AUFTRAGSVERARBEITUNGSVERTRAG

gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)

Stand: 09.06.2026

Präambel

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten im Auftrag zwischen den Vertragsparteien. Sie konkretisiert die Verpflichtungen aus der Auftragsverarbeitung gemäß Art. 28 DS-GVO und gilt für alle Tätigkeiten, bei denen der Auftragsverarbeiter personenbezogene Daten des Auftraggebers verarbeitet.

§ 1 Vertragsparteien und Definitionen

Auftraggeber (Verantwortlicher):

- [Name, Adresse des Kunden]
- nachfolgend „**Auftraggeber**" genannt

Auftragsverarbeiter:

- Tovias Network GmbH
- Fundermannsweg 51a, 46242 Bottrop
- vertreten durch Herrn Oliver Hesse
- nachfolgend „**Auftragsverarbeiter**" genannt

Gegenstand der Verarbeitung: Die Verarbeitung personenbezogener Daten erfolgt gemäß Anlage 1 (Auftragsumfang und Daten).

§ 2 Umfang der Auftragsverarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich nach den Weisungen des Auftraggebers. Gegenstand, Dauer, Art, Zweck und Kategorien der verarbeiteten Daten sowie Kategorien betroffener Personen sind in Anlage 1 dokumentiert.

(2) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des zugrunde liegenden Leistungsvertrags, sofern sich aus dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 3 Verantwortlichkeiten

(1) Der Auftraggeber ist allein verantwortlich für die Rechtmäßigkeit der Datenverarbeitung, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter und die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze.

(2) Der Auftragsverarbeiter bestätigt, dass ihm und seinen Mitarbeitern die Vorschriften der DS-GVO und sonstigen Datenschutzvorschriften bekannt sind und beachtet werden.

(3) Der Auftraggeber benennt einen Ansprechpartner für Datenschutzfragen.

§ 4 Weisungsrecht des Auftraggebers

(1) Die Weisungen werden anfänglich durch den Leistungsvertrag und diese Vereinbarung festgelegt. Der Auftraggeber kann diese danach in schriftlicher Form oder per E-Mail (Textform) durch Einzelweisungen ändern, ergänzen oder ersetzen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(2) Der Auftragsverarbeiter darf Daten nur im Rahmen des Auftrags und der Weisungen des Auftraggebers verarbeiten. Sollte eine Weisung gegen anwendbare Gesetze verstoßen, informiert der Auftragsverarbeiter den Auftraggeber unverzüglich und kann die Umsetzung aussetzen, bis sie bestätigt oder abgeändert wurde.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat die in Anlage 2 dokumentierten technischen und organisatorischen Maßnahmen (TOM) vor Beginn der Verarbeitung umzusetzen. Bei Akzeptanz durch den Auftraggeber werden diese Maßnahmen Grundlage des Auftrags.

(2) Der Auftragsverarbeiter gewährleistet ein dem Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, berücksichtigt dabei den Stand der Technik, Implementierungskosten und die Art, den Umfang und die Zwecke der Verarbeitung.

(3) Der Auftragsverarbeiter ist berechtigt, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

(4) Der Auftragsverarbeiter setzt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der TOM ein.

§ 6 Datenschutzbeauftragter und Ansprechpartner

Der Datenschutzbeauftragte des Auftragsverarbeiters ist:

Björn Leineweber
Datenschutz Ruhr GmbH

Hauptstr. 2, 45219 Essen
Tel.: 0201 246 888 00
E-Mail: leineweber@datenschutz-ruhr.de

Ein Wechsel wird dem Auftraggeber unverzüglich mitgeteilt.

§ 7 Pflichten des Auftragsverarbeiters

(1) **Dokumentation und Verzeichnis:** Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO und stellt diesem auf Anforderung zur Verfügung.

(2) **Unterstützung bei Datenschutzfolgenabschätzung:** Der Auftragsverarbeiter unterstützt den Auftraggeber mit allen verfügbaren Informationen, einschließlich vorheriger Konsultation der Aufsichtsbehörde.

(3) **Fernmeldegeheimnis:** Der Auftragsverarbeiter gewährleistet die Einhaltung des Fernmeldegeheimnisses gemäß § 88 TKG und verpflichtet alle zuständigen Personen entsprechend.

(4) **Geheimhaltung:** Der Auftragsverarbeiter gewährleistet, dass mit der Verarbeitung befasste Mitarbeiter die Daten außerhalb der Weisung nicht verarbeiten und sich zur Vertraulichkeit verpflichtet haben. Diese Pflicht besteht auch nach Beendigung des Auftrags fort.

(5) **Mitteilungspflicht bei Datenpannen:** Der Auftragsverarbeiter unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten bekannt werden.

(6) **Unterstützung bei Haftungsansprüchen:** Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person unterstützt der Auftragsverarbeiter bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten.

