AV

AUFTRAGSVERARBEITUNG

Auftragsverarbeitung

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag

Auftrag gemäß Art. 28 DS-GVO · Version 4.1 vom 14.07.2026

VERSION	STAND	AUFTRAGNEHMER	GESCHÄFTSFÜHRER	SITZ
4.1	14.07.2026	faktoora GmbH	Dr. Peter Schenkel	Amselweg 1, 89231 Neu-Ulm

Inhaltsverzeichnis

Vertragsparteien

Auftrag gemäß Art. 28 DS-GVO (Version 4.1 vom 14.07.2026)

Vereinbarung

zwischen

AUFTRAGNEHMER

faktoora GmbH
Amselweg 1
89231 Neu-Ulm

– Auftragnehmer –

und

AUFTRAGGEBER

_____

_____

_____

– Auftraggeber –

Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Vertragsverhältnis gemachten Angaben. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber i.S.d. Art. 4 Nr. 2 DSGVO (Verarbeitung) und Art. 28 DSGVO auf Grundlage dieses Auftrags.

Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen sind in Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in Ziffer 1 beschriebenen Vertragsverhältnisse ergibt.

Die Verarbeitung erfolgt grundsätzlich in der EU/EWR. Soweit im Rahmen der Leistungserbringung Unterauftragnehmer mit Sitz außerhalb der EU/EWR eingesetzt werden oder ein Zugriff aus Drittländern technisch nicht vollständig ausgeschlossen werden kann, erfolgt dies ausschließlich unter Einhaltung der Anforderungen der Art. 44 ff. DSGVO und unter den in dieser Vereinbarung vorgesehenen geeigneten Garantien.

Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO

(Art.28 Abs.3 Satz 2 lit.c DS-GVO)

(1) Der Auftragnehmer setzt geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO um, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die zum Zeitpunkt des Vertragsschlusses geltenden Maßnahmen sind in Anlage 2 beschrieben und gelten als vereinbart.

(2) Der Auftragnehmer ist berechtigt, die technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik und der Weiterentwicklung der IT-Sicherheit anzupassen und weiterzuentwickeln, sofern dadurch das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen der Maßnahmen werden dokumentiert.

(3) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die jeweils aktuelle Fassung der technischen und organisatorischen Maßnahmen zur Verfügung. Soweit eine Änderung wesentliche Auswirkungen auf die Sicherheit der Verarbeitung hat, informiert der Auftragnehmer den Auftraggeber in angemessener Frist vor Inkrafttreten der Änderung.

Berichtigung, Sperrung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Dominik Fünkner bestellt. Kontaktdaten

  > KONTAKTDATEN DATENSCHUTZBEAUFTRAGTER
  >
  > PROLIANCE GmbH
  > Leopoldstr. 21
  > 80802 München
  > dsb@datenschutzexperte.de
  > Tel.: +49 89 2500 392 20

- Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO und Anlage 2.

- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

Unterauftragsverhältnisse

Unterauftragnehmer sind Dritte, die im Auftrag des Auftragnehmers personenbezogene Daten im Zusammenhang mit der Leistungserbringung verarbeiten. Hierzu können auch Unterstützungsleistungen wie Hosting, Wartung, Support oder Monitoring gehören, sofern hierbei personenbezogene Daten verarbeitet werden.

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung zur Beauftragung weiterer Unterauftragnehmer im Sinne von Art. 28 Abs. 2 DSGVO. Der Auftragsverarbeiter informiert den Verantwortlichen rechtzeitig vor einer beabsichtigten Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bestehender Unterauftragnehmer. Der Verantwortliche hat das Recht, innerhalb von 3 Wochen nach Mitteilung der geplanten Änderung Einspruch zu erheben, sofern berechtigte datenschutzrechtliche Gründe vorliegen. Ein Sonderkündigungsrecht in diesem Fall wird eingeräumt.

(2) Der Auftragsverarbeiter versichert, alle Subunternehmer sorgfältig auszuwählen und dabei sicherzustellen, dass diese die Anforderungen des Art. 32 DSGVO durch geeignete technische und organisatorische Maßnahmen (z. B. branchenspezifische Zertifizierungen wie ISO 27001) erfüllen. Die relevanten Prüfunterlagen werden dem Auftraggeber auf Anfrage innerhalb angemessener Frist zur Verfügung gestellt.

(3) Der Auftragsverarbeiter überprüft regelmäßig die Einhaltung der Datenschutzpflichten durch seine Unterauftragnehmer und dokumentiert die Ergebnisse. Diese Dokumentation wird dem Verantwortlichen auf Anfrage bereitgestellt. Direkte physische Kontrollen durch den Verantwortlichen oder Dritte bei Unterauftragnehmern sind nicht vorgesehen, da der Auftragsverarbeiter die Verantwortung für die Einhaltung der Datenschutzstandards übernimmt.

