

Anlage 1 zum Auftragsverarbeitungsvertrag

Technische und organisatorische Maßnahmen (TOM)

Stand

11. Oktober 2026

Herausgeber

IonKon GmbH

Inhalt

Übersicht	3
1.1 Zutrittskontrolle (physisch)	3
1.2 Zugangskontrolle (Systeme)	3
1.3 Zugriffskontrolle (Berechtigungen)	3
1.4 Trennungskontrolle	4
1.5 Pseudonymisierung und Datenminimierung	4
2.1 Weitergabekontrolle (Transport)	4
2.2 Speicherverschlüsselung	5
2.3 Eingabekontrolle	5
3 Verfügbarkeit und Belastbarkeit	5
4.1 Entwicklungs- und Änderungsprozess	5
4.2 Löschkonzept	6
4.3 Auftragskontrolle (Subauftragsverarbeiter)	6

Übersicht

Anlage 1 zum Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 lit. c, Art. 32 DSGVO.

Auftragsverarbeiter ist die IonKon GmbH, Dessauer Straße 280, 06886 Lutherstadt Wittenberg.

Gegenstand der Verarbeitung: Einmalige Verarbeitung der vom Kunden bereitgestellten Dokumente zur Erzeugung eines kundenindividuellen Sprachmodells, Auslieferung auf einem lokalen KI-Server, anschließende Löschung. Nach der Lieferung findet keine laufende Verarbeitung von Kundendaten durch IonKon statt; das Modell arbeitet vollständig beim Kunden.

1.1 Zutrittskontrolle (physisch)

- Kundendaten werden ausschließlich in Rechenzentren von Infrastrukturpartnern in der EU oder der Schweiz verarbeitet und gespeichert; ein eigener Serverbetrieb mit Kundendaten in Geschäftsräumen findet nicht statt.
- Physische Sicherheit der Rechenzentren liegt bei den Infrastrukturpartnern; das Verzeichnis der eingesetzten Subauftragsverarbeiter mit Sitz und Zweck steht in Nummer 7 des AVV sowie in Nummer 4.3 dieser TOM.
- Geräterichtlinie: Arbeitsgeräte der Mitarbeitenden sind mit Festplattenverschlüsselung und automatischer Bildschirmsperre gesichert.

1.2 Zugangskontrolle (Systeme)

- Zugriff auf Produktionssysteme ist auf einen minimalen, namentlich dokumentierten Personenkreis beschränkt; die Aufstellung wird auf Anfrage offengelegt.
- Programmatischer Zugriff auf die Trainings-API nur mit geheimen API-Schlüsseln (mindestens 32 Byte Zufall); Schlüssel werden nicht im Quellcode, sondern ausschließlich als Umgebungsvariablen bzw. aus einem Secret-Store bereitgestellt. Ein automatischer Härtetest verweigert den Produktionsstart mit Platzhalter- oder Kurzschlüsseln.
- Integrationsschnittstelle für das eigene Kundenverwaltungssystem: Zugriff nur mit Zugangsdaten, die je Verwendungszweck ausgestellt und auf einzelne Berechtigungen begrenzt werden (Lesen von Aufträgen, Lesen von Kundendaten, Aktivierung, Auftragssteuerung).
- Kundenportal: passwortbasierte Konten (scrypt), E-Mail-Verifizierung vor Bestellung, Einmal-Tokens (gehasht, einmalverwendbar) für Anmelde- und Zurücksetz-Links, Brute-Force-Begrenzung je E-Mail- und IP-Kombination.

1.3 Zugriffskontrolle (Berechtigungen)

- Die Integrationsschnittstelle prüft je Aufruf die ausgestellte Berechtigung; jeder Zugriff wird mit Zeitpunkt, Ergebnis und betroffenem Datensatz protokolliert.
- Datenbankzugriffe nach dem Least-Privilege-Prinzip: Das Laufzeit-Credential der Anwendung besitzt keine Schemarechte (DDL); Migrationen laufen über ein getrenntes Credential in einem separaten, einmaligen Migrationsschritt. Ein versioniertes Prüfskript kontrolliert die Rechtevergabe fail-closed.

-
- Das Auditprotokoll ist ausschließlich anfügend; nachträgliche Änderungen sind durch Datenbankrechte ausgeschlossen.