(7) **Vertraulichkeit von Betriebsgeheimnissen:** Der Auftragsverarbeiter behandelt alle im Rahmen des Vertragsverhältnisses erlangten Betriebsgeheimnisse und Datensicherheitsmaßnahmen vertraulich.

(8) **Kopien und Duplikate:** Ohne vorherige Zustimmung darf der Auftragsverarbeiter keine Kopien oder Duplikate anfertigen, ausgenommen solche, die zur ordnungsgemäßen Datenverarbeitung, Leistungserbringung (einschließlich Datensicherung) oder Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(9) **Unterstützung bei behördlichen Kontrollen:** Der Auftragsverarbeiter unterstützt nach besten Kräften bei Kontrollen von Aufsichtsbehörden, Verfahren oder Haftungsansprüchen.

§ 8 Leistungsort und Datentransfer

(1) Der Auftragsverarbeiter erbringt Leistungen in der Europäischen Union (EU), im Europäischen Wirtschaftsraum (EWR) oder in sicheren Drittländern. Dies gilt auch für Unterauftragnehmer.

(2) Bei Datentransfers in sichere Drittländer garantiert der Auftragsverarbeiter die Einhaltung der DS-GVO-Vorgaben und weist dies auf Verlangen nach.

(3) Der Auftraggeber wird bei Verlagerungen des Leistungsortes innerhalb der EU/EWR informiert. Eine Zustimmungsverweigerung gilt nach vier Wochen als erteilt, sofern keine Einwände vorliegen.

§ 9 Datenschutzrechte betroffener Personen

(1) Wenn sich eine betroffene Person an den Auftragsverarbeiter wendet, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter.

(2) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung von Ansprüchen auf Auskunft, Berichtigung, Sperrung, Übertragbarkeit oder Löschung und teilt dem Auftraggeber unverzüglich, längstens innerhalb von fünf Werktagen, erforderliche Informationen mit.

(3) Der Auftragsverarbeiter berichtigt, löscht, sperrt oder überträgt Daten auf Weisung unverzüglich, spätestens innerhalb von fünf Werktagen, und bestätigt dies schriftlich.

§ 10 Auskunft an Dritte

Muss der Auftragsverarbeiter aufgrund gesetzlicher Bestimmungen Dritten Auskunft über Auftraggeber-Daten erteilen, informiert er den Auftraggeber rechtzeitig vor der Auskunftserteilung schriftlich über Empfänger, Zeitpunkt, Inhalt und Rechtsgrundlage.

§ 11 Rückgabe und Löschung von Daten

(1) Nach Beendigung der Leistungserbringung löscht der Auftragsverarbeiter sämtliche Auftraggeber-Daten oder gibt von dem Auftraggeber erhaltene Datenträger zurück. Mit Zustimmung erfolgt datenschutzgerechte Vernichtung. Gleiches gilt für Test- und Ausschussmaterial.

(2) Über Löschung oder Vernichtung erstellt der Auftragsverarbeiter ein Protokoll, das auf Anforderung vorgelegt wird.

(3) Dokumentationen zur Nachweispflicht auftragsgemäßer Datenverarbeitung werden entsprechend der Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt.

§ 12 Unterstützung bei Datensicherheit und Meldepflichten

(1) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der Pflichten zu Datensicherheit, Meldepflichten bei Datenpannen und Datenschutzfolgeabschätzungen gemäß Art. 32-36 DS-GVO.

(2) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich über Datenpannen gemäß Art. 33 Abs. 2 DS-GVO.

(3) Der Auftragsverarbeiter ergreift im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten und Minderung nachteiliger Folgen.

§ 13 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch benannte Prüfer durchführen zu lassen. Stichprobenkontrollen sind in der Regel rechtzeitig anzumelden.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung aller Pflichten überzeugen kann und erteilt auf Anforderung erforderliche Auskünfte sowie Nachweise der TOM-Umsetzung.

(3) Der Auftragsverarbeiter gewährt Zugangs-, Auskunfts- und Einsichtsrechte.

(4) Der Nachweis der TOM-Umsetzung kann alternativ zur Vor-Ort-Kontrolle durch anerkannte Zertifizierungen, Audit-Berichte, IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz) oder genehmigte Zertifizierungen gemäß Art. 42 DS-GVO erbracht werden.

§ 14 Unterauftragnehmer (Subunternehmer)

(1) Der Auftraggeber stimmt der Begründung von Unterauftragsverhältnissen gemäß Anlage 3 zu. Jeder Wechsel oder Austausch eines Unterauftragnehmers bedarf der Zustimmung durch den Auftraggeber; Anlage 3 ist dann zu aktualisieren.

