

Datenschutzerklärung - TriKoReg

Stand 25.08.2026

1. Wer ist verantwortlich?

Für die Verarbeitung der Daten von Triebfahrzeugführern ist der Kunde verantwortlich, der die Anwendung nutzt (Art. 4 Nr. 7 DSGVO). Er entscheidet über Zwecke und Mittel.

TriMo betreibt die Anwendung als Auftragsverarbeiter nach Art. 28 DSGVO und verarbeitet diese Daten ausschließlich nach Weisung des Unternehmens. Beide schließen dazu mit der Registrierung einen Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO; er ist unter /avv abrufbar und benennt in Anlage 2 die Unterauftragsverarbeiter.

Für die Daten der Nutzerkonten – Name, Telefonnummer, E-Mail-Adresse, Anmeldeprotokolle – ist TriMo selbst verantwortlich.

Kontakt: siehe Impressum.

2. Welche Daten verarbeitet die Anwendung?

Zum Nutzerkonto: Vorname, Nachname, Telefonnummer, E-Mail-Adresse, Passwort (ausschließlich als bcrypt-Hash), Rolle, Zeitpunkt der letzten Anmeldung, Zahl der Fehlversuche.

Zum Kunden: Firmenname, Art des Unternehmens, Sitz, Name und dienstliche Kontaktdaten des fachlichen Ansprechpartners, Fassung und Zeitpunkt der Zustimmung zum Nutzungsvertrag und zum Vertrag über die Auftragsverarbeitung.

Zu Triebfahrzeugführern: Name, Vorname, Geburtsdatum, Geburtsort und -land, Staatsangehörigkeit, Anschrift, Personalnummer, Arbeitsort, Nummer und Status des Triebfahrzeugführerscheins, Lichtbild, Unterschrift, Beschäftigungszeitraum, Befähigungen für Fahrzeuge und Infrastruktur, Sprachkenntnisse, firmenspezifische Anforderungen sowie hochgeladene Nachweise.

Technisch: IP-Adresse und Browserkennung der Sitzung, Zeitpunkte von Anmeldung und letzter Aktivität, Protokoll darüber, wer wann welche Personendaten exportiert hat.

3. Besondere Kategorien nach Art. 9 DSGVO

Die Anwendung verarbeitet Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO. Dazu gehören 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 Nr. 6 – etwa der Code b.1 (vorgeschriebenes Tragen von Brille oder Kontaktlinsen) oder b.2 (Kommunikationshilfe).

Die Verarbeitung ist nach Art. 9 Abs. 2 Buchst. b DSGVO zulässig: sie ist erforderlich, damit das Unternehmen seine Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit erfüllen kann. Konkret verpflichtet § 5 Abs. 2 TfV den Unternehmer, die Tauglichkeit vor der Ausstellung einer Zusatzbescheinigung zu prüfen, und § 10 Abs. 4 TfV, die Vorgänge in einem Register zu führen. Ergänzend gilt § 26 Abs. 3 BDSG.

Als geeignete Garantien im Sinne dieser Vorschrift sind vorgesehen: der Zugriff ist auf Beschäftigte des jeweiligen Unternehmens beschränkt und durch Rollen abgestuft; jeder lesende Zugriff auf eine Fahrerakte wird protokolliert und ist für das Unternehmen einsehbar; die Daten verschiedener Unternehmen sind durch zusammengesetzte Fremdschlüssel und einen Abfragefilter getrennt; ein Zugang des Anbieters kann nur lesen, solange das Unternehmen ihm nicht ausdrücklich einen widerruflichen Freigabecode erteilt; und das

ärztliche Ergebnis wird als Tatsache erfasst, nicht als Befund – gespeichert wird, ob und bis wann jemand tauglich ist, nicht warum.

Der Anbieter wertet diese Daten nicht aus. Es findet keine Profilbildung und keine automatisierte Entscheidung im Sinne des Art. 22 DSGVO statt. Die Anwendung rechnet ausschließlich Fristen aus Daten, die das Unternehmen selbst eingegeben hat. Eine Übermittlung an Dritte findet nicht statt.

Der Zugriff ist auf die Konten des jeweiligen Unternehmens begrenzt. Ein Betreiberkonto kann sich zur Fehlersuche ausdrücklich in einen Mandanten schalten; jeder solche Wechsel wird protokolliert und ist nur zulässig, soweit der Vertrag zur Auftragsverarbeitung ihn deckt.

