

Vertrag über die Auftragsverarbeitung - TriKoReg

Fassung 1.0 · Stand 15.08.2026

§ 1 Vertragsparteien und Gegenstand

(1) Dieser Vertrag wird zwischen dem Unternehmen, das sich für die Nutzung der Anwendung „TriKoReg“ registriert hat (nachfolgend „der Verantwortliche“), und TriMo (nachfolgend „der Auftragsverarbeiter“) geschlossen.

(2) Er konkretisiert die Pflichten aus Artikel 28 der Datenschutz-Grundverordnung für die Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter im Rahmen des Nutzungsvertrags im Auftrag des Verantwortlichen durchführt.

(3) Gegenstand der Verarbeitung ist das Bereitstellen und Betreiben der Anwendung: das Speichern, Anzeigen, Berechnen und Ausgeben der vom Verantwortlichen eingegebenen Daten sowie das Erzeugen der Dokumente nach der Verordnung über die Erteilung der Fahrberechtigung an Triebfahrzeugführer (TfV).

(4) Der Vertrag kommt mit der Registrierung zustande und ist Bestandteil des Nutzungsvertrags. Er wird in elektronischer Form geschlossen; Artikel 28 Absatz 9 DSGVO lässt das ausdrücklich zu. Der Auftragsverarbeiter speichert die Fassungsnummer und den Zeitpunkt der Zustimmung.

(5) Dauer: Der Vertrag läuft, solange der Nutzungsvertrag läuft. Er endet mit diesem, jedoch nicht vor der vollständigen Rückgabe oder Löschung der Daten nach § 9.

§ 2 Art und Zweck der Verarbeitung, Daten, Betroffene

(1) Art der Verarbeitung: Erheben, Erfassen, Organisieren, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln an den Verantwortlichen selbst, Einschränken, Löschen und Vernichten.

(2) Zweck: ausschließlich die Erfüllung der Pflichten des Verantwortlichen aus der TfV – insbesondere die Prüfung der Voraussetzungen nach § 5 Absatz 2, die Ausstellung und Änderung von Zusatzbescheinigungen nach §§ 9 und 11, die Führung des Registers nach § 10 Absatz 4 und die Überwachung der Fristen nach Anlage 11. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters findet nicht statt.

(3) Art der Daten: Stammdaten der Triebfahrzeugführer (Name, Vorname, Geburtsdatum, Geburtsort und -land, Staatsangehörigkeit, Anschrift, Lichtbild, Unterschrift), Beschäftigungsdaten (Personalnummer, Arbeitsort, Beschäftigungszeitraum), Angaben zum Triebfahrzeugführerschein, Befähigungen für Fahrzeuge und Infrastruktur, Sprachkenntnisse, firmenspezifische Anforderungen, hochgeladene Nachweisdokumente sowie Nutzerkontodaten der Beschäftigten des Verantwortlichen.

(4) Besondere Kategorien nach Artikel 9 DSGVO: Die Verarbeitung umfasst Gesundheitsdaten – das Ergebnis der ärztlichen Untersuchung nach Anlage 4 TfV, das Ergebnis der psychologischen Untersuchung, die Fälligkeit der nächsten Untersuchung sowie Einschränkungen des Leistungsvermögens nach Anlage 2 Nummer 6. Beide Parteien treffen dafür die zusätzlichen Maßnahmen nach Anlage 1; die Zulässigkeit richtet sich nach Artikel 9 Absatz 2 Buchstabe b DSGVO in Verbindung mit § 26 Absatz 3 BDSG.

(5) Kategorien betroffener Personen: Triebfahrzeugführer des Verantwortlichen, Bewerber, ausgeschiedene Beschäftigte innerhalb der Aufbewahrungsfrist nach § 10 Absatz 8 TfV sowie

die Beschäftigten des Verantwortlichen, die mit der Anwendung arbeiten.

§ 3 Weisungsbindung

(1) Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, auch hinsichtlich der Übermittlung in ein Drittland (Artikel 28 Absatz 3 Satz 2 Buchstabe a DSGVO). Eine Ausnahme gilt nur, soweit das Unionsrecht oder das Recht eines Mitgliedstaats ihn zur Verarbeitung verpflichtet; in diesem Fall unterrichtet er den Verantwortlichen vorher, sofern das Recht dies nicht verbietet.

(2) Die Bedienung der Anwendung durch den Verantwortlichen ist die Weisung. Was er eingibt, exportiert, ausstellt oder löscht, gilt als erteilte Weisung; einer gesonderten Erklärung bedarf es dafür nicht. Weisungen darüber hinaus ergehen in Textform an die im Impressum genannte Anschrift.