(2) Vor Hinzuziehung oder Ersetzung von Subunternehmern holt der Auftragsverarbeiter die Zustimmung des Auftraggebers ein, die nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

(3) Bei Unterbeauftragung überträgt der Auftragsverarbeiter seine datenschutzrechtlichen Pflichten dem Subunternehmer und räumt dem Auftraggeber Kontroll- und Überprüfungsrechte ein.

(4) Keiner Zustimmung bedarf die Einschaltung von Subunternehmern für Nebenleistungen wie Post-, Kurier-, Telekommunikations-, Geldtransport-, Bewachungs- und Reinigungsdienste. Mit diesen trifft der Auftragsverarbeiter branchenübliche Geheimhaltungsvereinbarungen.

(5) Bei Leistungserbringung außerhalb der EU/EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit sicher.

§ 15 Haftung und Schadensersatz

(1) Auftraggeber und Auftragsverarbeiter haften im Außenverhältnis gegenüber betroffenen Personen gemeinsam für Schäden durch nicht DS-GVO-konforme Verarbeitung.

(2) Der Auftragsverarbeiter haftet ausschließlich für Schäden, die auf einer Verarbeitung beruhen, bei der er den speziell für Auftragsverarbeiter geltenden Pflichten nicht nachgekommen ist, unter Nichtbeachtung oder gegen rechtmäßige Weisungen des Auftraggebers gehandelt hat.

(3) Im Innenverhältnis haftet der Auftragsverarbeiter nur unter den Bedingungen des Abs. 2.

(4) Weitergehende Haftungsansprüche nach allgemeinen Gesetzen bleiben unberührt.

§ 16 Informationspflichten und Formales

(1) Gefährden Pfändung, Beschlagnahme, Insolvenz oder Maßnahmen Dritter die Daten des Auftraggebers, informiert der Auftragsverarbeiter unverzüglich und teilt Verantwortlichen mit, dass Hoheit und Eigentum bei dem Auftraggeber liegen.

(2) Änderungen dieser Vereinbarung bedürfen einer schriftlichen Vereinbarung (auch in Textform) mit ausdrücklichem Hinweis auf die Änderung. Dies gilt auch für den Verzicht auf das Formerfordernis.

(3) Bei Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen des Hauptvertrags vor. Sollten einzelne Teile unwirksam sein, berührt dies die übrige Gültigkeit nicht.

(4) Es gilt deutsches Recht.

§ 17 Geltung

Dieser AV-Vertrag gilt für alle Kunden von Tovias Network. Tovias Network unterwirft sich der Bindung an diesen Vertrag im Rahmen der laufenden Geschäftsbeziehung.

ANLAGE 1: AUFTRAGSUMFANG UND VERARBEITETE DATEN

I. Leistungsumfang und Datenverarbeitung

Der Auftragsverarbeiter erbringt folgende Dienstleistungen für den Auftraggeber:

Dienstleistung	Tätigkeit	Verarbeitete Datenkategorien	Zweck	Betroffene Personenkreise
Administration und Hosting	Cloud-Administration, Server-Verwaltung, Datenbank-Administration	Identifikationsdaten (Name, E-Mail), Kontaktdaten, Log-Daten, IP-Adressen, Systemdaten	Administration, Wartung, Support, Sicherung	Mitarbeiter, Kunden, Endkunden
Backup & Recovery	Sicherung und Wiederherstellung von Kundendaten	Sämtliche vom Kunden gespeicherten Daten, Unternehmens- und Geschäftsdaten	Datensicherung, Notfallwiederherstellung	Kunden, Endkunden, Mitarbeiter
Cloud-Infrastruktur	Betrieb von Cloud-Servern und Speicherlösungen	Alle vom Kunden hochgeladenen oder in Systemen erzeugten Daten	Speicherung, Verarbeitung, Bereitstellung	Kunden, Endkunden
E-Mail-Dienste	Verwaltung von E-Mail-Accounts, Verschlüsselung, Filterung	E-Mail-Adressen, E-Mail-Inhalte, Anhänge, Metadaten	Kommunikation, Spam-Filterung, Archivierung	Kunden, externe Kommunikationspartner
Fernwartung	Remote-Zugriff für technischen Support	Computersystem-Daten, Bildschirm-Inhalte, Eingabedaten	Support, Troubleshooting, Wartung	Mitarbeiter, Kunden
VoIP & Telefonanlage	Verwaltung und Betrieb von Cloud-Telefonanlagen	Telefon-Metadaten, Gesprächsprotokolle, Benutzer-Identifikation	Telefonie, Kommunikation, Protokollierung	Mitarbeiter, Kunden, externe Anrufer
Domain-Verwaltung	Registrierung, Verwaltung und Hosting von Domains und Websites	Website-Besucherdaten (IP, User-Agent), Registrant-	Domain-Registrierung, Website-Betrieb	Website-Besucher, Registrants

