

Vereinbarung zur Auftragsverarbeitung

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO zwischen der Krafteq GmbH und ihren Kunden — Bestandteil des Angebots, kein gesondert zu unterzeichnendes Dokument.

Parteien

Diese Vereinbarung gilt zwischen der

Krafteq GmbH

Marie-Curie-Straße 8 · 51377 Leverkusen · Deutschland

Geschäftsführer: Ivan Bianco · Amtsgericht Köln, HRB 119397 · USt-IdNr.: DE323410650

— nachfolgend „Auftragsverarbeiter“ oder „Krafteq“ —

und dem im Angebot bezeichneten Kunden

— nachfolgend „Verantwortlicher“ —

— gemeinsam die „Parteien“ —

§ 1 Gegenstand, Rollen, Rangfolge

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen auf Grundlage des an ihn gerichteten Angebots nebst Anlagen sowie der darin bezeichneten Allgemeinen Geschäftsbedingungen der Krafteq GmbH (gemeinsam nachfolgend „Hauptvertrag“). Dabei verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien nach Art. 28 DSGVO.

(1a) **Zustandekommen.** Diese Vereinbarung ist Bestandteil des Hauptvertrags und kommt mit dessen Abschluss zustande — also mit der Annahme des Angebots durch den Verantwortlichen in Textform. Eine gesonderte Unterzeichnung ist nicht erforderlich: Art. 28 Abs. 9 DSGVO lässt für diese Vereinbarung ausdrücklich ein elektronisches Format genügen. Der Verantwortliche kann jederzeit eine von Krafteq unterzeichnete Ausfertigung verlangen; Krafteq stellt sie unverzüglich und ohne Kosten bereit.

(1b) **Fassung.** Maßgeblich ist die im Angebot bezeichnete Fassung dieser Vereinbarung. Jede veröffentlichte Fassung bleibt unter einer datierten Adresse unverändert abrufbar.

(2) Der Verantwortliche ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein entscheidet über Zwecke und Mittel der Verarbeitung und über die Rechtmäßigkeit der Datenerhebung. Der Auftragsverarbeiter ist Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO.

(3) Diese Vereinbarung gilt nur, soweit der Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen hat. Im Selbstbetrieb und im Offline-Betrieb (§§ 11, 12 AGB) findet keine Auftragsverarbeitung statt; wird der Auftragsverarbeiter dort im Einzelfall unterstützend tätig und erhält dabei Zugriff, gilt diese Vereinbarung für diesen Einzelfall entsprechend.

(4) Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag geht in datenschutzrechtlichen Fragen diese Vereinbarung vor.

§ 2 Gegenstand, Art, Zweck und Dauer der Verarbeitung

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

(2) Die Verarbeitung findet ausschließlich in Mitgliedstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verlagerung in ein Drittland erfolgt nur unter den Voraussetzungen des § 9.

(3) Die Vereinbarung beginnt mit ihrem Abschluss und läuft, solange der Auftragsverarbeiter für den Verantwortlichen personenbezogene Daten verarbeitet, längstens bis zum Ende des Hauptvertrags zuzüglich der Fristen nach § 11.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. In einem solchen Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Weisungen erfolgen in Textform. Der Hauptvertrag einschließlich Anlage 1 stellt die Erstweisung dar. Mündlich erteilte Weisungen bestätigt der Verantwortliche unverzüglich in Textform.

(3) **Weisungsberechtigt** auf Seiten des Verantwortlichen ist die im Hauptvertrag benannte Ansprechperson sowie jede Person, die der Verantwortliche Krafteq gegenüber in Textform als weisungsberechtigt benennt. **Weisungsempfänger** auf Seiten des Auftragsverarbeiters ist

Ivan Bianco, Geschäftsführer, ivan@krafteq.de.

(4) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er ist berechtigt, die Ausführung der Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

(5) Der Auftragsverarbeiter verwendet die Daten nicht für eigene Zwecke. Eine Nutzung zu Zwecken der Produktverbesserung, des Trainings von Modellen oder der Analyse über den Auftrag hinaus findet nicht statt.

§ 4 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit.** Der Auftragsverarbeiter setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

(2) **Sicherheit der Verarbeitung.** Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Der bei Vertragsschluss vereinbarte Stand ist in **Anlage 2** beschrieben. Der Auftragsverarbeiter darf die Maßnahmen fortentwickeln; das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen auf Anfrage mit.