Dabei kann er ausschließlich lesen. Ändern oder Daten ausleiten kann er nur, wenn das Unternehmen ihm dafür einen Freigabecode erteilt hat – dieser wird im Unternehmensbereich erzeugt, gilt bis zum Widerruf durch das Unternehmen und kann dort jederzeit zurückgenommen werden. Die Erteilung, die Verwendung und der Widerruf stehen im Protokoll des Unternehmens.

4. Rechtsgrundlagen im Überblick

Nutzerkonto und Vertragsabwicklung: Art. 6 Abs. 1 Buchst. b DSGVO (Erfüllung des Nutzungsvertrags).

Daten von Triebfahrzeugführern: Art. 6 Abs. 1 Buchst. c DSGVO (rechtliche Verpflichtung des Unternehmens aus der TfV) in Verbindung mit Art. 9 Abs. 2 Buchst. b DSGVO für Gesundheitsdaten.

Protokolle zu Anmeldung, Export und Mandantenwechsel: Art. 6 Abs. 1 Buchst. f DSGVO (berechtigtes Interesse an Betriebssicherheit und Nachvollziehbarkeit) sowie Art. 32 DSGVO.

Eine Einwilligung wird nicht eingeholt, weil sie im Beschäftigungsverhältnis regelmäßig nicht freiwillig wäre.

5. Wo werden die Daten verarbeitet?

Die Daten der Anwendung selbst – Datenbank und hochgeladene Nachweise – liegen bei Hetzner Online GmbH, Deutschland in Deutschland.

Datensicherungen werden zusätzlich verschlüsselt auf ein zweites Gerät des Anbieters in Deutschland übertragen und dort vorgehalten. Der Grund ist die Sache selbst: läge die einzige Sicherung neben den Daten, wäre ein Brand oder Diebstahl dort der endgültige Verlust – auch des Registers, das zehn Jahre aufzubewahren ist. Das Gerät ist vollverschlüsselt, die Übertragung erfolgt verschlüsselt, und die Daten verlassen Deutschland nicht. Verarbeitet wird dort nichts.

Eine Übermittlung in Staaten außerhalb der Europäischen Union findet nicht statt. Die automatisierte Dokumenten-Erkennung, die eine solche Übermittlung erfordern würde, ist nicht aktiviert (Nummer 10).

Es werden keine Analysedienste, keine Werbenetzwerke, keine externen Schriftarten und keine Inhalte von Fremdservern eingebunden.

6. Cookies

Die Anwendung setzt zwei Cookies, beide technisch notwendig und beide ohne Einwilligung zulässig nach § 25 Abs. 2 Nr. 2 TDDDG.

Das Sitzungscookie nach der Anmeldung. Es enthält nur ein Zufallstoken und ist als HttpOnly, SameSite=Strict und (im Betrieb) Secure gesetzt.

Das Anzeigecookie `nav`. Es merkt sich, ob Sie das Menü am linken Rand eingeklappt haben, und enthält ausschließlich den Wert `zu` oder `auf`. Es wird nur gesetzt, wenn Sie den Menüknopf betätigen, trägt keinen Personenbezug und eignet sich nicht zur Wiedererkennung. Löschen Sie es, erscheint das Menü wieder ausgeklappt – sonst ändert sich nichts.

Tracking-Cookies, Zählpixel und Wiedererkennungsmerkmale werden nicht eingesetzt.

7. Wie lange werden Daten gespeichert?

Daten zu Zusatzbescheinigungen: zehn Jahre nach dem Ungültigwerden der Bescheinigung – so verlangt es § 10 Abs. 8 TfV. Die Anwendung unterstützt diese Frist; über die Löschung entscheidet das Unternehmen.

Einträge im Register nach § 10 Abs. 4 TfV sind unveränderlich. Eine Korrektur entsteht durch einen zusätzlichen Eintrag, nicht durch Überschreiben.

Sitzungen, Schritt 1 – das Ende: Eine Sitzung endet mit der Abmeldung, spätestens mit Ablauf der eingestellten Frist. Ab diesem Moment kann mit ihr keine Anmeldung mehr erfolgen; das Sitzungscookie wird im Browser gelöscht. Der Datenbankeintrag verschwindet damit noch nicht.

