Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

cargo protection gf GmbH · Stand: November 2026

Parteien

Verantwortlicher (nachfolgend „Auftraggeber“): der Kunde, der die Plattform cargo protection auf Grundlage der Allgemeinen Geschäftsbedingungen nutzt, mit den bei der Registrierung angegebenen Daten.

Auftragsverarbeiter (nachfolgend „cargo protection“): cargo protection gf GmbH, Mitterstraße 287a, A-8073 Seiersberg-Pirka, Österreich, FN 685320 z, Landesgericht für Zivilrechtssachen Graz.

Vorbemerkung

Der Auftraggeber nutzt die Plattform cargo protection, um Frachtführer vor einer Auftragsvergabe zu überprüfen. Dabei übermittelt er Daten zu Frachtführern, die auch personenbezogene Daten enthalten können. Dieser Vertrag regelt die datenschutzrechtlichen Pflichten der Parteien bei dieser Verarbeitung nach Art. 28 DSGVO. Er ergänzt die Allgemeinen Geschäftsbedingungen von cargo protection und geht diesen in datenschutzrechtlichen Fragen vor.

§ 1 Gegenstand und Dauer

1.1 cargo protection verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers, um die vom Auftraggeber eingegebenen Daten zu Frachtführern auf Unstimmigkeiten zu prüfen und ihm eine Auswertung (CP-Score, Empfehlung, Einzelergebnisse) bereitzustellen.

1.2 Der Vertrag beginnt mit der Annahme bei der Registrierung und gilt für die Dauer des Nutzungsvertrags. Er endet automatisch mit dessen Beendigung; § 8 gilt darüber hinaus.

§ 2 Art und Zweck der Verarbeitung, Art der Daten, Betroffene

2.1 Die Verarbeitung umfasst das Erheben, Speichern, Abgleichen, Auswerten, Bereitstellen und Löschen der vom Auftraggeber übermittelten Daten.

2.2 Die Daten werden ausschließlich für die Auswertung zugunsten des jeweiligen Auftraggebers verwendet. Sie fließen nicht in Bewertungen für andere Kunden ein, werden anderen Kunden nicht zugänglich gemacht und nicht für eigene Zwecke von cargo protection genutzt, ausgenommen die Aufbewahrung nach § 8.3. Frühere Prüfungen desselben Frachtführers durch denselben Auftraggeber können bei dessen weiteren Prüfungen berücksichtigt werden, solange sie nach § 8.3 gespeichert sind.

Kategorie betroffener Personen	Arten personenbezogener Daten
Ansprechpersonen, Disponierende und Fahrpersonal von Frachtführern	Name, Funktion, Telefonnummer, E-Mail-Adresse, Fahrzeugkennzeichen
Frachtführer als Einzelunternehmer oder Ein-Personen-Unternehmen	Firmenname, Anschrift, UID-Nummer, Kontaktdaten, Angaben aus Lizenzen, Versicherungsnachweisen und weiteren hochgeladenen Dokumenten
Nutzende des Auftraggebers	Name, geschäftliche E-Mail-Adresse, Zugangs- und Protokolldaten (Zeitpunkt, IP-Adresse, durchgeführte Abfragen)

2.3 Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) und Daten über strafrechtliche Verurteilungen (Art. 10 DSGVO) sind nicht Gegenstand der Verarbeitung. Der Auftraggeber lädt solche Daten nicht hoch.

§ 3 Weisungen

3.1 cargo protection verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers. Die Nutzung der Plattformfunktionen gilt als Weisung; weitere Weisungen erteilt der Auftraggeber in Textform an office@cargo-protection.com.

3.2 Ist cargo protection der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, weist sie den Auftraggeber unverzüglich darauf hin und darf die Ausführung bis zur Klärung aussetzen.

3.3 Eine Verarbeitung ohne Weisung erfolgt nur, wenn cargo protection nach Unionsrecht oder österreichischem Recht dazu verpflichtet ist; in diesem Fall informiert sie den Auftraggeber vorab, soweit das Gesetz dies nicht verbietet.

§ 4 Pflichten von cargo protection

4.1 Vertraulichkeit: Alle Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht.

4.2 Sicherheit: cargo protection trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Sie darf diese an den Stand der Technik anpassen, sofern das Schutzniveau nicht unterschritten wird.

4.3 Betroffenenrechte: cargo protection unterstützt den Auftraggeber bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 22 DSGVO). Richtet sich eine betroffene Person direkt an cargo protection, leitet sie den Antrag unverzüglich an den Auftraggeber weiter, soweit dieser zuordenbar ist.

4.4 Datenpannen: cargo protection informiert den Auftraggeber unverzüglich, möglichst binnen 24 Stunden nach Kenntnis, über jede Verletzung des Schutzes der Daten des Auftraggebers. Die Meldung enthält die Angaben nach Art. 33 Abs. 3 DSGVO, soweit bekannt; fehlende Angaben werden nachgereicht.

4.5 Weitere Unterstützung: cargo protection unterstützt den Auftraggeber bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 35 und 36 DSGVO), soweit sie dazu Informationen beitragen kann.