Dienstleistung	Tätigkeit	Verarbeitete Datenkategorien	Zweck	Betroffene Personenkreise
		Daten, Domain-Kontaktdaten		
KI-Telefonassistent	Betrieb von automatisierten Telefonanruf-Systemen	Anrufer-Identifikation, Gesprächsinhalte, Transkriptionen	Automatisierte Anrufbearbeitung, Kundenkommunikation	Anrufer, Kunden
Zahlungsabwicklung	Integration von Zahlungsgateway-Systemen	Zahlungsdaten, Zahlungs-Identifikationen, Transaktionsdaten	Zahlungsverarbeitung	Kunden, Geschäftspartner
ERP & CRM-Verwaltung	Betrieb und Administration von ERP- und CRM-Systemen	Kundendaten, Geschäftsdaten, Kontaktinformationen, Transaktionsdaten	Geschäftsverwaltung, Kundenverwaltung, Auftragsverwaltung	Kunden, Endkunden, Mitarbeiter
Kommunikationstools	Administration von Messaging- und Kommunikationsplattformen	Benutzer-IDs, Nachrichteninhalte, Metadaten, Kontaktlisten	Unternehmenskommunikation	Mitarbeiter, externe Kontakte
Sicherheitstools & Monitoring	Einsatz von Firewalls, Intrusion-Detection, Malware-Scanning	Netzwerk-Daten, Log-Daten, Verdachtsindikatoren	Sicherheitsüberwachung, Bedrohungserkennung	Alle Benutzer

II. Kategorien personenbezogener Daten

Der Auftragsverarbeiter verarbeitet folgende Datenkategorien:

- **Identifikationsdaten:** Name, Vorname, Titel, Kundennummer
- **Kontaktdaten:** E-Mail-Adresse, Telefonnummer, Postadresse
- **Authentifizierungsdaten:** Benutzernamen, Passwort-Hashes, Authentifizierungs-Token
- **Nutzungsdaten:** Login-Zeiten, Zugriffszeiten, Geräte-Informationen
- **Technische Daten:** IP-Adressen, MAC-Adressen, Browser-Daten, System-Identifikatoren
- **Transaktionsdaten:** Zahlungsinformationen, Bestellhistorie, Vertragsdaten

- **Geschäftsdaten:** Unternehmensstruktur, Organisationsdaten, Geschäftskommunikation
- **Kommunikationsdaten:** E-Mail-Inhalte, Anrufprotokolle, Nachrichteninhalte
- **Systemdaten:** Log-Dateien, Fehlerberichte, Monitoring-Daten
- **Optionale: Besondere Kategorien** (sofern vom Auftraggeber hochgeladen): Gesundheitsdaten, Standortdaten

III. Betroffene Personenkreise

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers
- Endkunden/Geschäftspartner des Auftraggebers
- Website-Besucher
- Externe Kommunikationspartner

IV. Verarbeitungszwecke

- Administration und Wartung von IT-Systemen
- Bereitstellung vereinbarter Cloud- und SaaS-Dienste
- Sicherung und Wiederherstellung von Daten
- Technischer Support und Troubleshooting
- Sicherheitsüberwachung und Compliance
- Geschäftsabwicklung und Vertragserfüllung
- Kommunikation und Zusammenarbeit
- Einhaltung gesetzlicher Aufbewahrungspflichten

V. Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des Leistungsvertrags. Nach Beendigung werden Daten gemäß § 11 dieses AV-Vertrags gelöscht oder zurückgegeben.

ANLAGE 2: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

A. VERTRAULICHKEIT (Art. 32 Abs. 1 lit. b DS-GVO)

1. Zutrittskontrolle

Ziel: Verhinderung unbefugten physischen Zutritts zu Räumen mit Datenverarbeitungsanlagen

Umgesetzte Maßnahmen:

- ☑ Automatisches Zugangskontrollsystem / Schließsystem mit Codesperre
- ☑ Biometrische Zugangssperren (wo vorhanden)
- ☑ Videoüberwachung der Zugänge (nicht in Zweigstellen)
- ☑ Alarmanlage mit automatischer Benachrichtigung
- ☑ Chipkarten-/Transponder-Schließsystem
- ☑ Sicherheitsschlösser
- ☑ Manuelles Schließsystem mit sorgfältiger Schlüsselverwaltung
- ☑ Sicherheitsbereich definiert und dokumentiert
- ☑ Datenträger unter Verschluss (Serverräume, Archive)
- ☑ Personenkontrolle beim Empfang
- ☑ Vom Publikumsverkehr getrennter Bereich
- ☑ Sorgfältige Auswahl und Überwachung von Reinigungspersonal
- ☑ Kameraüberwachung nur im Falle von Alarm bzw. bei Ankunft (LIVE)

