

Auftragsverarbeitungsvertrag

Zuletzt aktualisiert 17.09.2026

Vertrag zur Auftragsverarbeitung

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Anlage zum Nutzungsvertrag über die Software Fristner

Vertragsparteien

Auftraggeber (Verantwortlicher): der Kunde, dessen Firma und Anschrift bei Vertragsschluss im Bestellprozess angegeben und im Nutzerkonto hinterlegt sind.

Auftragnehmer (Auftragsverarbeiter): Max Günther, Fristner, Stettinerweg 23, 74523 Schwäbisch Hall, Deutschland.

Vertragsschluss: Dieser Vertrag wird durch Zustimmung des Kunden im Bestellprozess in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Er ist Bestandteil des Nutzungsvertrags und gilt für dessen gesamte Laufzeit.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

(2) Die Dauer der Verarbeitung entspricht der Laufzeit des Nutzungsvertrags. Nach dessen Beendigung stehen die Daten dem Auftraggeber für 30 Tage zum

Export zur Verfügung; anschließend werden sie gelöscht (§ 3 Abs. 10).

(3) Der Auftraggeber kann diesen Vertrag und den Nutzungsvertrag aus wichtigem Grund fristlos kündigen, wenn der Auftragnehmer schwerwiegend gegen datenschutzrechtliche Pflichten verstößt.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers. Der Auftraggeber ist allein für die Rechtmäßigkeit der Verarbeitung verantwortlich.

(2) Die Weisungen sind durch den Nutzungsvertrag, die Allgemeinen Geschäftsbedingungen und die Leistungsbeschreibung der Software festgelegt. Weitere Weisungen können in Textform (E-Mail) erteilt werden. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

(3) Die Software ist so gestaltet, dass der Auftraggeber die Verarbeitung durch eigene Eingaben, Einstellungen und Freigaben steuert. Diese Handlungen gelten als Weisungen im Sinne dieses Vertrags.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet Daten nur im Rahmen der getroffenen Vereinbarungen und Weisungen.

(2) Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin und kann die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

(3) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind. Er darf sie an den Stand der Technik anpassen, sofern das Schutzniveau nicht unterschritten wird, und dokumentiert wesentliche Änderungen.

(4) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen (Kapitel III DSGVO) sowie bei den Pflichten aus Art. 33 bis 36 DSGVO. Erfordert dies Aufwand, der über die Funktionen der Software hinausgeht, kann der Auftragnehmer eine angemessene Vergütung verlangen.

(5) Der Auftragnehmer stellt sicher, dass mit der Verarbeitung befasste Personen zur Vertraulichkeit verpflichtet sind; die Verpflichtung besteht nach Beendigung der Tätigkeit fort.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Verletzungen des Schutzes personenbezogener Daten. Die Meldung enthält, soweit bekannt: Art des Vorfalls, betroffene Datenkategorien und ungefähre Anzahl der Betroffenen, Ansprechpartner, voraussichtliche Folgen und ergriffene Maßnahmen. Die Meldung erfolgt an die im Nutzerkonto hinterlegte E-Mail-Adresse des Auftraggebers.

(7) Ansprechpartner des Auftragnehmers für Datenschutz ist Max Günther, erreichbar unter kontakt@fristner.de oder telefonisch unter 0791 20213498. Ein Datenschutzbeauftragter ist nach § 38 BDSG nicht zu benennen.

(8) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen nach Anlage 2 regelmäßig.

(9) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung ein, wenn der Auftraggeber dies weist. Der Auftraggeber kann Berichtigung und Löschung in der Regel selbst in der Software vornehmen.

(10) Nach Beendigung des Nutzungsvertrags löscht der Auftragnehmer alle personenbezogenen Daten des Auftraggebers einschließlich Sicherungskopien innerhalb von 60 Tagen nach Ablauf der Exportfrist nach § 1 Abs. 2, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Auf Weisung des Auftraggebers stellt er vor der Löschung einen vollständigen Export der Daten bereit. Auf Verlangen bestätigt er die Löschung in Textform.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

(2) Der Auftraggeber ist dafür verantwortlich, dass die Verarbeitung der in Anlage 1 genannten Daten in der Software eine Rechtsgrundlage hat und die betroffenen Personen informiert sind.

