AV

AUFTRAGSVERARBEITUNG

Auftragsverarbeitung

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag

Hinweis:** Diese Fassung gilt ab dem 01.12.2026. Bis zum 30.11.2026 gilt die bisherige Fassung: [AVV Version 4.1 (PDF)](https://faktoora.com/dokumente/faktoora-avv-v4.1.pdf). · gültig ab 01.12.2026

VERSION	STAND	AUFTRAGNEHMER	GESCHÄFTSFÜHRER	SITZ
4.2	01.12.2026	faktoora GmbH	Dr. Peter Schenkel	Amselweg 1, 89231 Neu-Ulm

Inhaltsverzeichnis

	Vertragsparteien	03
01	Allgemeines	04
02	Gegenstand und Dauer des Auftrags	05
03	Umfang, Art und Zweck der Verarbeitung von Daten	06
04	Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO	07
05	Berichtigung, Einschränkung der Verarbeitung und Löschung von Daten	08
06	Qualitätssicherung und sonstige Pflichten des Auftragnehmers	09
07	Unterauftragsverhältnisse	10
08	Kontrollrechte des Auftraggebers	11
09	Unterstützung nach Art. 32 bis 36 DSGVO und Meldung von Datenschutzverletzungen	12
10	Weisungsbefugnis des Auftraggebers	13
11	Support- und Fehleranalysezugriff (kontogebundener Zugriff / Impersonation)	14
12	Löschung und Rückgabe von personenbezogenen Daten	15
13	Mobiles Arbeiten (Remote-first)	16
14	Sonstige Vereinbarungen	17
	Unterschriften	18
A1	Anlage 1 · Personenbezogene Daten und Zweck der Verarbeitung	19
A2	Anlage 2 · Technische und organisatorische Maßnahmen	20
A3	Anlage 3 · Unterauftragnehmer	24

Vertragsparteien

Auftrag gemäß Art. 28 DSGVO (Version 4.2, gültig ab 01.12.2026)

Vereinbarung zwischen

AUFTRAGNEHMER

faktoora GmbH, Amselweg 1, 89231 Neu-Ulm

– Auftragnehmer –

und

AUFTRAGGEBER

(Der Auftraggeber ergibt sich aus dem jeweiligen Vertragsverhältnis.)

– 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 Verarbeitung von Daten

Der Umfang, die Art und der Zweck der Verarbeitung 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 2 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 DSGVO

(Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(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.

Berichtigung, Einschränkung der Verarbeitung 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) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte der betroffenen Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 Satz 2 lit. e DSGVO). Löschung, Berichtigung, Datenportabilität und Auskunft setzt er nach dokumentierter Weisung des Auftraggebers um.

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- Als Datenschutzbeauftragter ist beim Auftragnehmer die PROLIANCE GmbH bestellt: Leopoldstr. 21, 80802 München, datenschutzbeauftragter@datenschutzexperte.de
- Die jeweils aktuellen Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt; ein Wechsel wird dort veröffentlicht.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 Satz 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 gemäß 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 in angemessenem Umfang zu unterstützen; Ziffer 14.1 gilt.
- 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 Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zur Beauftragung weiterer Unterauftragnehmer im Sinne von Art. 28 Abs. 2 DSGVO. Der Auftragnehmer informiert den Auftraggeber mindestens drei Wochen vor einer beabsichtigten Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bestehender Unterauftragnehmer in Textform. Der Auftraggeber hat das Recht, innerhalb von drei Wochen nach Zugang der Mitteilung Einspruch zu erheben, sofern berechtigte datenschutzrechtliche Gründe vorliegen. Erhebt der Auftraggeber berechtigten Einspruch und wird keine einvernehmliche Lösung gefunden, kann jede Partei den Hauptvertrag und diese Vereinbarung außerordentlich zum Zeitpunkt des Wirksamwerdens der Änderung kündigen. Kündigt keine Partei bis zum Wirksamwerden, kann der Auftragnehmer die Änderung umsetzen. In dringenden Fällen, insbesondere aus Sicherheitsgründen oder bei Wegfall eines Unterauftragnehmers, genügt eine unverzügliche nachträgliche Mitteilung; das Einspruchsrecht gilt entsprechend. Die Sätze 2 bis 6 gelten entsprechend, wenn ein bestehender Unterauftragnehmer die Verarbeitung in ein Drittland verlagert.