2. Zugangskontrolle

Ziel: Verhinderung unbefugter Nutzung von Datenverarbeitungsanlagen und -verfahren

Umgesetzte Maßnahmen:

- ☑ Berechtigungsvergabeverfahren mit dokumentierter Genehmigung
- ☑ Authentifikation mit Benutzername / Passwort
- ☑ Authentifikation mit biometrischen Verfahren (wo verfügbar)
- ☑ Zwei-Faktor-Authentifizierung für kritische Systeme

Passwort-Richtlinien:

- ☑ Zeichen-Mix (Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen)
- ☑ Mindestens 8 Zeichen

- ☑ Regelmäßiger Passwortwechsel (mindestens alle 6 Monate)
- ☑ Passworthistorie (Wiederverwendung ausgeschlossen)
- ☑ Keine Gruppenpasswörter
- ☑ Sichere Aufbewahrung von Admin-Passwörtern
- ☑ Automatische Begrenzung Anmeldeversuche (max. 3 Versuche)
- ☑ Passwortrücksetzungsverfahren gemäß Anweisung

Weitere Zugriffskontrollen:

- ☑ Benutzerprofile mit rollenbasierten Rechten
- ☑ Protokollierung des Systemzugangs und der Zugriffsrechte
- ☑ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☑ Festlegung von Aufbewahrungsorten für Datenträger
- ☑ Einsatz von VPN-Technologie für Remote-Zugriffe
- ☑ Verschlüsselung von Datenträgern
- ☑ Verbot externer Schnittstellen (USB) oder Whitelist-Konzept
- ☑ Vertragliche und technische Regelung von Drittsystemen
- ☑ Verschlüsselung auf Website (HTTPS/TLS)
- ☑ Einhaltung Need-to-Know-Prinzip

3. Zugriffskontrolle

Ziel: Sicherstellung, dass nur berechtigte Personen auf ihre Zugriffsberechtigung unterliegende Daten zugreifen

Umgesetzte Maßnahmen:

- ☑ IT-Berechtigungskonzept dokumentiert und aktualisiert
- ☑ Anzahl Administratoren auf das Notwendigste reduziert
- ☑ Protokollierung von Zugriffen auf Anwendungen (Eingabe, Änderung, Löschung)
- ☑ Auswertung von Logs (regelmäßig und im Verdachtsfall)
- ☑ Zwei-Faktor-Authentifizierung für administrative Zugriffe
- ☑ Einsatz von Intrusion-Detection-Systemen (IDS)
- ☑ Plausibilitätskontrolle bei Dateneingabe und -änderung
- ☑ Anforderungen zur Passwortrücksetzung dokumentiert
- ☑ Vergabe und Verwaltung von Zugriffscodes geregelt

4. Trennungskontrolle

Ziel: Sicherstellung Separation von Kundendaten und Verarbeitungsvorgängen

Umgesetzte Maßnahmen:

- ☑ Verwaltung der Rechte durch Systemadministrator mit differenzierten Berechtigungen (Lesen, Ändern, Löschen)
- ☑ Sichere Aufbewahrung von Datenträgern
- ☑ Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- ☑ Protokollierung der Vernichtung
- ☑ Festlegung und Einhaltung von Löschfristen
- ☑ Verschlüsselung von Smartphones, Laptops, mobilen Geräten
- ☑ Verschlüsselung von Back-Up-Daten
- ☑ Trennung von Berechtigungsbewilligung und Berechtigungsvergabe
- ☑ Getrennte Verarbeitung von Daten unterschiedlicher Zwecke
- ☑ Physikalisch getrennte Speicherung auf gesonderten Systemen ODER logische Mandanten-/Kundentrennung (softwareseitig)

Daten-Segregation:

- ☑ Berechtigungskonzept für Trennung der Kundendaten im System
- ☑ Festlegung spezieller Rechte pro Benutzer (Lesen, Schreiben, Ändern)
- ☑ Zweckbindung des Zugriffs
- ☑ Festlegung von Datenbankrechten
- ☑ Getrennte Aufbewahrung von Datenträgern verschiedener Kunden
- ☑ Trennung von Kundendaten basierend auf Berechtigungskonzept
- ☑ Funktionstrennung (z.B. Buchhaltung und Kundendaten)
- ☑ Trennung von Produktiv- und Testsystemen
- ☑ Bei Pseudonymisierung: Trennung der Zuordnungsdatei auf gesondertem, abgesicherten IT-System
- ☑ Verarbeitung verschiedener Kundendaten durch verschiedene Mitarbeiter oder nach Need-to-Know-Prinzip

B. PSEUDONYMISIERUNG (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Ziel: Verarbeitung von Daten derart, dass diese ohne zusätzliche Informationen nicht mehr einer Person zugeordnet werden können

Umgesetzte Maßnahmen:

- ☑ Pseudonymisierung von Geschäfts-/Kundendaten (wo applicable)
- ☑ Pseudonymisierung von IP-Adressen bei Weitergabe zu Analyse/Marketing/Tracking
- ☑ Trennung der Zuordnungsdatei von den pseudonymisierten Daten
- ☑ Aufbewahrung auf gesondertem, abgesicherten IT-System
- ☑ Pseudonymisierung von Userdaten/Privatkunden (wo applicable)
- ☑ Pseudonymisierung von Mitarbeiterdaten (wo applicable)

C. INTEGRITÄT (Art. 32 Abs. 1 lit. b DS-GVO)

1. Weitergabekontrolle

Ziel: Sicherung gegen unbefugtes Lesen, Kopieren, Ändern oder Entfernen bei Übermittlung und Transport

Maßnahmen elektronischer Übertragung:

- ☑ VPN-Tunnel für Remote-Zugriffe
- ☑ Berechtigungskonzept mit Identifizierung / Authentifizierung
- ☑ Logging aller Zugriffe
- ☑ Sperrmechanismen bei Verstößen
- ☑ Verschlüsselung von Datenübermittlungen (TLS, HTTPS)
- ☑ E-Mail-Verschlüsselung (Hornetsecurity oder äquivalent)
- ☑ Nutzung elektronischer Signatur für kritische Transaktionen
- ☑ Dokumentation von Übermittlungsvorgängen und Empfängern

Maßnahmen physischer Transport:

- ☑ Sichere Transportbehälter
- ☑ Verschlüsselte Datenträger
- ☑ Sorgfältige Auswahl und Überprüfung von Transportpersonal
- ☑ Empfangsbestätigung
- ☑ Rückgabedokumentation
- ☑ Übersicht der Empfänger und Leihfristen

2. Eingabekontrolle

Ziel: Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten

Umgesetzte Maßnahmen:

- ☑ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☑ Protokollierung von Administratortätigkeiten
- ☑ Nachvollziehbarkeit durch individuelle Benutzernamen (keine Benutzergruppen)
- ☑ Vergabe von Rechten basierend auf Berechtigungskonzept
- ☑ Einsatz von Intrusion-Detection-Systemen
- ☑ Übersicht über Applikationen und verarbeitete Daten
- ☑ Plausibilitätskontrolle bei Dateneingabe und -änderung
- ☑ Aufbewahrung von Formularen, aus denen Daten übernommen werden

D. VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs. 1 lit. b und c DS-GVO)

1. Verfügbarkeitskontrolle

Ziel: Schutz gegen zufällige Zerstörung/Verlust und rasche Wiederherstellbarkeit

Stromversorgung und Klimatechnik:

- ☑ Unterbrechungsfreie Stromversorgung (USV)
- ☑ Schutzsteckdosenleisten in Serverräumen
- ☑ Klimaanlage in Serverräumen
- ☑ Geräte zur Überwachung von Temperatur und Feuchtigkeit

Brandschutz und Sicherheit:

- ☑ Feuer- und Rauchmeldeanlagen
- ☑ Feuerlöschgeräte in Serverräumen
- ☑ Alarmmeldung bei unbefugten Zutritte zu Serverräumen/Büros
- ☑ Serverräume nicht unter sanitären Anlagen
- ☑ In Hochwassergebieten: Serverräume über Wassergrenze

Backup und Recovery:

- ☑ Backup- & Recoverykonzept mit täglicher Sicherung
- ☑ Aufbewahrung an katastrophensicherer, ausgelagerter Lokalität
- ☑ Festplattenspiegelung
- ☑ Trennung von Sicherung (Daten, Programme, Systeme)
- ☑ Regelmäßiges Testen von Datenwiederherstellung

- ☑ Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung
- ☑ Dokumentierter Notfallplan

Netzwerk- und Systemsicherheit:

- ☑ Einsatz von Sicherheitssoftware:VirenscannerFirewalls (Hardware und Software)SPAM-FilterVerschlüsselungsprogrammeIntrusion-Detection-Systeme
- ☑ Abweisung unberechtigter User
- ☑ Sichere Aufbewahrung von Keys / Codes
- ☑ Cloud-Speicher in Europa (DSGVO-konform)

E. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 32 Abs. 1 lit. d DS-GVO)

1. Datenschutzmanagement

- ☑ Technische und organisatorische Maßnahmen durch Datenschutzbeauftragten überprüft
- ☑ Selbstverpflichtung zur regelmäßigen Überprüfung des Schutzniveaus
- ☑ Selbstverpflichtung zur regelmäßigen Löschung von Daten außerhalb der Aufbewahrungsfrist
- ☑ Datenschutzfreundliche Voreinstellung (Daten-Minimierung)
- ☑ Selbstverpflichtung zur Überprüfung neuer Verfahren
- ☑ Dokumentation: Unverzügliche Kontaktaufnahme zum Datenschutzbeauftragten und Aufsichtsbehörde bei Datenpannen (Maximalfrist: 72 Stunden)