(3) Der Auftraggeber verarbeitet in der Software keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Ansprüchen nach Art. 15 bis 21 DSGVO an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter und unterstützt ihn bei der Beantwortung im Rahmen von § 3 Abs. 4.

§ 6 Nachweismöglichkeiten und Kontrollrechte

(1) Der Auftragnehmer weist die Einhaltung seiner Pflichten mit geeigneten Mitteln nach, insbesondere durch die Dokumentation nach Anlage 2, Auskünfte in Textform und, soweit vorhanden, Zertifizierungen oder Prüfberichte seiner Subunternehmer.

(2) Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrags zu überprüfen. Die Überprüfung erfolgt in erster Linie durch schriftliche Auskunft und Vorlage von Nachweisen. Für das Rechenzentrum gilt der Nachweis durch die ISO-27001-Zertifizierung des Subunternehmers (Anlage 3); ein Zutritt ist dort nicht möglich. Eine Vor-Ort-Kontrolle beim Auftragnehmer ist bei konkretem Anlass nach vorheriger Ankündigung mit angemessener Frist während der üblichen Geschäftszeiten möglich. Jede Partei trägt ihre eigenen Kosten.

(3) Beauftragt der Auftraggeber einen Dritten mit der Kontrolle, ist dieser zur Vertraulichkeit zu verpflichten. Der Auftragnehmer kann einen Dritten ablehnen,

der in einem Wettbewerbsverhältnis zu ihm steht.

§ 7 Subunternehmer

(1) Der Auftragnehmer setzt für die Erbringung der Leistung die in Anlage 3 genannten Subunternehmer ein. Der Auftraggeber stimmt deren Einsatz mit Abschluss dieses Vertrags zu.

(2) Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen (Hinzufügen oder Ersetzen von Subunternehmern) mindestens 30 Tage im Voraus in Textform. Der Auftraggeber kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Bei begründetem Widerspruch kann der Auftraggeber den Nutzungsvertrag zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.

(3) Der Auftragnehmer verpflichtet Subunternehmer vertraglich zu Datenschutzpflichten, die denen dieses Vertrags entsprechen, und überprüft deren Einhaltung in angemessenem Umfang.

§ 8 Übermittlung in Drittstaaten

(1) Die Verarbeitung findet grundsätzlich in Mitgliedstaaten der EU oder des EWR statt. Die Speicherung der Daten erfolgt auf Servern in Deutschland (Anlage 3).

(2) Eine Übermittlung in Drittstaaten findet nicht statt. Will der Auftragnehmer einen Subunternehmer in einem Drittstaat einsetzen, gilt § 7 Abs. 2; die Übermittlung setzt Garantien nach Kapitel V DSGVO voraus.

§ 9 Haftung

(1) Für die Haftung der Parteien gelten die Regelungen des Nutzungsvertrags und der Allgemeinen Geschäftsbedingungen, soweit Art. 82 DSGVO nichts Zwingendes bestimmt.

§ 10 Informationspflichten, Schriftform, Rechtswahl

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn die Daten des Auftraggebers durch Pfändung, Beschlagnahme, Insolvenzverfahren oder Maßnahmen Dritter gefährdet werden, und weist die Beteiligten darauf hin, dass die Daten im Auftrag verarbeitet werden und der Auftraggeber über sie verfügt.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform und müssen ausdrücklich auf diesen Vertrag Bezug nehmen. Das gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

(4) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 – Gegenstand der Verarbeitung

Gegenstand und Zweck

Bereitstellung der Software Fristner zur Verwaltung von Prüfobjekten, Prüffristen, Prüfungen, Mängeln und Prüfnachweisen des Auftraggebers. Zweck ist die Erfüllung der Prüf- und Dokumentationspflichten des Auftraggebers für Arbeitsmittel, insbesondere nach BetrSichV, sowie die Erinnerung an fällige Prüfungen.

Art der Verarbeitung

Speichern, Anzeigen, Ändern, Auswerten, Exportieren und Löschen von Daten in der Software; Versand von Erinnerungen und Systemnachrichten per E-Mail; Erstellung von Berichten und Prüfplaketten.