(3) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, so teilt er dies unverzüglich mit (Artikel 28 Absatz 3 Satz 3 DSGVO). Er darf die Ausführung aussetzen, bis der Verantwortliche die Weisung bestätigt oder ändert.

(4) Der Auftragsverarbeiter greift auf die Daten eines Mandanten nur zu, soweit es zur Fehlersuche, zur Wiederherstellung nach einer Störung oder zur Erfüllung einer Weisung erforderlich ist. Jeder solche Zugriff wird protokolliert und dem Verantwortlichen auf Verlangen offengelegt.

§ 4 Vertraulichkeit

(1) Der Auftragsverarbeiter setzt zur Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Artikel 28 Absatz 3 Satz 2 Buchstabe b DSGVO). Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus.

(2) Er stellt sicher, dass diese Personen die Daten nur auf Weisung verarbeiten, und macht sie mit den für sie geltenden Pflichten vertraut.

§ 5 Sicherheit der Verarbeitung

(1) Der Auftragsverarbeiter trifft die nach Artikel 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Sie sind in Anlage 1 beschrieben; Anlage 1 ist Bestandteil dieses Vertrags.

(2) Die Maßnahmen dürfen weiterentwickelt werden, solange das Schutzniveau nicht unterschritten wird. Eine wesentliche Änderung wird dem Verantwortlichen mitgeteilt.

(3) Anlage 1 benennt ausdrücklich auch die Grenzen der getroffenen Maßnahmen. Der Verantwortliche trifft seine Risikoabwägung nach Artikel 32 Absatz 1 auf dieser Grundlage.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt hiermit seine Zustimmung zum Einsatz der in Anlage 2 namentlich genannten Unterauftragsverarbeiter (Artikel 28 Absatz 2 DSGVO). Weitere setzt der Auftragsverarbeiter nicht ein.

(2) Beabsichtigt der Auftragsverarbeiter, einen Unterauftragsverarbeiter hinzuzuziehen oder auszutauschen, so teilt er dies mindestens sechs Wochen vorher in Textform mit. Der Verantwortliche kann innerhalb dieser Frist Widerspruch einlegen. Widerspricht er aus einem sachlichen Grund, so kann jede Partei den Nutzungsvertrag zum Zeitpunkt der geplanten Änderung kündigen.

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter dieselben Datenschutzpflichten auf, die ihn selbst nach diesem Vertrag treffen (Artikel 28 Absatz 4

DSGVO). Er haftet dem Verantwortlichen gegenüber für deren Verhalten wie für eigenes.

(4) Der in Anlage 2 als bedingt gekennzeichnete Unterauftragsverarbeiter verarbeitet Daten ausschließlich dann, wenn eine Bearbeiterin oder ein Bearbeiter die Texterkennung für ein einzelnes Dokument auslöst. Wird die Funktion nicht benutzt, findet keine Übermittlung statt.

(5) Nicht als Unterauftragsverarbeitung gilt die Inanspruchnahme von Telekommunikations-, Post-, Wartungs- oder Prüfleistungen, bei denen ein Zugriff auf Personendaten nicht Gegenstand, sondern allenfalls nicht ausschließbare Nebenfolge ist.

§ 7 Unterstützung bei den Rechten betroffener Personen

(1) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, so leitet er das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen nach Kapitel III DSGVO nachzukommen – Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Artikel 28 Absatz 3 Satz 2 Buchstabe e DSGVO).

(3) Die Anwendung stellt dafür bereit: die vollständige Akte einer betroffenen Person als PDF und als Archiv, die Bearbeitung und Löschung einzelner Angaben sowie ein Protokoll darüber, wer wann welche Personendaten ausgeleitet hat.

(4) Für Daten der Nutzerkonten – Name, Telefonnummer, E-Mail-Adresse, Anmeldeprotokolle – ist der Auftragsverarbeiter selbst Verantwortlicher; Anträge dazu richten die Betroffenen unmittelbar an ihn.

§ 8 Unterstützung bei den Pflichten aus Art. 32 bis 36

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus den Artikeln 32 bis 36 DSGVO, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen (Artikel 28 Absatz 3 Satz 2 Buchstabe f DSGVO).

(2) Verletzung des Schutzes personenbezogener Daten: Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis (Artikel 33 Absatz 2 DSGVO). Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien, ungefähre Zahl der Betroffenen, wahrscheinliche Folgen und getroffene Gegenmaßnahmen. Die Fristen des Artikels 33 Absatz 1 gegenüber der Aufsichtsbehörde laufen für den Verantwortlichen; die kurze Meldefrist soll ihm die Einhaltung ermöglichen.