4.6 Ansprechperson: Gernot Fischbach, Geschäftsführung, office@cargo-protection.com, +43 316 395334-0. Ein Datenschutzbeauftragter ist nicht bestellt, da die Voraussetzungen des Art. 37 DSGVO derzeit nicht vorliegen.

§ 5 Unterauftragsverarbeiter

5.1 Der Auftraggeber genehmigt die in Anlage 2 genannten Unterauftragsverarbeiter.

5.2 Der Auftraggeber erteilt eine allgemeine Genehmigung für weitere Unterauftragsverarbeiter. cargo protection informiert ihn mindestens 14 Tage vor einer Hinzuziehung oder Ersetzung per E-Mail. Der Auftraggeber kann binnen dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kommt keine Einigung zustande, kann er den Nutzungsvertrag zum Zeitpunkt der Änderung kündigen.

5.3 cargo protection verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Schutzniveau, das diesem Vertrag entspricht, und haftet gegenüber dem Auftraggeber für dessen Pflichterfüllung.

5.4 Keine Unterauftragsverarbeitung sind Abfragen öffentlich zugänglicher Quellen und Register, bei denen keine personenbezogenen Daten zur Verarbeitung im Auftrag übergeben werden, insbesondere die Prüfung einer UID-Nummer über das MwSt-Informationsaustauschsystem der EU (VIES) und nationale Steuer- und Unternehmensregister, Abfragen von Lizenzverzeichnissen, die Zuordnung von Postleitzahlen über OpenStreetMap Nominatim sowie Abfragen zu Domainnamen. Übermittelt werden dabei jeweils nur UID- oder Lizenznummer, Postleitzahl oder Domain.

§ 6 Übermittlung in Drittländer

6.1 Die Daten werden in Rechenzentren in der Europäischen Union gespeichert (Anwendung: Region Amsterdam, Niederlande; Datenbank und Dateispeicher: EU-Region).

6.2 Eine Übermittlung in ein Land außerhalb des Europäischen Wirtschaftsraums, auch durch einen Fernzugriff eines Unterauftragsverarbeiters mit Sitz in einem Drittland, erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (etwa des EU-US Data Privacy Framework), von Standardvertragsklauseln der Europäischen Kommission oder genehmigter verbindlicher interner Datenschutzvorschriften. Die jeweilige Grundlage ist in Anlage 2 angegeben.

§ 7 Nachweise und Kontrollen

7.1 cargo protection stellt dem Auftraggeber auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind, insbesondere eine aktuelle Beschreibung der Maßnahmen nach Anlage 1 und vorhandene Prüfberichte.

7.2 Reichen diese Nachweise nicht aus, kann der Auftraggeber eine Überprüfung selbst oder durch eine zur Verschwiegenheit verpflichtete prüfende Stelle durchführen, höchstens einmal jährlich, nach Ankündigung von mindestens 30 Tagen, während der Geschäftszeiten und ohne Einsicht in Daten anderer Kunden oder in Betriebs- und

Geschäftsgeheimnisse von cargo protection, insbesondere die Prüfmethoden. Anlassbezogene Prüfungen nach einer Datenpanne oder auf Anordnung einer Aufsichtsbehörde bleiben unberührt.

7.3 Den Aufwand einer Vor-Ort-Prüfung kann cargo protection zu angemessenen Sätzen verrechnen, außer die Prüfung ergibt einen wesentlichen Verstoß.

§ 8 Rückgabe, Löschung und Aufbewahrung

8.1 Nach Ende des Nutzungsvertrags kann der Auftraggeber seine Auswertungen binnen 30 Tagen über die Plattform exportieren.

8.2 Danach löscht cargo protection die Daten des Auftraggebers, soweit nicht § 8.3 oder eine gesetzliche Aufbewahrungspflicht entgegensteht. Daten in Sicherungskopien werden im regulären Sicherungszyklus überschrieben, spätestens nach 7 Tagen.

8.3 Prüfhistorie und Aufbewahrung zur Rechtssicherheit: Die eingegebenen Abfragedaten, hochgeladenen Dokumente und zugehörigen Auswertungen werden für dreieinhalb Jahre ab der jeweiligen Abfrage aufbewahrt. Während der Laufzeit des Nutzungsvertrags stehen sie dem Auftraggeber als Prüfhistorie zur Verfügung, damit er durchgeführte Prüfungen innerhalb der für Transportverträge maßgeblichen Verjährungsfristen (insbesondere Art. 32 CMR) nachweisen kann; insoweit verarbeitet cargo protection die Daten im Auftrag. Prüft der Auftraggeber denselben Frachtführer erneut, können seine eigenen gespeicherten früheren Prüfungen dieses Frachtführers berücksichtigt werden. Jede Prüfung wird im Übrigen neu und unabhängig durchgeführt; Daten eines Auftraggebers werden weder für Prüfungen anderer Kunden noch für sonstige Auswertungen verwendet. Nach Ende des Nutzungsvertrags und Ablauf der Exportfrist nach § 8.1 bewahrt cargo protection die Daten bis zum Ende der Frist als eigener Verantwortlicher auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit Art. 17 Abs. 3 lit. e DSGVO gesperrt auf und verwendet sie ausschließlich zur Rechtsverfolgung oder -verteidigung. Nach Ablauf der Frist werden sie gelöscht, sofern kein Verfahren anhängig ist.

