw. die Vertraulichkeit (Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO) sowie Sensibilisierung/Unterweisung zum Datenschutz.
- Auftragskontrolle: Verarbeitung im Auftrag nur nach dokumentierter Weisung; eindeutige Vertragsgestaltung; Auswahl von Unter-Auftragsverarbeitern nach Eignung (Art. 28 Abs. 1 DSGVO) und vertragliche Verpflichtung auf dasselbe Schutzniveau (Art. 28 Abs. 4 DSGVO).
- Verfahren zur Behandlung von Datenschutzvorfällen (Incident-Response) einschließlich Meldewegen nach AVV § 10.
- Berücksichtigung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO).

---

§ 5 AUFTRAGS-/WEISUNGSKONTROLLE

- Verarbeitung personenbezogener Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen (siehe AVV § 5).
- Schriftliche bzw. textformgebundene Fixierung der Weisungen; Erstweisung durch Hauptvertrag und Leistungsschein (Anlage 1).
- Klare Zuständigkeiten und Ansprechpartner für Datenschutzfragen: Datenschutz-Kontakt der KETESO ist info@keteso.com; verantwortlich ist die Geschäftsführung.

§ 6 LÖSCHKONZEPT (ART. 17, ART. 5 ABS. 1 LIT. E DSGVO; UMSETZUNG VON AVV § 11)

Ziel: Sicherstellung, dass personenbezogene Daten gelöscht werden, sobald der Zweck entfällt oder die nach AVV § 11 getroffene Wahl des Verantwortlichen dies verlangt, und dass die Löschung technisch nachvollziehbar und vollständig (einschließlich Sicherungskopien) erfolgt.

6.1 Löschauslöser und Löschfristen

- **Vertragsende:** Nach Beendigung des Hauptvertrags werden die im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen gelöscht oder zurückgegeben (AVV § 11 Abs. 1). Trifft der Verantwortliche binnen 30 Tagen keine Wahl, erfolgt Löschung.
- **Zweckfortfall während der Laufzeit:** Daten, die für die laufende Profilpflege nicht mehr benötigt werden (z. B. nicht mehr benötigtes Bild-/Textmaterial des Kunden), werden nach Erledigung des jeweiligen Vorgangs gelöscht.
- **Protokolldaten/Logs:** Automatische Löschung nach 365 Tagen (§ 2.2).
- **Gesetzliche Aufbewahrungspflichten:** Daten, die aufgrund gesetzlicher Pflichten weiter aufzubewahren sind, werden bis zum Ablauf der Frist gesperrt und sodann gelöscht (AVV § 11 Abs. 3).

6.2 Technische Umsetzung der Löschung

- Löschung der Datensätze in den produktiven Datenbank- und Speicherdiensten der Cloud-Umgebung (AWS, eu-central-1). Bei der KI-Verarbeitung über Amazon Bedrock entstehen keine dauerhaft gespeicherten Ein-/Ausgabedaten (zustandslose Verarbeitung, § 1.5); insoweit bedarf es keiner gesonderten Löschung.
- Automatisierte Löschroutinen: Protokolldaten werden über S3-Lifecycle-Regeln automatisch nach Fristablauf gelöscht. Für künftige produktive Datenbestände werden Löschroutinen auf Datensatzebene (Löschung auf Weisung bzw. bei Vertragsende) sowie Lifecycle-Regeln für Speicherdienste eingerichtet; verschlüsselte Datenbestände können ergänzend durch Vernichtung der zugehörigen Schlüssel unbrauchbar gemacht werden (Crypto-Shredding), soweit Customer-managed Keys eingesetzt werden.
- Berücksichtigung von Sicherungskopien (Backups): Sicherungskopien, die gelöschte Daten noch enthalten, werden nach Ablauf des Backup-Aufbewahrungszyklus von 35 Tagen (§ 3.1) überschrieben bzw. gelöscht; die endgültige Löschung aus Sicherungskopien ist damit spätestens 35 Tage nach der Löschung im Produktivsystem abgeschlossen. Bis dahin sind Sicherungskopien gegen Wiederherstellung in den Produktivbetrieb geschützt (Wiederherstellung nur im dokumentierten Notfall-/Wiederanlaufverfahren).
- Berücksichtigung der vom Kunden bereitgestellten Materialien und etwaiger Exporte/Berichte: Löschung an allen Ablageorten innerhalb der KETESO-kontrollierten Systeme.

6.3 Verantwortlichkeit und Nachweis

- Verantwortlich für die Durchführung der Löschung: die Geschäftsführung der KETESO GmbH.
- KETESO bestätigt die Löschung oder Rückgabe auf Verlangen des Kunden in Textform (AVV § 11 Abs. 4).
- Die Durchführung der Löschungen wird dokumentiert.

§ 7 MASSNAHMEN DES UNTER-AUFTRAGSVERARBEITERS (AWS, EU-CENTRAL-1)

- Die produktive Infrastruktur wird durch Amazon Web Services in der Region eu-central-1 (Frankfurt am Main) bereitgestellt. AWS unterhält ein umfassendes, durch unabhängige Stellen zertifiziertes Sicherheitsprogramm (u. a. ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1/2/3, BSI C5).
- Der Nachweis der Maßnahmen des Unter-Auftragsverarbeiters erfolgt über dessen öffentlich verfügbare bzw. auf Anforderung bereitgestellte Compliance-Berichte und Zertifikate (siehe AVV § 12 Abs. 2).

- Die Verarbeitung erfolgt ausschließlich in EU-Regionen (Datenhaltung: eu-central-1; KI-Inferenz: EU-Inferenzprofile); kein Drittlandtransfer im Standardbetrieb (siehe AVV § 8 Abs. 2).

Dokument PH-TOM, Version 1.1, Stand 07.07.2026, Status: Freigegeben zur Verwendung (anwaltlich geprüfte Fassung).