(3) **Unterstützung.** Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen des Zumutbaren und unter Berücksichtigung der Art der Verarbeitung sowie der ihm zur Verfügung stehenden Informationen bei

1. der Beantwortung von Anträgen betroffener Personen (§ 6),
2. der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei der Meldung von Datenschutzverletzungen (§ 7), bei Datenschutz-Folgenabschätzungen und bei vorherigen

Konsultationen der Aufsichtsbehörde (Art. 28 Abs. 3 lit. e und f DSGVO).

(4) **Berichtigung, Löschung, Einschränkung.** Der Auftragsverarbeiter berichtigt, löscht oder schränkt die Verarbeitung personenbezogener Daten nur auf Weisung des Verantwortlichen ein. Soweit eine betroffene Person sich unmittelbar an den Auftragsverarbeiter wendet, leitet er das Anliegen unverzüglich an den Verantwortlichen weiter.

(5) **Datenschutzbeauftragter.** Eine Pflicht zur Benennung nach Art. 37 DSGVO, § 38 BDSG besteht beim Auftragsverarbeiter derzeit nicht; die Schwelle von 20 ständig mit automatisierter Verarbeitung beschäftigten Personen ist nicht erreicht. Ansprechpartner für den Datenschutz ist Ivan Bianco, Geschäftsführer, ivan@krafteq.de. Entsteht die Benennungspflicht, teilt der Auftragsverarbeiter dem Verantwortlichen den Datenschutzbeauftragten unaufgefordert mit.

(6) **Ort der Verarbeitung.** Die Verarbeitung erfolgt an den in Anlage 3 bezeichneten Verarbeitungsorten.

§ 5 Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich. Er stellt sicher, dass für die Übermittlung der Daten an den Auftragsverarbeiter und für deren Verarbeitung eine Rechtsgrundlage besteht.

(2) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er bei der Prüfung der Ergebnisse Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen feststellt.

(3) Führt der Verantwortliche mehrere rechtlich eigenständige Firmen in einer Instanz, ist er dafür verantwortlich, für eine firmenübergreifende Verarbeitung eine tragfähige Rechtsgrundlage zu schaffen. Das Produkt stellt die Steuerbarkeit der Trennung bereit, nicht die Rechtsgrundlage (§ 26 Abs. 3 AGB).

(4) Der Verantwortliche verwaltet die Zugänge seiner Beschäftigten und deren Berechtigungen. Er sorgt dafür, dass ausscheidende Personen unverzüglich gesperrt werden.

§ 6 Betroffenenrechte

(1) Wendet sich eine betroffene Person mit einem Antrag auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit oder Widerspruch an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an den Verantwortlichen weiter und beantwortet ihn nicht selbst.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung nachzukommen — insbesondere durch die im Produkt vorhandenen Auskunfts-, Export-, Berichtigungs- und Löschfunktionen.

(3) Ein über die Nutzung dieser Funktionen hinausgehender Aufwand wird nach vorheriger Abstimmung nach Aufwand vergütet, soweit der Auftragsverarbeiter den Anlass nicht zu vertreten hat.

§ 7 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten **unverzüglich, spätestens innerhalb von 24 Stunden** nach Kenntniserlangung (Art. 33 Abs. 2 DSGVO).

(2) Die Meldung enthält, soweit verfügbar: eine Beschreibung der Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen. Sind nicht alle Angaben sofort verfügbar, erfolgt die Meldung schrittweise.

(3) Meldungen an die Aufsichtsbehörde nach Art. 33 DSGVO und Benachrichtigungen betroffener Personen nach Art. 34 DSGVO obliegen dem Verantwortlichen.

(4) **Meldeweg.** Die Meldung erfolgt an die im Hauptvertrag benannte Ansprechperson des Verantwortlichen, ersatzweise an dessen allgemeine geschäftliche E-Mail-Adresse. Der Verantwortliche kann Krafteq in Textform eine abweichende Meldeadresse benennen.

§ 8 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die **allgemeine schriftliche Genehmigung** zur Hinzuziehung weiterer Auftragsverarbeiter nach Art. 28 Abs. 2 Satz 2 DSGVO. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in **Anlage 3** benannt und damit genehmigt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen **mindestens 30 Tage im Voraus** in Textform über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter. Der Verantwortliche kann einer Änderung innerhalb von 14 Tagen ab Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen.