(4) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(5) Zurzeit sind die in Anlage 3 aufgeführten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Kontrollrechte des Auftraggebers

(1) Kontrollen erfolgen vorrangig durch Auskünfte, Dokumentationen, Sicherheitsnachweise, Zertifikate, Prüfberichte und sonstige geeignete Nachweise. Soweit diese Nachweise im Einzelfall nicht ausreichen, um die Einhaltung der Pflichten nach Art. 28 DSGVO angemessen zu überprüfen, ermöglicht der Auftragnehmer nach vorheriger Abstimmung auch weitergehende Prüfungen, einschließlich Inspektionen in angemessenem Umfang. Dabei sind Vertraulichkeit, Betriebs- und Sicherheitsinteressen des Auftragnehmers sowie Rechte Dritter zu wahren. Vor-Ort-Prüfungen erfolgen nur nach angemessener Vorankündigung, während üblicher Geschäftszeiten und soweit sie im konkreten Fall erforderlich und verhältnismäßig sind.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen, soweit diese nicht aus den bestehenden und zugänglichen Dokumenten ersichtlich sind.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder eine geeignete Zertifizierung durch IT Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen, soweit die Kontrolle nicht aufgrund eines nachweisbaren Verstoßes des Auftragnehmers gegen diese Vereinbarung oder gegen datenschutzrechtliche Pflichten erforderlich geworden ist.

Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden, zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Dies gilt auch für die Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation, sofern der Auftragnehmer nicht durch Unionsrecht oder das Recht eines Mitgliedstaats, dem er unterliegt, hierzu verpflichtet ist. In diesem Fall informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung über diese rechtliche Verpflichtung, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Support- und Fehleranalysezugriff (kontogebundener Zugriff / Impersonation)

(1) Der Auftraggeber weist den Auftragnehmer an und ermächtigt ihn, zum Zweck der Fehleranalyse, Störungsbeseitigung, technischen Unterstützung und Bearbeitung von Support-Anfragen im erforderlichen Umfang auf die im Auftrag verarbeiteten personenbezogenen Daten zuzugreifen, einschließlich des Zugriffs über die Benutzeroberfläche in der Ansicht eines Nutzerkontos (Impersonation). Diese Weisung gilt als dokumentierte allgemeine Weisung i.S.d. Art. 28 Abs. 3 DSGVO; einer gesonderten Einzelfallweisung oder -freigabe bedarf es nicht.

(2) Der Zugriff erfolgt zweckgebunden, nach dem Grundsatz der Datenminimierung und ausschließlich durch berechtigtes, auf die Vertraulichkeit verpflichtetes (Art. 28 Abs. 3 lit. b, Art. 29, 32 Abs. 4 DSGVO) und geschultes Personal des Auftragnehmers.

(3) Sämtliche Impersonation- bzw. Support-Zugriffe werden protokolliert (Zeitpunkt, zugreifende Person, betroffenes Konto, Zweck). Die Protokolle werden dem Auftraggeber auf Anfrage im Rahmen seiner Kontrollrechte (Ziffer 8) zur Verfügung gestellt.

(4) Auch im Rahmen dieses Zugriffs verarbeitet der Auftragnehmer die Daten ausschließlich im Rahmen dieses Vertrags und nicht zu eigenen Zwecken.

Löschung und Rückgabe von personenbezogenen Daten

(1) 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer 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. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Homeoffice

Die Verarbeitung von Daten in Privatwohnungen durch Beschäftigte des Auftragnehmers ist gestattet. Die Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 DSGVO und Kontrollmöglichkeiten sind auch in solchen Fällen vom Auftragnehmer zu gewährleisten. Die regelmäßige Überprüfung dieser Maßnahmen obliegt dem Auftragsverarbeiter. Er hat diese zu dokumentieren und diese Dokumentation auf Anforderung dem Auftraggeber zur Verfügung zu stellen

Sonstige Vereinbarungen

14.1 Entgelte

Ein Entgelt für diesen Auftrag wird nicht gefordert. Soweit der Auftraggeber Unterstützung nach Ziffer 5 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten. Soweit der Auftraggeber nach Ziffer 8 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters. Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 10, die über den vereinbarten Leistungsumfang hinausgehen oder zusätzliche Aufwände verursachen, so hat er die hierdurch entstehenden angemessenen Kosten zu erstatten.

Eine Vergütungspflicht besteht nicht, soweit die jeweilige Unterstützung, Kontrolle oder Maßnahme aufgrund eines nachweisbaren Verstoßes des Auftragnehmers gegen diese Vereinbarung oder gegen datenschutzrechtliche Pflichten erforderlich geworden ist.