(2) Der Auftragnehmer versichert, alle Unterauftragnehmer 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, soweit der Unterauftragnehmer ihre Weitergabe gestattet.

(3) Der Auftragnehmer überprüft regelmäßig die Einhaltung der Datenschutzpflichten durch seine Unterauftragnehmer und dokumentiert die Ergebnisse. Nachweise darüber stellt er dem Auftraggeber auf Anfrage bereit, soweit Vertraulichkeitspflichten gegenüber dem Unterauftragnehmer nicht entgegenstehen. Kontrollen bei Unterauftragnehmern erfolgen vorrangig anhand ihrer Zertifizierungen und Prüfberichte; die Kontrollrechte des Auftraggebers nach Ziffer 8 und Art. 28 Abs. 3 Satz 2 lit. h DSGVO bleiben unberührt.

(4) Der Auftragnehmer erlegt jedem Unterauftragnehmer vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen der DSGVO entspricht (Art. 28 Abs. 4 DSGVO).

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

(6) Zurzeit sind die in Anlage 3 aufgeführten Unterauftragnehmer 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. Der Auftraggeber kann Prüfungen selbst oder durch einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer durchführen, der nicht im Wettbewerb zum Auftragnehmer steht. Inspektionen finden in der Regel höchstens einmal je Kalenderjahr statt, es sei denn, ein konkreter Anlass oder eine Aufsichtsbehörde erfordert eine weitere Prüfung.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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 DSGVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, 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) Die Bereitstellung vorhandener Nachweise und die Erteilung von Auskünften nach den Absätzen 1 bis 3 erfolgen unentgeltlich. Für Inspektionen sowie für individuelle Prüfungen und Fragebögen kann der Auftragnehmer eine angemessene Vergütung nach seinen jeweils gültigen Stundensätzen verlangen, soweit die Kontrolle nicht aufgrund eines nachweisbaren Verstoßes des Auftragnehmers gegen diese Vereinbarung oder gegen datenschutzrechtliche Pflichten erforderlich geworden ist.

Unterstützung nach Art. 32 bis 36 DSGVO und Meldung von Datenschutzverletzungen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen 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 zeitnahe Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden; die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO, noch nicht vorliegende Informationen werden schrittweise nachgereicht (Art. 33 Abs. 4 DSGVO)

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang die ihm vorliegenden relevanten Informationen unverzüglich 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 und 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. Die Weisungen sind in dieser Vereinbarung und im Hauptvertrag festgelegt und werden durch die Nutzung der Funktionen der Plattform erteilt. 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 Satz 2 lit. b, Art. 29, 32 Abs. 4 DSGVO) Personal des Auftragnehmers.

(3) Zugriffe über die Benutzeroberfläche (Impersonation) werden mit Zeitpunkt, zugreifender Person und betroffenem Konto protokolliert; administrative Zugriffe auf Produktivsysteme werden personenbezogen protokolliert. 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 Kopien, die der Auftragnehmer zur Erfüllung eigener gesetzlicher Pflichten benötigt.

(2) Nach Beendigung der Leistungsvereinbarung stellt der Auftragnehmer dem Auftraggeber sämtliche im Auftrag verarbeiteten Daten während eines Abrufzeitraums von 30 Tagen zum Export bereit (Ziffer 5.2 der AGB). Nach Ablauf des Abrufzeitraums oder früher auf Weisung des Auftraggebers löscht der Auftragnehmer diese Daten datenschutzgerecht, einschließlich der Inhalte von API-Anfragen und -Antworten; die Aufbewahrung nach handels- und steuerrechtlichen Vorschriften obliegt dem Auftraggeber. Protokolldaten zu Anmeldungen, Zugriffen und Änderungen (Audit-Trail) sind Teil der im Auftrag verarbeiteten Daten und werden mit diesen gelöscht. Sicherungskopien werden im regulären Backup-Zyklus von bis zu 12 Monaten überschrieben; bis dahin sind sie verschlüsselt und zugriffsbeschränkt und werden nur zur Wiederherstellung verwendet. Werden Daten aus einer Sicherungskopie wiederhergestellt, wendet der Auftragnehmer zuvor ausgeführte Löschungen erneut an. 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.