(3) Widerspricht der Verantwortliche, suchen die Parteien eine einvernehmliche Lösung. Kommt eine solche nicht zustande und kann der Auftragsverarbeiter die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht in zumutbarer Weise erbringen, kann jede Partei den betroffenen Leistungsteil mit einer Frist von einem Monat kündigen. Bereits im Voraus vergütete Leistungen erstattet der Auftragsverarbeiter anteilig.

(4) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in dieser Vereinbarung festgelegt sind (Art. 28 Abs. 4 DSGVO). Er bleibt dem Verantwortlichen gegenüber für die Einhaltung verantwortlich.

(5) Keine Unterauftragsverarbeitung im Sinne dieser Vorschrift sind Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt und die die Verarbeitung personenbezogener Daten nicht zum Gegenstand haben (etwa Telekommunikationsleistungen oder Reinigungsdienste).

§ 9 Verarbeitung in Drittländern

(1) Die Verarbeitung findet ausschließlich in der Europäischen Union statt. Sämtliche in Anlage 3 benannten Unterauftragsverarbeiter verarbeiten die Daten an Standorten innerhalb der EU; administrative Zugriffe durch Beschäftigte des Auftragsverarbeiters erfolgen ausschließlich aus dem EU-/EWR-Gebiet.

(2) Eine Verarbeitung außerhalb der EU beziehungsweise des EWR findet nur statt, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind — insbesondere auf Grundlage eines Angemessenheitsbeschlusses nach Art. 45 DSGVO oder von Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO nebst der erforderlichen Zusatzmaßnahmen. Der Auftragsverarbeiter weist dies auf Verlangen nach.

§ 10 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen (Art. 28 Abs. 3 lit. h DSGVO).

(2) Der Nachweis kann geführt werden durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Stellen, eine geeignete Zertifizierung, eine Selbstauskunft anhand eines Fragebogens oder die Vorlage der Dokumentation der Maßnahmen nach Anlage 2.

(3) Reichen diese Nachweise im Einzelfall nicht aus, kann der Verantwortliche nach Ankündigung mit angemessener Frist — in der Regel **20 Werktage** — während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs eine Überprüfung vornehmen oder durch einen zur Verschwiegenheit verpflichteten, nicht mit dem Auftragsverarbeiter im Wettbewerb stehenden Prüfer vornehmen lassen. Die Überprüfung findet höchstens **einmal je Kalenderjahr** statt; dies gilt nicht bei einem konkreten Anlass, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten oder auf Anordnung einer Aufsichtsbehörde.

(4) Der Auftragsverarbeiter kann für einen über Absatz 2 hinausgehenden Prüfungsaufwand eine angemessene Vergütung verlangen, sofern er den Anlass der Prüfung nicht zu vertreten hat.

§ 11 Löschung und Rückgabe nach Beendigung

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Der Verantwortliche kann seine Daten jederzeit und ohne gesondertes Entgelt in gängigen, maschinenlesbaren Formaten exportieren. Nach Wirksamwerden einer Kündigung stellt der Auftragsverarbeiter den Export für **30 Tage** bereit (§ 16 AGB).

(3) Nach Ablauf dieser Frist löscht der Auftragsverarbeiter die Daten des Verantwortlichen einschließlich der Sicherungskopien. Sicherungskopien werden im Rahmen des regulären Sicherungszyklus überschrieben; die Vorhaltezeit beträgt sieben Tage.

(4) Auf Wunsch bestätigt der Auftragsverarbeiter die Löschung in Textform.

§ 12 Haftung

- (1) Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrags, insbesondere § 24 AGB.
- (2) Art. 82 DSGVO bleibt unberührt.

§ 13 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.
- (2) Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem wirtschaftlichen Zweck am nächsten kommt.
- (3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist Köln, sofern der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.
- (4) Die Anlagen 1 bis 3 sind Bestandteil dieser Vereinbarung.