14.2 Vertragsdauer

Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 2. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 2 beendet diese Vereinbarung, vorbehaltlich der nachfolgenden Fortgeltungsregelung. Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

Soweit nach Beendigung des Hauptvertragsverhältnisses noch personenbezogene Daten im Zusammenhang mit Rückgabe, Export, Löschung, Sperrung, Backup-Retention, Nachweisführung oder gesetzlichen Aufbewahrungspflichten verarbeitet werden, gelten die Regelungen dieser Vereinbarung bis zum vollständigen Abschluss dieser Verarbeitungsvorgänge fort.

14.3 Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland

14.4 Gerichtsstand

Die Parteien vereinbaren als Gerichtsstand den Sitz des für Neu-Ulm zuständigen Gerichts.

Unterschriften

AUFTRAGNEHMER

Dr. Peter Schenkel

Geschäftsführer
faktoora GmbH

Ort, Datum, Unterschrift

AUFTRAGGEBER

Name:

Ort, Datum, Unterschrift

Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO

Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung

I. Art der Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Firmenbezeichnung mit Namen der Ansprechpartner und Adresse der Firma
- Kontaktdaten
- Benutzer- und Zugangs-/Authentifizierungsdaten (z. B. Benutzerkennung, Rollen/ Berechtigungen, Zugriffsprotokolle)
- Nutzungs- und Protokolldaten (z. B. IP-Adresse, Zeitstempel, technische Metadaten)
- Zahlungsdaten
- Kundendaten der Firma zur Rechnungsstellung
- Produktbezeichnungen und Dienstleistungsbezeichnungen der Firma

II. Kreis der Betroffenen

Kreis der von der Datenverarbeitung betroffenen Personen:

- Mitarbeiter und Kunden des Auftraggebers
- Partner und Servicedienstleister des Auftraggebers
- Lieferanten des Auftraggebers

III. Art und Zweck der Verarbeitung

Bereitstellung einer Web-Anwendung, die die Erstellung von Rechnungen und Gutschriften gemäß EN16931 und anderen Formaten ermöglicht.

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

> HINWEIS
>
> Spezielle Maßnahmen für das Arbeiten im Homeoffice orientieren sich an den empfohlenen Maßnahmen des BSI (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html)

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

a. Zutrittskontrolle

RECHENZENTRUM

Unsere Server befinden sich in den deutschen Rechenzentren der Hetzner Online GmbH.

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters

VERWALTUNG/HOMEOFFICE

- Zugang zu Systemen, über die auf Server und Applikationen zugegriffen werden könnte, sind in abschließbaren Räumen bzw. in einem separaten abschließbaren Raum (z.B. bei Homeoffice)
- Geschäftskritische Unterlagen, die Rückschlüsse auf Kundenbeziehungen und/oder deren Kundendaten zulassen (Verträge, gedruckte Schriftwechsel etc.) werden ausschließlich in gesicherten Aktenschränken archiviert
- Beim Verlassen des Arbeitsplatzes werden Arbeitsplatzgeräte stets gesperrt
- Ausschließlich datenschutzrechtlich geschultes und sensibilisiertes Personal greift für Supportzwecke auf personenbezogene Daten zu
- Keine Datenverarbeitung in Anwesenheit Dritter

b. Zugangskontrolle

RECHENZENTRUM

Administrative Zugangsdaten und Zugriffsmittel für Server- und Infrastruktursysteme sind nur den jeweils berechtigten Mitarbeitern des Auftragnehmers zugänglich und werden ausschließlich zum Zwecke der Administration, Wartung und Kontrolle der Infrastruktur verwendet.

HOMEOFFICE

- Alle Passwörter für den Zugriff Konten oder Systeme werden lokal ausschließlich in verschlüsselten Kennwortverwaltungsprogrammen (z.B. KeePass) gespeichert.

c. Zugriffskontrolle

INFRASTRUKTUR

- Der Infrastrukturprovider betreibt seine Infrastruktur nach einem dokumentierten Sicherheitskonzept; der Auftragnehmer berücksichtigt bei der Auswahl u. a. anerkannte Sicherheitsnachweise/Zertifizierungen.
- Der Infrastrukturprovider setzt Zutritts- und Zugriffskontrollen nach anerkannten Standards um; Nachweise ergeben sich aus entsprechenden Zertifizierungen/Prüfberichten des Providers.
- die Verantwortung der Zugriffskontrolle obliegt den Mitarbeitern des Auftragnehmers.

APPLIKATIONEN / INTERNE VERWALTUNGSSYSTEME

- werden durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) sichergestellt, dass unberechtigte Zugriffe verhindert werden.
- sind nur durch passwortgeschützte, personalisierte Zugänge erreichbar
- mit Zugriff auf Kundendaten sind zusätzlich nur über ein VPN oder SSH-Tunnel erreichbar
- Regelmäßige Überprüfung und Anpassung der Zugriffsberechtigungen

d. Datenträgerkontrolle

RECHENZENTRUM

- Festplatten werden durch den Infrastrukturanbieter mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum des Infrastrukturproviders zerstört (geschreddert).