(3) Datenschutz-Folgenabschätzung: Verarbeitet der Verantwortliche Gesundheitsdaten in größerem Umfang, kann eine Abschätzung nach Artikel 35 DSGVO erforderlich sein. Der Auftragsverarbeiter stellt dafür die Beschreibung der Verarbeitungsvorgänge und der Maßnahmen nach Anlage 1 zur Verfügung. Die Abschätzung selbst obliegt dem Verantwortlichen.

§ 9 Rückgabe und Löschung nach Ende des Vertrags

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter alle personenbezogenen Daten oder gibt sie zurück, nach Wahl des Verantwortlichen; vorhandene Kopien werden gelöscht, soweit keine Rechtsvorschrift ihre Aufbewahrung verlangt (Artikel 28 Absatz 3 Satz 2 Buchstabe g DSGVO).

(2) Der Verantwortliche teilt seine Wahl innerhalb von 30 Tagen nach Vertragsende mit. Trifft er keine Wahl, werden die Daten nach Ablauf dieser Frist zur Rückgabe bereitgestellt und anschließend gelöscht.

(3) Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format. Der Auftragsverarbeiter stellt die vollständigen Akten aller Triebfahrzeugführer samt hochgeladener Nachweise bereit.

(4) Datensicherungen werden nicht gesondert gelöscht, sondern altern nach ihrem Aufbewahrungsplan aus: Vollarchive nach 12 Monaten. Bis dahin dienen sie ausschließlich der Wiederherstellung nach einem Ausfall und werden nicht ausgewertet.

(5) § 10 Absatz 8 TfV bleibt unberührt. Der Verantwortliche ist verpflichtet, die Daten einer Zusatzbescheinigung zehn Jahre nach ihrem Ungültigwerden aufzubewahren und danach zu löschen. Eine vorzeitige Löschung durch den Auftragsverarbeiter kommt nicht in Betracht; die Wahl nach Absatz 1 trifft der Verantwortliche in eigener Verantwortung.

§ 10 Nachweise und Überprüfungen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Artikel 28 DSGVO erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen (Artikel 28 Absatz 3 Satz 2 Buchstabe h DSGVO).

(2) Eine Überprüfung wird mit einer Frist von vier Wochen in Textform angekündigt, findet zu den üblichen Geschäftszeiten statt und stört den Betrieb nicht unangemessen. Sie darf einmal je Kalenderjahr verlangt werden; bei einem konkreten Anlass – insbesondere nach einer Meldung nach § 8 – auch häufiger.

(3) Der Nachweis kann auch durch die Vorlage eines aktuellen Berichts einer unabhängigen Stelle oder einer geeigneten Zertifizierung geführt werden, soweit dieser die Prüfgegenstände abdeckt.

(4) Der Auftragsverarbeiter führt ein Verzeichnis aller Verarbeitungstätigkeiten, die er im Auftrag durchführt (Artikel 30 Absatz 2 DSGVO), und legt es dem Verantwortlichen auf Verlangen vor.

§ 11 Verantwortlichkeit und Haftung

(1) Der Verantwortliche ist für die Zulässigkeit der Verarbeitung und für die Wahrung der Rechte betroffener Personen verantwortlich (Artikel 24 DSGVO). Er beurteilt insbesondere, ob eine Angabe erforderlich ist, ob eine Löschfrist greift und ob eine Datenschutz-Folgenabschätzung nötig ist.

(2) Die Haftung im Verhältnis der Parteien richtet sich nach § 10 des Nutzungsvertrags. Artikel 82 DSGVO bleibt unberührt; die Außenhaftung gegenüber betroffenen Personen kann durch diesen Vertrag nicht beschränkt werden.

(3) Verarbeitet der Auftragsverarbeiter Daten unter Verstoß gegen diesen Vertrag zu eigenen Zwecken oder bestimmt er selbst über Zwecke und Mittel, so gilt er insoweit als Verantwortlicher (Artikel 28 Absatz 10 DSGVO).

§ 12 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem Vertrag und dem Nutzungsvertrag geht dieser Vertrag vor, soweit es um die Verarbeitung personenbezogener Daten geht.

(2) Änderungen und Ergänzungen bedürfen der Textform. Jede Fassung trägt eine eigene Nummer; der Auftragsverarbeiter speichert, welcher Fassung ein Verantwortlicher zugestimmt hat.

(3) Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

(4) Es gilt das Recht der Bundesrepublik Deutschland.