§ 14 Nachweis des Abschlusses

Der Abschluss dieser Vereinbarung ergibt sich aus dem Abschluss des Hauptvertrags. Krafteq dokumentiert Fassung und Zeitpunkt und legt beides auf Verlangen vor. Verlangt der Verantwortliche eine unterzeichnete Ausfertigung — etwa weil seine eigene Dokumentationspflicht das vorsieht —, genügt eine Mitteilung in Textform.

Anlage 1 — Gegenstand, Art, Zweck, Daten, Betroffene

Gegenstand der Verarbeitung Bereitstellung, Betrieb und Wartung der Betriebssoftware krafteq Handwerk als Instanz des Verantwortlichen, einschließlich Einrichtung, Datenmigration aus Altsystemen, Support und der im Angebot vereinbarten Anpassungen. Eingeschlossen ist die zentrale Benutzerverwaltung des Auftragsverarbeiters (Krafteq-Portal / IAM), über die Benutzerkonten und Anmeldungen laufen.

Art der Verarbeitung Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln (E-Mail-Versand aus dem System), Löschen und Vernichten — jeweils im Rahmen des Softwarebetriebs.

Zweck der Verarbeitung Abwicklung der Geschäftsprozesse des Verantwortlichen: Auftragsbearbeitung, Angebots- und Rechnungsstellung, elektronische Rechnungsstellung, Korrespondenz, Terminplanung, Zeiterfassung, Belegverwaltung und Auswertungen.

Kategorien betroffener Personen

- Beschäftigte des Verantwortlichen (einschließlich Arbeitszeiten, Abwesenheiten, Einsatzplanung) - Kundinnen und Kunden des Verantwortlichen, auch Privatpersonen
- Ansprechpartner bei Geschäftskunden, Lieferanten, Netzbetreibern, Zertifizierungsstellen und Behörden
- Interessenten und sonstige Korrespondenzpartner

Arten personenbezogener Daten

- Stammdaten: Name, Anschrift, Kundennummer, Rechtsform
- Kontaktdaten: Telefon, Mobilfunk, E-Mail-Adresse
- Vertrags- und Vorgangsdaten: Angebote, Auftragsbestätigungen, Rechnungen, Zahlungsstatus, Vorgangsstände, Fristen, Notizen
- Kommunikationsdaten: ein- und ausgehende E-Mails samt Anhängen, Gesprächsnotizen
- Bank- und Zahlungsdaten, soweit für Rechnungsstellung und Zahlungsabgleich erfasst
- Beschäftigtendaten: Arbeitszeitmodelle, erfasste Zeiten, Abwesenheiten mit Genehmigungsstatus, Rolle und Berechtigungen
- Bild- und Unterschriftsdaten: erfasste Unterschriften, Fotos zu Vorgängen
- Anlagen- und Objektdaten mit Personenbezug (Anschrift der Anlage, Anlagenbetreiber)
- Benutzerkonten der Beschäftigten des Verantwortlichen in der zentralen Benutzerverwaltung (Name, dienstliche E-Mail-Adresse, Rolle, Anmeldedaten)
- Zugangsdaten zu den vom Verantwortlichen angebundenen E-Mail-Postfächern
- Protokolldaten des Systems (Zugriffszeitpunkte, Benutzerkennung, IP-Adresse)

E-Mail-Versand Die Geschäftskorrespondenz des Verantwortlichen wird ausschließlich über das von ihm angebundene eigene Postfach versendet und empfangen; ein Versanddienst des Auftragsverarbeiters ist daran nicht beteiligt. Gleiches gilt für System-Nachrichten der Anwendung (etwa Einladung, Kennwortzurücksetzung, Benachrichtigung), soweit im Angebot nicht ausdrücklich ein gesonderter Versanddienst vereinbart und in Anlage 3 benannt ist.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) Sind nicht Gegenstand des Auftrags. Der Verantwortliche wird angehalten, solche Daten nicht in Freitextfeldern zu erfassen. Werden Abwesenheiten aus Krankheitsgründen erfasst, beschränkt sich dies auf die Tatsache der Abwesenheit ohne Angabe von Diagnosen oder Gesundheitsdaten.

Dauer Für die Laufzeit des Hauptvertrags zuzüglich der Fristen nach § 11 dieser Vereinbarung.

Anlage 2 — Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

> Stand: 3. September 2026. Der Auftragsverarbeiter entwickelt die Maßnahmen fort; das Schutzniveau
> wird dabei nicht unterschritten (§ 4 Abs. 2).