Mobiles Arbeiten (Remote-first)

(1) Der Auftragnehmer arbeitet ortsunabhängig („Remote-first“) und unterhält keine eigenen Büro- oder Serverräume. Die Plattform wird in Rechenzentren in Deutschland betrieben (Anlage 2); für Unterauftragnehmer gilt Anlage 3.

(2) Beschäftigte und sonstige für den Auftragnehmer tätige Personen dürfen ihre Tätigkeit aus Privatwohnungen und von anderen mobilen Arbeitsorten aus erbringen. Dabei gilt insbesondere:

- Der Zugriff auf die Systeme des Auftragnehmers erfolgt ausschließlich verschlüsselt und mit persönlicher Authentifizierung.
- Arbeitsgeräte sind vollverschlüsselt, sperren sich bei Inaktivität automatisch und werden mit aktuellen Sicherheitsupdates betrieben.
- Daten des Auftraggebers werden auf Arbeitsgeräten nur gespeichert, soweit dies zur Fehleranalyse und zum Nachstellen gemeldeter Fehler im Einzelfall erforderlich ist, und nach Abschluss der Analyse gelöscht. Auf Wechseldatenträgern oder in privaten Cloud-Speichern werden sie nicht gespeichert.
- Es wird so gearbeitet, dass Dritte keine Einsicht in personenbezogene Daten nehmen können; über öffentliche Netzwerke wird auf Produktivsysteme nur über eine gesicherte Verbindung zugegriffen.

(3) Ein Zugriff auf personenbezogene Daten des Auftraggebers von einem Arbeitsort außerhalb der EU/EWR ist nur unter den Voraussetzungen der Art. 44 ff. DSGVO zulässig (Ziffer 3).

(4) Der Auftragnehmer gewährleistet die Maßnahmen nach Art. 32 DSGVO (Anlage 2) auch beim mobilen Arbeiten, überprüft sie regelmäßig, dokumentiert dies und stellt die Dokumentation dem Auftraggeber auf Anforderung zur Verfügung. Kontrollen nach Ziffer 8 erfolgen insoweit anhand dieser Dokumentation und sonstiger Nachweise; ein Zutritt zu Privatwohnungen ist ausgeschlossen.

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. Für Kontrollen gilt Ziffer 8 Abs. 4. Datenexport und Anbieterwechsel nach Ziffer 5.2 der AGB sind unentgeltlich. 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, Backup-Retention oder Nachweisführung 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

Für den Gerichtsstand gilt Ziffer 12.1 der AGB.

14.5 Haftung

Für die Haftung gilt Ziffer 9 der AGB; Art. 82 DSGVO bleibt unberührt.

Unterschriften

AUFTRAGNEHMER

Dr. Peter Schenkel

Geschäftsführer
faktoora GmbH

Ort, Datum, Unterschrift

AUFTRAGGEBER

(im Einzelvertrag)

Ort, Datum, Unterschrift

Anlage 1 · Personenbezogene Daten und Zweck der Verarbeitung

Anlage 1 zum Auftrag gemäß Art. 28 DSGVO – 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
- Ausgangs- und Eingangsrechnungen samt Anhängen
- Banktransaktionen (bei Anbindung eines Bankkontos)
- Kommunikations- und Übermittlungsdaten (E-Mail-Versand und -Empfang, Peppol, Übermittlungen an Steuerbehörden)
- API-Protokolle (Anfragen und Antworten an die Programmierschnittstelle)
- 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
- Rechnungsempfänger und Rechnungsabsender des Auftraggebers

III. Art und Zweck der Verarbeitung

Bereitstellung einer Web-Anwendung und Programmierschnittstelle für die Erstellung, den Empfang, die Prüfung, die Zustellung und die Speicherung während der Vertragslaufzeit von Rechnungen, Gutschriften und weiteren Geschäftsdokumenten gemäß EN 16931 und weiteren Formaten; Zahlungsabgleich; Übermittlung an E-Rechnungsnetzwerke und Steuerbehörden; optionale automatische Datenerfassung aus Eingangsrechnungen; Support.