ALLGEMEIN / HOMEOFFICE

- Nicht mehr benötigte oder defekte Datenträger von Mitarbeitern werden mehrfach überschrieben (gelöscht) und vernichtet.
- Sensible Daten werden lokal ausschließlich verschlüsselt auf Datenträgern gespeichert.

e. Trennungskontrolle

- Kundendaten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung der Kundendaten erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a. Weitergabekontrolle

ALLGEMEIN

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Daten werden ausschließlich verschlüsselt übertragen (TLS)

HOMEOFFICE

- Die Mitarbeiter werden angewiesen vertrauliche Dokumente/Ausdrucke nur in Ausnahmefällen zu erstellen und unmittelbar nach der Verwendung zu vernichten. Die notwendige Hardware wird zu Verfügung gestellt (z.B. Aktenvernichter).
- Die Mitarbeiter werden angewiesen und geschult nicht mehr benötigte Datenträger einer angemessenen Vernichtung zuzuführen.

b. Protokollierung / Monitoring / Fehleranalyse

Zur Sicherstellung von Stabilität, Verfügbarkeit und Fehlerbehebung werden technische Ereignis- und Diagnosedaten verarbeitet. Die Verarbeitung erfolgt nach dem Prinzip der Datenminimierung; identifizierende Inhalte werden soweit möglich reduziert bzw. durch Filter/Scrubbing entfernt. Zugriffe auf Diagnose- und Monitoring-Systeme sind rollenbasiert beschränkt und werden protokolliert. Aufbewahrungsfristen für Diagnose-/Fehlerdaten sind zweckgebunden begrenzt. Ein kontogebundener Support-Zugriff (Impersonation) auf Nutzerkonten erfolgt ausschließlich rollenbasiert durch berechtigtes Personal und wird protokolliert (Zeitpunkt, zugreifende Person, betroffenes Konto, Zweck)."

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a. Verfügbarkeitskontrolle

SERVER

- Unsere Server befinden sich in einem Hetzner-Rechenzentrum in Deutschland, das nach ISO 27001 zertifiziert ist.
- Daten werden regelmäßig gesichert.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.

HOMEOFFICE

- Lokal gespeicherte Daten werden kontinuierlich auf einem zentralen Backupserver gesichert.

b. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

SERVER

- Für alle Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

HOMEOFFICE

- Daten der Mitarbeiter können von dem zentralen Backupserver wiederhergestellt werden.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Diese umfassen

- Sorgfältige Auswahl von Subunternehmern/Auftragsverarbeitern, vor allem in Bezug auf den Datenschutz
- Abschluss notwendiger Vereinbarungen mit eventuellen Subunternehmern/Auftragsverarbeitern und deren Überprüfung

b. Organisationskontrolle

Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Diese umfasst folgende Maßnahmen

- Regelmäßige Schulung aller mit personenbezogenen Daten in Berührung kommenden Personen, um die Einhaltung der gesetzlichen Vorschriften zu gewährleisten
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens einmal jährlich durchgeführt.
- Kundenspezifische Dokumentation von Weisungen und Tätigkeiten im Rahmen der Auftragsverarbeitung
- Datenschutzvorfälle werden unverzüglich dokumentiert und ausgewertet.

Anlage 3 Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag personenbezogene Daten verarbeiten („Unterauftragnehmer“). Dabei handelt es sich um folgende Unternehmen:

1. **Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland**

   LEISTUNG/ZWECK

   Hosting / Rechenzentrums- und Infrastrukturleistungen (Betrieb der Server-, Speicher- und Backup-Umgebung)

   ORT DER VERARBEITUNG

   Deutschland / EU (EU/EWR)

   DATENKATEGORIEN

   alle in Anlage 1 genannten Daten, soweit im Rahmen des Hostings gespeichert oder verarbeitet

2. **Functional Software, Inc. d/b/a Sentry (Sentry.io), 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA**

   LEISTUNG/ZWECK

   Fehler- und Performance-Monitoring (Error Tracking / APM) zur Stabilitätsanalyse und Fehlerdiagnose

   ORT DER VERARBEITUNG

   EU (EU Data Residency / EU-Region konfiguriert); etwaige Zugriffe aus Drittländern nur im erforderlichen Umfang und unter Einhaltung Art. 44 ff. DSGVO.

   DATENKATEGORIEN

   technische Ereignis- und Diagnosedaten (z. B. Fehlerereignisse, Stacktraces, Zeitstempel, Release-/Build-Metadaten), nach dem Prinzip der Datenminimierung/Filterung