Anlage 1 Technische und organisatorische Maßnahmen (Art. 32)

Vertraulichkeit – Zutritt und Zugang. Die Anwendung läuft in einem Rechenzentrum von Hetzner Online GmbH, Deutschland. Der Zutritt zu den Servern unterliegt den dortigen Maßnahmen. Ein Zugang zur Anwendung besteht nur über ein persönliches Konto mit E-Mail-Adresse und Passwort; Sammelkonten sind nicht vorgesehen. Passwörter werden nie im Klartext gespeichert, sondern als bcrypt-Hash mit Kostenfaktor 12. Das Sitzungstoken liegt nur als SHA-256 in der Datenbank; im Klartext existiert es ausschließlich im Cookie des Browsers.

Vertraulichkeit – Zugriff. Drei Rollen (Leser, Bearbeiter, Administrator) begrenzen, was ein Konto tun darf. Eine Sitzung endet spätestens nach 12 Stunden, unabhängig von der Aktivität. Nach 5 Fehlanmeldungen wird ein Konto für 30 Minuten gesperrt; dieselbe Sperre greift je Absenderadresse.

Trennung. Die Daten verschiedener Verantwortlicher sind doppelt getrennt: durch zusammengesetzte Fremdschlüssel in der Datenbank, die eine Verknüpfung über die Mandantengrenze hinweg strukturell unmöglich machen, und durch einen Filter, der an jede Abfrage angehängt wird. Ein Konto des Auftragsverarbeiters kann sich zur Fehlersuche in genau einen Mandanten schalten; jeder Wechsel wird protokolliert.

Integrität – Übertragung. Der Zugriff erfolgt ausschließlich über TLS. Der vorgeschaltete Proxy erzwingt HTTPS, setzt eine Inhaltssicherheitsrichtlinie ohne fremde Quellen und begrenzt die Zahl der Anfragen je Absenderadresse. Formulare sind gegen Aufrufe von fremden Seiten abgesichert.

Integrität – Eingabe. Die Vorgänge des Registers nach § 10 Absatz 4 TfV sind durch einen Datenbank-Trigger gegen nachträgliche Änderung gesperrt. Eine Korrektur entsteht durch einen zusätzlichen Eintrag, nie durch Überschreiben. Jeder Export von Personendaten wird mit Konto, Zeitpunkt und Umfang protokolliert. Hochgeladene Dateien werden auf ihre Signatur geprüft und auf 50 MB je Datei begrenzt.

Verfügbarkeit. Die Datenbank wird stündlich gesichert, das Vollarchiv einschließlich der hochgeladenen Nachweise alle 48 Stunden. Einzelsicherungen werden 14 Tage vorgehalten, Vollarchive 12 Monate. Jedes Archiv trägt eine Prüfsumme und eine Anleitung zur Wiederherstellung. Die Archive liegen getrennt von den Arbeitsdaten.

Belastbarkeit und Löschung. Ein Aufräumlauf schließt und löscht Sitzungsdaten nach 7 Tagen und entfernt temporäre Dateien. Aus den Sicherungsschnappschüssen werden Sitzungsdaten vor dem Ablegen entfernt.

Was diese Maßnahmen NICHT umfassen. Diese Aufzählung ist vollständig und ausdrücklich: Die Datenbank liegt auf dem Server unverschlüsselt im Dateisystem; geschützt ist sie durch die Zugriffskontrolle des Betriebssystems, nicht durch Verschlüsselung des Inhalts. Eine Zwei-Faktor-Anmeldung gibt es nicht. Es gibt keine automatische Ausleitung an ein externes Protokollsystem und keine durchgehende Überwachung rund um die Uhr. Der Verantwortliche berücksichtigt dies bei seiner Abwägung nach Artikel 32 Absatz 1 DSGVO.

Anlage 2 Unterauftragsverarbeiter (Art. 28 Abs. 2)

Die folgenden Unterauftragsverarbeiter sind vom Verantwortlichen genehmigt. Ein Wechsel läuft über § 6 dieses Vertrags und führt zu einer neuen Fassungsnummer.

1. Hetzner Online GmbH

Sitz: Deutschland

Zweck: Betrieb der Server, auf denen die Anwendung und ihre Datenbank laufen, sowie Verwahrung der Datensicherungen

Grundlage: Auftragsverarbeitungsvertrag mit dem Anbieter; Verarbeitung ausschließlich innerhalb der Europäischen Union

2. Anthropic PBC (bedingt – nur bei Nutzung der Texterkennung)

Sitz: San Francisco, USA

Zweck: Auslesen der Feldwerte aus einem Dokument, das eine Bearbeiterin oder ein Bearbeiter für genau diesen Zweck hochlädt (Texterkennung)

Grundlage: Auftragsverarbeitungsvertrag einschließlich der Standardvertragsklauseln nach Art. 46 Abs. 2 Buchst. c DSGVO