1 · Vertraulichkeit

Zutrittskontrolle (physisch) Der Betrieb erfolgt in Rechenzentren der in Anlage 3 benannten Infrastrukturanbieter innerhalb der Europäischen Union. Für die physische Sicherheit gelten deren Maßnahmen und Zertifizierungen. Eigene Serverräume unterhält der Auftragsverarbeiter nicht. Der Auftragsverarbeiter selbst ist nicht nach ISO/IEC 27001 zertifiziert und behauptet dies nicht.

Zugangskontrolle (Systeme)

- Persönliche, nicht geteilte Benutzerkonten für alle administrativen Zugänge
- Zwei-Faktor-Authentisierung ist für administrative Zugänge verpflichtend
- Administrative Zugriffe erfolgen ausschließlich über Bastion-Hosts und verschlüsselte Verbindungen - Der Kreis der administrativ berechtigten Personen ist auf Senior Engineers beschränkt
- Die Anwendung selbst speichert keine Kennwörter: Anmeldung und Benutzerverwaltung laufen über die zentrale Benutzerverwaltung des Auftragsverarbeiters, die Anmeldeverfahren einschließlich Mehr-Faktor-Authentisierung bereitstellt
- Betriebsgeheimnisse (Schlüssel, Zugangsdaten) werden in einem Secret-Management-System vorgehalten und nicht im Quellcode abgelegt
- Automatische Sitzungsbeendigung nach Inaktivität

Zugriffskontrolle (Daten)

- Rollen- und Rechtssystem in der Anwendung; Zugriff nach dem Prinzip der geringsten Rechte - Administrativer Zugriff durch Beschäftigte des Auftragsverarbeiters nur, soweit für Betrieb, Fehlerbehebung oder Support erforderlich
- Administrative Zugriffe werden protokolliert

Trennungskontrolle Jeder Verantwortliche erhält eine eigene Instanz mit **eigener Datenbank, eigenen Containern und einem eigenen Mandanten in der zentralen Benutzerverwaltung**. Test-, Entwicklungs- und Vorführungsumgebungen sind von der Produktivumgebung getrennt und enthalten **keine Produktivdaten**; dort werden ausschließlich synthetische Datensätze verwendet.

Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung nach dem Stand der Technik (TLS 1.2 oder höher) für alle Verbindungen - Verschlüsselung der Datenträger im Ruhezustand auf Ebene der Infrastrukturanbieter
- Zugangsdaten zu angebundenen E-Mail-Postfächern werden zusätzlich auf Anwendungsebene mit **AES-256-GCM** verschlüsselt gespeichert
- Datensicherungen werden verschlüsselt abgelegt

2 · Integrität

Eingabekontrolle Änderungen an Vorgängen, Dokumenten und Stammdaten werden mit Zeitstempel und Benutzerkennung protokolliert. Rechnungen und Dokumente mit Nummernkreis sind nach Festschreibung nicht mehr veränderbar; Korrekturen erfolgen über Storno und Neuausstellung.

Weitergabekontrolle Datenübertragungen erfolgen ausschließlich verschlüsselt. Ein Datenträgertransport findet nicht statt. Der Datenexport erfolgt über die Anwendung an authentifizierte Nutzer.

3 · Verfügbarkeit und Belastbarkeit

- Automatisierte tägliche Sicherung mit einer Vorhaltezeit von sieben Tagen; längere Vorhaltung auf Wunsch gegen gesonderte Vergütung
- Sicherungen werden **getrennt von den Produktivsystemen** und verschlüsselt abgelegt
- Die Wiederherstellbarkeit der Sicherungen wird überprüft
- Verfügbarkeits- und Fehlerüberwachung; die Überwachung wird auf eigener Infrastruktur des Auftragsverarbeiters betrieben
- Zeitnahes Einspielen von Sicherheitsaktualisierungen für Betriebssystem, Container-Abbilder, Rahmenwerke und Abhängigkeiten
- Jedes Container-Abbild wird vor der Auslieferung automatisiert auf bekannte Schwachstellen geprüft