Anlage 2 · Technische und organisatorische Maßnahmen

Anlage 2 zum Auftrag gemäß Art. 28 DSGVO – Technische und organisatorische Maßnahmen nach Art. 32 DSGVO.

Hinweis: Spezielle Maßnahmen für das Arbeiten im Homeoffice orientieren sich an den empfohlenen Maßnahmen des BSI (Empfehlungen zum Homeoffice).

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a. Zutrittskontrolle

Rechenzentrum – Unsere Server befinden sich in ISO 27001-zertifizierten deutschen Rechenzentren der Hetzner Online GmbH.

- Zutrittskontrolle, Überwachung und Begleitung von Besuchern gemäß der ISO 27001-Zertifizierung des Rechenzentrumsbetreibers

Verwaltung/Homeoffice

- Arbeitsgeräte sind vollverschlüsselt; Beschäftigte sind angewiesen, sie nicht unbeaufsichtigt zu lassen
- Arbeitsgeräte sperren sich automatisch nach kurzer Inaktivität und werden beim Verlassen des Arbeitsplatzes gesperrt
- Ausdrucke mit personenbezogenen Daten werden nach Gebrauch vernichtet
- Ausschließlich auf Vertraulichkeit und Datenschutz verpflichtetes Personal greift für Supportzwecke auf personenbezogene Daten zu
- Beschäftigte sind angewiesen, personenbezogene Daten nicht in Anwesenheit Dritter zu verarbeiten

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

- Beschäftigte sind angewiesen, Passwörter für den Zugriff auf Konten oder Systeme in einem verschlüsselten Passwortmanager zu speichern.
- Administrative Zugänge zu Server-, Cloud- und Entwicklungssystemen sind mit Mehrfaktor-Authentifizierung geschützt.

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.

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
- Datenbanken und interne Datenspeicher sind nicht aus dem Internet erreichbar; ein direkter Zugriff ist nur über administrative Zugänge mit Mehrfaktor-Authentifizierung möglich
- Administrative Anwendungen erfordern eine Anmeldung über den Identity Provider mit rollenbasierter Berechtigung
- 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.
- Arbeitsgeräte und Datenträger sind vollverschlüsselt; Daten des Auftraggebers werden lokal nur nach Ziffer 13 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 DSGVO)

a. Weitergabekontrolle

Allgemein

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs. 4 DSGVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

- Externe Übertragungen erfolgen verschlüsselt (TLS 1.2 oder höher)
- Produktionssysteme und Backups sind verschlüsselt (Art. 32 Abs. 1 lit. a DSGVO)

Homeoffice

- Die Mitarbeiter werden angewiesen, vertrauliche Dokumente/Ausdrucke nur in Ausnahmefällen zu erstellen und unmittelbar nach der Verwendung zu vernichten.
- Die Mitarbeiter werden angewiesen, 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).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

a. Verfügbarkeitskontrolle

Server

- Unsere Server befinden sich in einem Hetzner-Rechenzentrum in Deutschland, das nach ISO 27001 zertifiziert ist.
- Alle persistenten Datenbestände der Produktivplattform werden in kurzen Abständen (derzeit mindestens alle 2 Stunden) verschlüsselt gesichert und an einem räumlich getrennten Standort gespeichert.
- Stromversorgung und Netzwerkschutz gemäß der ISO 27001-Zertifizierung des Rechenzentrumsbetreibers.

Homeoffice

- Kundendaten werden auf Arbeitsgeräten nur nach Ziffer 13 und nur vorübergehend gespeichert; Arbeitsgeräte sind vollverschlüsselt.

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.
- Die Wiederherstellung aus Sicherungen wird regelmäßig geübt und dokumentiert.