Sitzungen, Schritt 2 – die Löschung: Der Eintrag zur beendeten Sitzung – IP-Adresse, Browserkennung, der Hash des Sitzungstokens und die Zeitpunkte – wird noch 7 Tage aufbewahrt, damit ein Missbrauchsverdacht nachvollziehbar bleibt (Art. 6 Abs. 1 Buchst. f DSGVO). Danach wird die Zeile automatisch gelöscht – restlos aus der Datenbank entfernt: es bleibt keine anonymisierte Kopie, kein Archiv und kein Verweis zurück. Ein Aufräumlaufr in der Anwendung erledigt das stündlich; es ist kein manueller Schritt nötig und keine Einstellung, die man vergessen kann.

Nutzerkonten: bis zum Ende des Vertrags, danach 30 Tage zur Datenabholung.

Datensicherungen werden gestaffelt aufbewahrt: die Stände der letzten zwei Tage vollständig, darüber ein Stand je Tag für 2 Wochen und ein Stand je Monat für ein Jahr. Ältere werden automatisch gelöscht. Sitzungsdaten sind in Sicherungen nicht enthalten – sie werden beim Erstellen entfernt, damit die oben zugesagte Löschung nicht durch ein Archiv unterlaufen wird.

Wird ein Datensatz auf Verlangen gelöscht, verschwindet er aus der laufenden Datenbank sofort. In bereits erstellten Sicherungen bleibt er bis zu deren Ablauf enthalten; diese werden ausschließlich zur Wiederherstellung nach einem Ausfall verwendet und nicht ausgewertet. Nach spätestens ein Jahr ist er auch dort verschwunden.

8. Ihre Rechte

Betroffene Personen haben das Recht auf Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18) und Datenübertragbarkeit (Art. 20 DSGVO).

Widerspruchsrecht nach Art. 21 DSGVO. Sie können jederzeit Widerspruch gegen die Verarbeitung Ihrer Daten einlegen, soweit diese auf einem berechtigten Interesse beruht (Art. 6 Abs. 1 Buchst. f DSGVO) – das betrifft die technischen Protokolle und die Maßnahmen zur Betriebssicherheit unter Nummer 11. Wir verarbeiten diese Daten dann nicht mehr, es sei denn, es liegen zwingende schutzwürdige Gründe vor, die Ihre Interessen überwiegen. Der Widerspruch ist an die unter Nummer 1 genannte Stelle zu richten und formfrei möglich.

Nicht widersprechen können Sie der Führung des Registers selbst: sie beruht auf einer rechtlichen Verpflichtung des Unternehmens (§ 10 TfV) und nicht auf einer Abwägung.

Soweit es um Daten von Triebfahrzeugführern geht, sind diese Rechte gegenüber dem verantwortlichen Unternehmen geltend zu machen, nicht gegenüber dem Anbieter. Der Anbieter unterstützt das Unternehmen dabei nach Art. 28 Abs. 3 Buchst. e DSGVO.

Soweit es um die eigenen Nutzerkontodaten geht – Name, Telefonnummer, E-Mail-Adresse, Anmeldeprotokolle –, ist TriMo nach Nummer 1 selbst verantwortlich. Inhaber eines Zugangs wenden sich damit unmittelbar an ihn; die Anschrift steht im Impressum.

Ein Löschanspruch besteht nicht, soweit eine gesetzliche Aufbewahrungspflicht entgegensteht – insbesondere § 10 Abs. 8 TfV.

Es besteht ein Beschwerderecht bei einer Aufsichtsbehörde (Art. 77 DSGVO). Zuständig ist die Behörde am Sitz des verantwortlichen Unternehmens.

Ihr Widerspruchsrecht

Sie haben das Recht, jederzeit gegen die Verarbeitung Ihrer personenbezogenen Daten Widerspruch einzulegen, soweit diese auf ein berechtigtes Interesse gestützt ist (Art. 6 Abs. 1 Buchst. f in Verbindung mit Art. 21 Abs. 1 DSGVO). Gründe, die sich aus Ihrer besonderen Situation ergeben, genügen.

Legen Sie Widerspruch ein, werden die betroffenen Daten nicht mehr verarbeitet – es sei denn, es lassen sich zwingende schutzwürdige Gründe nachweisen, die Ihre Interessen überwiegen, oder die Verarbeitung dient der Geltendmachung oder Verteidigung von Rechtsansprüchen.

Betroffen sind hier die technischen Protokolle (Nummer 11) und die Anmeldedaten Ihres Zugangs. Nicht betroffen sind die Registerdaten der Triebfahrzeugführer: sie beruhen auf einer gesetzlichen Pflicht nach § 10 der Triebfahrzeugführerscheinverordnung und nicht auf einer Interessenabwägung.