4 · Verfahren zur regelmäßigen Überprüfung

- Datenschutz-Management: Prüfung dieser Vereinbarung und ihrer Anlagen mindestens jährlich sowie anlassbezogen
- Verpflichtung aller Beschäftigten auf Vertraulichkeit vor Aufnahme der Tätigkeit
- Auftragskontrolle: Unterauftragsverarbeiter werden vor Einsatz geprüft und vertraglich nach Art. 28 Abs. 4 DSGVO gebunden
- Verfahren zur Erkennung, Meldung und Behandlung von Datenschutzverletzungen nach § 7
- Änderungen an der Produktivumgebung erfolgen nachvollziehbar über ein versioniertes Verfahren

Anlage 3 — Unterauftragsverarbeiter und Verarbeitungsorte

Die folgenden Unterauftragsverarbeiter sind nach § 8 Abs. 1 genehmigt:

Unternehmen	Anschrift	Leistung	Verarbeitungsort	Status
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Deutschland	Server- und Speicherinfrastruktur, Ablage der Datensicherungen	Deutschland	im Einsatz
OVH GmbH	Christophstraße 19, 50670 Köln, Deutschland	Server- und Speicherinfrastruktur, Ablage der Datensicherungen	Europäische Union	genehmigt, derzeit nicht im Einsatz

Die Spalte **Status** benennt, wer die Daten des Verantwortlichen tatsächlich verarbeitet. Ein mit „genehmigt, derzeit nicht im Einsatz“ bezeichneter Anbieter hält zum Zeitpunkt des Vertragsschlusses keine Daten des Verantwortlichen; die Genehmigung nach § 8 Abs. 1 erstreckt sich bereits auf ihn, damit ein späterer Wechsel oder ein Ausweichbetrieb keine gesonderte Zustimmung erfordert. Der Auftragsverarbeiter teilt die Aufnahme des Einsatzes nach § 8 Abs. 2 mit.

Mit beiden Anbietern bestehen abgeschlossene Vereinbarungen zur Auftragsverarbeitung nach Art. 28 DSGVO, die ihnen dieselben Datenschutzpflichten auferlegen wie diese Vereinbarung dem Auftragsverarbeiter (§ 8 Abs. 4):

- Hetzner Online GmbH — Auftragsverarbeitungsvertrag Version 1.2 (Stand 16.02.2026), abgeschlossen am 04.09.2026
- OVH GmbH — Auftragsverarbeitungsvertrag Version 8.0 vom 17.10.2025

Auf Wunsch legt der Auftragsverarbeiter dem Verantwortlichen beide Vereinbarungen vor.

E-Mail-Versand: Für den produktiven Betrieb wird kein Versanddienst eines Dritten eingesetzt. Ein- und ausgehende Nachrichten laufen über das vom Verantwortlichen angebundene eigene Postfach. Wird für System-Nachrichten ausnahmsweise ein gesonderter Versanddienst eingesetzt, ist er hier zu benennen, bevor er in Betrieb geht.

Keine Unterauftragsverarbeiter sind:

- Die Verfügbarkeits- und Fehlerüberwachung — sie wird auf eigener Infrastruktur des

Auftragsverarbeiters betrieben, ein externer Dienst wird dafür nicht eingesetzt.

- Die zentrale Benutzerverwaltung (Krafteq-Portal / IAM) — sie ist eine eigene Komponente des Auftragsverarbeiters und läuft auf derselben Infrastruktur.

Verarbeitungsorte des Auftragsverarbeiters Administrative Zugriffe durch Beschäftigte des Auftragsverarbeiters erfolgen ausschließlich aus dem Gebiet der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums.

Abweichung für Test- und Vorführinstanzen Wird diese Vereinbarung für eine Testphase nach § 3 Abs. 3 AGB geschlossen und werden dabei personenbezogene Daten verarbeitet, ist zu prüfen, ob der Versand von System-Nachrichten dort über einen Dienst eines Dritten läuft. Ist das der Fall, muss dieser Dienst **vor** Aufnahme der Testphase in diese Anlage aufgenommen werden — mit Anschrift, Leistung, Verarbeitungsort und der Rechtsgrundlage einer etwaigen Drittlandübermittlung. Eine Testinstanz, in der ein echtes Postfach angebunden wird, verarbeitet reale personenbezogene Daten und ist insoweit nicht anders zu behandeln als ein produktiver Betrieb.

Stand dieser Anlage: 4. September 2026

Stand: 4. September 2026