2. Auftragskontrolle

- ☑ Auswahl von Unterauftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere Datensicherheit)
- ☑ Schriftliche Weisungen durch Auftragsdatenverarbeitungsvertrag
- ☑ Überprüfung: Unterauftragnehmer hat Datenschutzbeauftragten bestellt
- ☑ Wirksame Kontrollrechte gegenüber Unterauftragnehmer vereinbart
- ☑ Vertragsstrafen bei Verstößen
- ☑ Vorherige Prüfung und Dokumentation der Sicherheitsmaßnahmen
- ☑ Verpflichtung der Mitarbeiter auf Datengeheimnis
- ☑ Sicherstellung der Vernichtung von Daten nach Auftragsbeendigung

- ☑ Laufende Überprüfung der Unterauftragnehmer und ihrer Tätigkeiten

F. DATENVERARBEITUNG AUSSERHALB DER EU/EWR

- ☑ Datenspeicherung grundsätzlich in der EU
- ☑ Bei Datenübertragung in sichere Drittländer: Nachweis äquivalenter Schutzvorkehrungen (z.B. Standarddatenschutzklauseln)
- ☑ Einsatz von Analyse-Tools und Tracking-Tools mit Hinweis an Nutzer und vertraglicher Sicherung von Datenschutz
- ☑ Transparenzmitteilungen an Nutzer/Betroffene

G. INCIDENT RESPONSE UND DATENSCHUTZVERLETZUNGEN

- ☑ Dokumentierter Prozess zur Meldung von Datenpannen
- ☑ Unverzügliche Benachrichtigung des Auftraggebers
- ☑ Unterstützung bei Meldung an Behörden (Frist: 72 Stunden)
- ☑ Dokumentation und Analyse von Vorfällen
- ☑ Maßnahmen zur Schadensminderung

Status der Maßnahmen: Vollständig implementiert und dokumentiert
Letzter Review: [Datum einfügen]
Nächster Review: [Datum einfügen]

Verantwortlich: Björn Leineweber (Datenschutzbeauftragter)
Kontakt: leineweber@datenschutz-ruhr.de

ANLAGE 3: UNTERAUFTRAGNEHMER

Übersicht beauftragte Unterauftragnehmer

Der Auftraggeber stimmt der Nutzung folgender Unterauftragnehmer (Auftragsverarbeiter) zu:

Unterauftragnehmer	Sitz	Tätigkeiten	Datenkategorien	Zweck	Betroffene Personen
3CX DMCC	Dubai, VAE	Bereitstellung VoIP-Telefonanlage	Anrufer-IDs, Gesprächsprotokolle, Nutzer-Daten	Telefonie, Cloud-Telefonanlage	Mitarbeiter, Kunden, externe Anrufer
Acronis Germany GmbH	München, DE	Cloud-Backup-Lösung	Sämtliche vom Kunden gespeicherte Daten, Geschäftsdaten, Kundendaten, Bankdaten	Datensicherung, Notfallwiederherstellung	Kunden, Endkunden, Mitarbeiter
ADN Advanced Digital Network Distribution GmbH	Bochum, DE	Vertrieb und Vermittlung von Cloud-Lösungen	Kundendaten zur Vertragsabwicklung	Vertrieb und Vermittlung	Kunden
AnyDesk Software GmbH	Stuttgart, DE	Remote-Desktop-Software für technischen Support	Computersystem-Daten, Bildschirminhalte, Eingabedaten	Fernwartung, technischer Support	Mitarbeiter, Kunden
fonio GmbH	Wien, AT	KI-Telefonassistent und automatisierte Anrufbearbeitung	Anrufer-Identifikation, Gesprächsinhalte, Transkriptionen	Automatisierte Anrufbearbeitung	Anrufer, Kunden
Hetzner Online GmbH	Gunzenhausen, DE	Hosting und Server-Infrastruktur	Alle vom Kunden in der Cloud gespeicherten Daten	Server-Betrieb, Hosting, Datenverarbeitung	Kunden, Endkunden, Mitarbeiter
Hornetsecurity GmbH	Hannover, DE	E-Mail-Verschlüsselung und Mailfilter	E-Mail-Adressen, E-Mail-Inhalte, Anhänge, Metadaten	E-Mail-Sicherheit, Spam-Filterung, Verschlüsselung	Kunden, externe Kommunikationspartner