1.4 Trennungskontrolle

- Strikte Silo-Trennung pro Kunde: Jeder Auftrag erzeugt ein eigenes Modell ausschließlich aus den Dokumenten dieses einen Kunden. Eine Vermischung von Trainingsdaten oder Modellen verschiedener Kunden ist im Ablauf nicht vorgesehen und durch auftragsgebundene Speicherpfade und auftragsgebundene Verschlüsselungskontexte technisch unterbunden.
- Für jeden Trainingsauftrag wird eine eigene, dedizierte GPU-Instanz erzeugt und nach Abschluss in jedem Ausgang (Erfolg, Fehler, Abbruch) zerstört; unverschlüsselte Zwischenstände auf der Instanz werden gelöscht.
- Die Website-Datenbank (Konten, Bestellungen, Zahlungsstatus) ist von der Verarbeitungs-Datenbank vollständig getrennt; Kundendokumente erreichen die Website-Ebene zu keinem Zeitpunkt (Upload erfolgt direkt in den Objektspeicher, siehe 2.1).

1.5 Pseudonymisierung und Datenminimierung

- Vor der Erzeugung von Trainingsdatensätzen durchläuft der extrahierte Text eine eigene PII-Filterstufe der Pipeline.
- Über die Integrationsschnittstelle sind ausschließlich minimierte Bestell-, Kunden- und Zustandsdaten abrufbar; hochgeladene Kundendokumente sind dort nicht erreichbar.
- Es werden keine Zahlungsmitteldaten (z. B. Kartennummern) gespeichert; Rechnungsstellung und Zahlungsabgleich laufen über die BuchhaltungsButler GmbH.

2.1 Weitergabekontrolle (Transport)

- Sämtliche externen Verbindungen sind transportverschlüsselt (TLS/HTTPS); in Produktion erzwingt die Anwendung HTTPS für öffentliche Basis- und Callback-URLs fail-closed.
- Der Dokumenten-Upload erfolgt über kurzlebige, vorsignierte Formulare (Gültigkeit 1 Stunde) direkt in den EU-Objektspeicher, ohne Transit über Anwendungsserver.
- Status-Rückmeldungen zwischen Verarbeitung und Website sind je Nachricht HMAC-SHA-256-signiert; Nachrichten mit ungültiger Signatur werden ohne Seiteneffekt verworfen. Callback-Ziele werden gegen eine Allowlist geprüft (Schutz vor SSRF), in Produktion ausschließlich HTTPS auf öffentliche Ziele.

2.2 Speicherverschlüsselung

- Artefakte im Objektspeicher (Korpus, Datensätze, Modellstände, Auslieferungspakete) werden anwendungsseitig mit AES-256-GCM verschlüsselt, im Envelope-Verfahren: je Artefakt ein eigener Datenschlüssel, der seinerseits mit dem Master-Key verschlüsselt abgelegt wird; das Format ist versioniert und an den Auftragskontext gebunden (kein Austausch zwischen Aufträgen).
- Der Master-Key wird getrennt von den verschlüsselten Artefakten verwahrt und unterliegt demselben Produktions-Härtetest wie alle Geheimnisse.

2.3 Eingabekontrolle

- Statusübergänge der Aufträge werden mit Zeitstempeln versioniert erfasst (monotone Ereignisfolge, Schutz gegen veraltete oder mehrdeutige Fakten).
- Zugriffe über die Integrationsschnittstelle werden mit Akteur, Aktion, Ressource und Ergebnis im ausschließlich anfügenden Auditprotokoll erfasst.
- Uploads werden vor der Annahme serverseitig validiert; abgewiesen wird, was den vereinbarten Rahmen sprengt.