Den Widerspruch richten Sie formlos an TriMo; die Anschrift steht im Impressum. Er ist an keine Form und keine Frist gebunden.

9. Sicherheit der Verarbeitung

Übertragung ausschließlich über TLS. Passwörter werden nie im Klartext gespeichert, sondern als bcrypt-Hash. Das Sitzungstoken liegt nur als SHA-256 in der Datenbank; im Klartext existiert es ausschließlich im Cookie des Browsers.

Die Daten verschiedener Unternehmen sind doppelt getrennt: durch zusammengesetzte Fremdschlüssel in der Datenbank und durch einen Filter, der an jede Abfrage angehängt wird. Eine Abfrage kann die Mandantengrenze nicht versehentlich überschreiten.

Wiederholte Fehlanmeldungen sperren ein Konto vorübergehend. Jeder Export von Personendaten wird protokolliert.

Die Anwendung versendet keine E-Mails. Sie hat keinen Postausgang: weder Vertragsunterlagen noch Benachrichtigungen verlassen sie per E-Mail. Ihre Vertragsbestätigung erhalten Sie ausschließlich als PDF zum Herunterladen.

Zugangsdaten versenden wir nicht per E-Mail – weder Passwörter noch Zugangscode noch Anmeldelinks. Eine Nachricht, die Ihnen so etwas anbietet und sich auf diese Anwendung beruft, stammt nicht von uns.

10. Automatisierte Dokumenten-Erkennung (OCR)

Die Anwendung kann Angaben zu Triebfahrzeugführern aus einem hochgeladenen Dokument – etwa einem eingescannten Triebfahrzeugführerschein – vorschlagen, um das Abtippen zu ersparen. Diese Funktion ist derzeit nicht aktiviert.

Solange sie nicht aktiviert ist, verlässt kein Dokument und keine daraus gelesene Angabe die Anwendung. Es findet keine Übermittlung an Dritte und keine Verarbeitung außerhalb der Europäischen Union statt.

Wird die Funktion aktiviert, ändert sich diese Erklärung an dieser Stelle automatisch und benennt den Empfänger, die Rechtsgrundlage und die Aufbewahrung. Der Betrieb der Anwendung protokolliert beide Zustände beim Start nachweisbar mit.

11. Technische Protokolle (Server-Logs)

Der Betrieb führt technische Protokolle, um Störungen zu erkennen und Angriffe abzuwehren. Darin stehen Zeitpunkt, IP-Adresse, aufgerufener Pfad, Antwortstatus sowie Fehlermeldungen der Anwendung.

Keine Klartext-Personendaten von Triebfahrzeugführern: Namen, Geburtsdaten, Untersuchungsergebnisse, Einschränkungen und Dateiinhalte erscheinen in diesen Protokollen nicht. Diese Datensätze werden ausschließlich über technische Kennungen benannt, Dateien ausschließlich über den Hash-Wert ihres Inhalts. Passwörter und Sitzungstoken werden nie protokolliert, auch nicht gekürzt.

Zu Konten wird mehr protokolliert. Sicherheitsrelevante Vorgänge – ein fehlgeschlagener Passwortwechsel, das Hineinschalten des Betreibers in einen Mandanten – werden mit der E-Mail-Adresse des handelnden Kontos und dem Namen des betroffenen Unternehmens festgehalten. Das ist beabsichtigt: Art. 28 DSGVO verlangt, dass nachvollziehbar bleibt, wer wann auf fremde Daten zugegriffen hat, und eine Protokollzeile aus bloßen Nummern beantwortet diese Frage nicht.

IP-Adressen sind personenbezogene Daten. Rechtsgrundlage für ihre Protokollierung ist Art. 6 Abs. 1 Buchst. f DSGVO – das Interesse am sicheren und störungsfreien Betrieb. Sie betreffen die anmeldende Person, nicht die Triebfahrzeugführer, über die Daten geführt werden.

Die Protokolle liegen auf demselben Server wie die Anwendung und werden nicht an Dritte weitergegeben; es ist kein externer Protokolldienst eingebunden.

12. Änderungen dieser Erklärung

Diese Erklärung wird angepasst, wenn sich die Verarbeitung ändert. Maßgeblich ist die jeweils hier veröffentlichte Fassung.