Unterauftragnehmer	Sitz	Tätigkeiten	Datenkategorien	Zweck	Betroffene Personen
Host Europe GmbH	Köln, DE	Domain-Registrierung und Hosting	Registrant-Daten, Domain-Kontaktdaten, Website-Besucherdaten, Website-Inhalte	Domain-Registrierung, Website-Hosting	Registrants, Website-Besucher
Microsoft Corporation	Redmond, USA	Cloud-Office-Suite (Microsoft 365)	Sämtliche vom Kunden gespeicherte Daten, Geschäftsdaten, Kundendaten, Kontaktdaten	Cloud-Office, Zusammenarbeit, Datenspeicherung	Kunden, Endkunden, Mitarbeiter
OVH GmbH	Saarbrücken, DE	Rechenzentrum und Hosting-Infrastruktur	Alle vom Kunden gespeicherten Daten, Website-Inhalte, Backup-Daten	Datenspeicherung, Hosting, Backups	Kunden, Endkunden, Website-Besucher
Stripe, LLC	San Francisco, USA	Zahlungsgateway und Zahlungsabwicklung	Zahlungsdaten, Zahlungs-Identifikationen, Transaktionsdaten	Zahlungsverarbeitung, Rechnungswesen	Kunden, Zahlende
weclapp SE	Frankfurt am Main, DE	ERP- und CRM-System	Kundendaten, Geschäftsdaten, Kontaktinformationen, Transaktionsdaten	Geschäftsverwaltung, Kundenverwaltung, Bestellverwaltung	Kunden, Endkunden, Geschäftspartner
WhatsApp Ireland Ltd.	Dublin, IE	Messaging-Plattform	Benutzer-IDs, Nachrichteninhalte, Kontaktlisten, Metadaten	Geschäftskommunikation	Mitarbeiter, Kunden, externe Kontakte
Xiamen Yeastar Digital Technology Co., Ltd.	Xiamen, China	Telefonanlage und VoIP-Systeme	Anrufer-IDs, Gesprächsprotokolle, Nutzer-Daten, Log-Daten	Telefonie, Telefonanlagen-Verwaltung	Mitarbeiter, Kunden, externe Anrufer
ZEP GmbH	Ditzingen, DE	Facility-Management und Gebäudebewirtschaftung	Zugriffsdaten, Besucherlisten (falls applicable)	Gebäudeverwaltung, Zutrittskontrolle	Mitarbeiter, Besucher

Datenschutzrechtliche Anforderungen an Unterauftragnehmer

Für alle Unterauftragnehmer gelten folgende Anforderungen:

1. **Auftragsverarbeitungsvertrag:** Jeder Unterauftragnehmer ist vertraglich verpflichtet, personenbezogene Daten nach den Vorgaben der DS-GVO zu verarbeiten.

2. **Datenschutzbeauftragter:** Unterauftragnehmer, die umfangreiche Verarbeitungen vornehmen, müssen einen Datenschutzbeauftragten benannt haben oder einen Ansprechpartner für Datenschutzfragen bereitstellen.

3. **Technische und organisatorische Maßnahmen:** Alle Unterauftragnehmer müssen angemessene TOM gemäß Art. 32 DS-GVO implementieren und nachweisen.

4. **Datentransfer außerhalb EU/EWR:** Für Unterauftragnehmer mit Sitz außerhalb der EU/EWR werden zusätzliche Sicherheitsmaßnahmen und Schutzklauseln vereinbart (z.B. Standarddatenschutzklauseln).

5. **Kontrollrechte:** Der Auftraggeber behält sich das Recht vor, die Einhaltung der Datenschutzverpflichtungen bei allen Unterauftragnehmern zu überprüfen.

6. **Meldepflichten:** Unterauftragnehmer sind verpflichtet, Datenpannen und Datenschutzverstöße unverzüglich zu melden.

Hinweise zu Datentransfers

USA-basierte Dienste (Microsoft, Stripe): Diese Dienste unterliegen möglicherweise US-amerikanischem Recht und dem Zugriff durch US-Behörden. Für diese Dienste werden Standarddatenschutzklauseln und weitere geeignete Sicherungsvorkehrungen vereinbart.

China-basierte Dienste (Yeastar): Für Dienste mit Sitz in China werden zusätzliche Compliance-Maßnahmen und Verträge mit erweiterten Datenschutzgarantien abgeschlossen.

EU/EWR-basierte Dienste: Diese Dienste unterliegen direkt der DS-GVO und dem europäischen Datenschutzrecht.

Änderungen und Aktualisierungen

Diese Liste wird regelmäßig überprüft und aktualisiert. Änderungen bei:

- Hinzufügung neuer Unterauftragnehmer
- Austausch bestehender Unterauftragnehmer
- Änderung von Tätigkeiten oder Datenkategorien

werden dem Auftraggeber schriftlich mitgeteilt. Der Auftraggeber kann der Nutzung eines neuen Unterauftragnehmers innerhalb von zwei Wochen widersprechen, sofern datenschutzrechtliche Bedenken bestehen.

Stand: 09.06.2026