Homeoffice

- Arbeitsgeräte können ohne Verlust von Kundendaten ersetzt werden, da der maßgebliche Datenbestand ausschließlich in der zentral gesicherten Plattform liegt.

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

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 Unterauftragnehmern, vor allem in Bezug auf den Datenschutz
- Abschluss notwendiger Vereinbarungen mit Unterauftragnehmern 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:

- Beschäftigte werden auf Vertraulichkeit verpflichtet und zum Datenschutz unterwiesen
- Die technischen und organisatorischen Maßnahmen werden regelmäßig überprüft und weiterentwickelt.
- Kundenspezifische Dokumentation von Weisungen und Tätigkeiten im Rahmen der Auftragsverarbeitung
- Für Sicherheits- und Datenschutzvorfälle besteht ein dokumentierter Prozess zur Erkennung, Bewertung, Eindämmung und Meldung; Vorfälle werden unverzüglich dokumentiert und ausgewertet.
- Schwachstellen werden durch automatisierte Prüfungen erkannt und risikobasiert behoben.

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:

#	UNTERAUFTRAGNEHMER	LEISTUNG/ZWECK	ORT DER VERARBEITUNG	DATENKATEGORIEN
1	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting / Rechenzentrums- und Infrastrukturleistungen (Betrieb der Server-, Speicher- und Backup-Umgebung, einschließlich der selbst betriebenen Fehlerüberwachung)	Deutschland (EU); Fehlerüberwachung: EU	alle in Anlage 1 genannten Daten, soweit im Rahmen des Hostings gespeichert oder verarbeitet
2	Mailjet SAS (Sinch-Gruppe), Frankreich	Versand transaktionaler E-Mails (Rechnungsversand, Benachrichtigungen)	EU (Deutschland, Belgien); Support-Zugriff aus den USA auf Grundlage des EU-US Data Privacy Framework und der EU-Standardvertragsklauseln	E-Mail-Adressen, E-Mail-Inhalte und Anhänge
3	Mindee SAS, 14 rue Charles V, 75004 Paris, Frankreich	Automatische Datenerfassung aus Eingangsrechnungen (nur bei Aktivierung)	EU	Inhalte hochgeladener Eingangsrechnungen
4	Invopop S.L., Calle Diseminado 1629, Miraflores de la Sierra (Madrid), Spanien	Übermittlung französischer E-Rechnungen und Statusmeldungen (nur Frankreich)	EU (Belgien, Deutschland); Nachrichtenvermittlung ohne Speicherung auch über einen Dienstleister in den USA	Rechnungsdaten
5	OpenAI Ireland Ltd., 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	KI-gestützte Dokumentensuche (nur bei Aktivierung)	USA (OpenAI OpCo, LLC); Übermittlung auf Grundlage der EU-Standardvertragsklauseln	ausschließlich die eingegebene Suchanfrage

Empfänger, die Daten aufgrund einer gesetzlichen Verpflichtung erhalten (z. B. Steuerbehörden bei VeriFactu, KSeF oder der französischen E-Rechnung), zugelassene Zahlungsdienstleister, die Kontoinformations- und Zahlungsauslösedienste gegenüber den Nutzern in eigener Verantwortung erbringen (BANKSapi Technology GmbH, München), sowie vom Auftraggeber selbst angebundene Dienste (z. B. Buchhaltungs-, ERP- oder CRM-Systeme) sind keine Unterauftragnehmer im Sinne dieser Anlage. Die jeweils aktuelle Übersicht ist zusätzlich unter trust.faktoora.com abrufbar.

Diese Fassung gilt ab dem 01.12.2026. Für Auftraggeber, deren Vertrag vor diesem Tag geschlossen wurde, gilt sie ab dem 01.12.2026, frühestens jedoch vier Wochen nach Zugang der Änderungsmitteilung, sofern der Auftraggeber nicht innerhalb dieser Frist widerspricht (Änderungsregelung der bisherigen AGB, künftig Ziffer 8.10 AGB); das Einspruchsrecht gegen neue Unterauftragnehmer nach Ziffer 7 Abs. 1 bleibt unberührt. Bis dahin gilt die bisherige Fassung.