Kategorien personenbezogener Daten

- Stammdaten von Nutzern des Auftraggebers: Name, E-Mail-Adresse, Rolle, Standortzuordnung
- Angaben zu prüfenden Personen: Name, Qualifikation, Firma bei externen Prüfern
- Prüf- und Mängeldaten mit Personenbezug: Name der prüfenden Person, Zeitpunkt, Ergebnis, Freitexte, Fotos
- Nutzungs- und Protokolldaten: Anmeldezeitpunkte, IP-Adressen, technische Ereignisse

Kategorien betroffener Personen

- Beschäftigte des Auftraggebers
- Externe Prüfer, Sicherheitsfachkräfte und Dienstleister, denen der Auftraggeber Zugang gewährt

Dauer

Laufzeit des Nutzungsvertrags zuzüglich 30 Tage Exportfrist und bis zu 60 Tage Löschfrist.

Anlage 2 – Technische und organisatorische Maßnahmen

Zutritts- und Zugangskontrolle

- Betrieb der Software auf einem Server der Hetzner Online GmbH in einem Rechenzentrum in Deutschland (ISO 27001-zertifiziert); Zutritt zum Rechenzentrum ausschließlich durch Hetzner
- Zugang zur Software nur mit persönlichem Konto und Passwort nach Mindestanforderungen; Einladung neuer Nutzer nur durch berechtigte Nutzer des Auftraggebers
- Administrativer Zugang zum Server nur per SSH mit Schlüssel, Passwort-Login deaktiviert; Zugang zum Hetzner-Konto mit Zwei-Faktor-Authentifizierung

- Firewall auf dem Server, nur die für den Betrieb nötigen Ports geöffnet

Zugriffskontrolle

- Rollen- und Rechtekonzept in der Software: Nutzer sehen nur Daten des eigenen Auftraggebers und der zugewiesenen Standorte
- Mandantentrennung auf Datenbankebene durch Zuordnung jedes Datensatzes zu genau einem Auftraggeber
- Protokollierung wesentlicher Änderungen (Anlegen, Ändern, Löschen von Prüfobjekten und Prüfungen) mit Nutzer und Zeitpunkt

Weitergabe- und Transportkontrolle

- Verschlüsselte Übertragung aller Daten (TLS 1.2 oder höher)
- Verschlüsselte Sicherungen: Datenbank-Sicherungen werden vor dem Verlassen des Servers mit einem Public-Key-Verfahren (age) verschlüsselt; der private Schlüssel liegt nicht auf dem Server
- Datenexport nur durch berechtigte Nutzer des Auftraggebers aus dem Konto heraus
- Versand von E-Mails über einen Anbieter in der EU (Anlage 3), verschlüsselt per TLS

Verfügbarkeit und Belastbarkeit

- Automatische Sicherungen der Datenbank alle sechs Stunden, Aufbewahrung 35 Tage (7 Tage vollständig, danach wöchentlich), verschlüsselte Speicherung auf einer Hetzner Storage Box in Deutschland
- Regelmäßige Sicherheitsupdates des Betriebssystems und der eingesetzten Software
- Wiederherstellung aus Sicherungen wird monatlich automatisch getestet
- Trennung von Entwicklungs- und Produktivumgebung

Verfahren zur regelmäßigen Überprüfung

- Jährliche Überprüfung dieser Maßnahmen durch den Auftragnehmer
- Verwaltung von Datenschutzvorfällen nach dem Meldeprozess in § 3 Abs. 6
- Verpflichtung aller mit der Entwicklung befassten Personen auf Vertraulichkeit

Anlage 3 – Subunternehmer

Subunternehmer	Leistung	Sitz, Verarbeitungsort, Grundlage
Hetzner Online GmbH	Server - Hosting (Anwendung, Datenbank, Dateiablage, Sicherungen)	Sitz Deutschland · Rechenzentrum Falkenstein · Verarbeitung in Deutschland
Scaleway SAS (Transactional Email)	Versand von Erinnerungen und Systemnachrichten	Sitz Frankreich · Verarbeitung in der EU

Stand der Liste: 17.09.2026. Änderungen werden nach § 7 Abs. 2 angekündigt.