3 Verfügbarkeit und Belastbarkeit

- Die Verarbeitung ist als kurzlebiger, wiederanlauffähiger Workflow orchestriert (Temporal); abgebrochene Läufe können deterministisch fortgesetzt oder kontrolliert als fehlgeschlagen abgeschlossen werden.
- Produktionscontainer laufen ohne Root-Rechte mit schreibgeschütztem Dateisystem, mit Healthchecks, Neustart-Richtlinien und Ressourcenlimits; Container-Images sind über Digests unveränderlich festgeschrieben und werden vor dem Ausrollen skriptgeprüft.
- Ein Abgleichsjob (Reconciliation) erkennt hängende Aufträge und verwaiste Ressourcen und führt sie nach.
- Datensicherung: Die beiden Datenbanken (Trainings-Pipeline und Website) werden per dokumentiertem pg_dump-Export gesichert; Artefakte im Objektspeicher liegen redundant bei Exoscale (Frankfurt am Main) vor. Der Master-Key wird getrennt von beiden Sicherungen aufbewahrt, sodass ein einzelner kompromittierter Bestandteil allein nicht zur Entschlüsselung ausreicht.
- Da Kundendaten nur für die Dauer der Fertigung vorgehalten werden (siehe 4.2), ist der Schaden eines Totalverlusts strukturell begrenzt: Der Kunde besitzt die Quelldokumente, IonKon kann die Fertigung wiederholen.

4.1 Entwicklungs- und Änderungsprozess

Diese TOM werden mindestens einmal jährlich sowie bei wesentlichen Änderungen der Verarbeitung durch die Geschäftsführung überprüft und bei Bedarf fortgeschrieben.

- Änderungen laufen über Versionskontrolle mit Continuous Integration: automatisierte Tests (Web und Backend), statische Analysen und ein Secret-Scanner (Gitleaks) vor jeder Zusammenführung.
- Sicherheitsrelevante Konfiguration ist fail-closed voreingestellt; Test- und Entwicklungsschalter sind in Produktion technisch wirkungslos (doppelte Guards gegen Fehlkonfiguration).
- Adversariale Sicherheitsprüfungen (Red-Team-Durchläufe) werden anlassbezogen durchgeführt und ihre Befunde nachweisbar behoben.

4.2 Löschkonzept

- Trainingsdaten und eigene Modellkopien werden nach Empfangsbestätigung der Lieferung gelöscht; bestätigt der Kunde trotz zweier Erinnerungen nicht, greift die vertragliche Zugangsfiktion und die Löschung erfolgt zu diesem Zeitpunkt. Sobald die Löschung erfolgt ist, wird automatisch ein Löschnachweis erteilt.
- Unabhängig davon gilt eine technische Aufbewahrungsobergrenze (Standard 30 Tage ab Bereitstellung, absolute Obergrenze 180 Tage ab Auftragsbeginn), nach deren Ablauf Artefakte automatisch bereinigt werden.
- Kontaktanfragen werden spätestens nach 365 Tagen automatisch gelöscht; die Löschung eines Kundenkontos entfernt kaskadierend alle zugehörigen personenbezogenen Datensätze der Website-Ebene.

4.3 Auftragskontrolle (Subauftragsverarbeiter)

- Vollständiges Verzeichnis der Subauftragsverarbeiter, jeweils mit Auftragsverarbeitungsvertrag: STRATO GmbH (Deutschland), Betrieb des Webservers und der Datenbank; DataCrunch Oy, Cloud-Marke „Verda“ (Finnland), GPU-Rechenleistung für Training und Datensynthese; Akenes SA, Marke „Exoscale“ (Schweiz), Objektspeicher in Frankfurt am Main sowie GPU-Rechenleistung für Training und Datensynthese in Frankfurt, Zagreb oder Zürich je nach verfügbarer Kapazität; Hetzner Online GmbH (Deutschland), nur bei gebuchtem Hosting der Server des Kunden in Deutschland oder Finnland; BuchhaltungsButler GmbH (Deutschland), Rechnungsstellung und Zahlungsabgleich. Verarbeitung von Kundendokumenten findet ausschließlich in der EU oder der Schweiz statt. Ein externer KI-Anbieter wird nicht eingesetzt; die inhaltliche Verarbeitung läuft ausschließlich auf der für den Auftrag bereitgestellten Instanz.
- Weisungsrechte, Kontrollrechte und Meldewege bei Datenschutzvorfällen regelt der AVV (Nummer 9): IonKon meldet eine Verletzung des Schutzes personenbezogener Daten dem Kunden unverzüglich, spätestens 48 Stunden nach Kenntniserlangung, über die Kontaktadresse info@ionkon.de.