8.4 Abfrage- und Systemprotokolle: Protokolle über Anmeldungen und durchgeführte Abfragen (insbesondere Zeitpunkt, Zugangskonto, IP-Adresse und geprüfter Frachtführer) werden für ein Jahr gespeichert und dienen der Sicherheit, der Support- und Fehleranalyse sowie der Erkennung und Aufklärung von Missbrauch, etwa systematischer Mehrfachabfragen. Eine längere Speicherung erfolgt nur, soweit dies zur Verfolgung eines konkreten Missbrauchsverdachts erforderlich ist oder eine gesetzliche Pflicht besteht.

§ 9 Haftung

9.1 Die Haftung der Parteien gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO.

9.2 Im Verhältnis der Parteien zueinander gelten die Haftungsregeln der Allgemeinen Geschäftsbedingungen von cargo protection, soweit Art. 82 DSGVO dem nicht zwingend entgegensteht.

§ 10 Schlussbestimmungen

10.1 Dieser Vertrag wird elektronisch abgeschlossen (Art. 28 Abs. 9 DSGVO), indem der Auftraggeber ihn bei der Registrierung durch ausdrückliche Bestätigung annimmt. Er steht dauerhaft zum Download bereit.

10.2 Änderungen, die aufgrund geänderter Rechtslage oder Behördenpraxis erforderlich sind, teilt cargo protection mindestens 30 Tage vor Inkrafttreten mit. Widerspricht der Auftraggeber nicht binnen dieser Frist, gelten sie als angenommen; auf diese Folge wird in der Mitteilung hingewiesen.

10.3 Bei Widersprüchen geht dieser Vertrag den Allgemeinen Geschäftsbedingungen in datenschutzrechtlichen Fragen vor. Ist eine Bestimmung unwirksam, bleibt der übrige Vertrag wirksam.

10.4 Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen. Gerichtsstand ist das sachlich zuständige Gericht in Graz.

Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Schutzziel	Maßnahmen
Zutritt	Hosting in professionellen Rechenzentren in der Europäischen Union (Region Amsterdam, Niederlande); kein eigener Serverbetrieb
Zugang	Persönliche Benutzerkonten, Passwortrichtlinie, Zwei-Faktor-Anmeldung für Administratoren und Infrastruktur-Konten (in Umsetzung)
Zugriff	Mandantentrennung auf Unternehmensebene: Jeder Kunde sieht nur seine eigenen Abfragen und Auswertungen; Administratorrechte nur für Geschäftsführung und technische Leitung

Schutzziel	Maßnahmen
Weitergabe	Verschlüsselte Übertragung (TLS) für Plattform, Schnittstellen und Administration; Verschlüsselung gespeicherter Daten; keine Weitergabe an andere Kunden
Eingabe	Protokollierung von Anmeldungen, Abfragen und Änderungen mit Zeitstempel und Zugangskonto; Aufbewahrung der Protokolle für ein Jahr
Verfügbarkeit	Tägliche automatisierte Sicherung der Datenbank beim Hosting-Anbieter mit Aufbewahrung für 7 Tage, dokumentierter Notfallplan für Sicherheitsvorfälle und Datenpannen
Trennung	Getrennte Umgebungen für Entwicklung und Betrieb; Daten nach Kunden logisch getrennt
Überprüfung	Sicherheitstest (Penetrationstest) vor Marktstart; Überprüfung der Maßnahmen mindestens jährlich und nach jedem schwerwiegenden Vorfall
Organisation	Verpflichtung aller Beteiligten zur Vertraulichkeit; Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern; Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Anlage 2: Unterauftragsverarbeiter

Stand bei Vertragsabschluss. Änderungen nach § 5.2. Die jeweils aktuelle Liste ist unter www.cargo-protection.com/de/subprocessors abrufbar.

Unternehmen	Leistung	Ort der Verarbeitung	Grundlage Drittlandtransfer
Railway Corporation, San Francisco, USA	Hosting der Plattform	EU, Region Amsterdam (Niederlande)	EU-US Data Privacy Framework bzw. Standardvertragsklauseln laut DPA
Supabase Pte. Ltd., Singapur	Datenbank, Anmeldung, Dateispeicher	EU	Standardvertragsklauseln laut DPA
Google Cloud EMEA Ltd., Dublin, Irland	Dokumentenauslesung (Document AI)	EU	Standardvertragsklauseln laut Cloud Data Processing Addendum
OpenAI Ireland Ltd., Dublin, Irland	Auslesen und Strukturieren von E-Mail- und Dokumentinhalten	EU (Datenresidenz Europa)	EU-US Data Privacy Framework bzw. Standardvertragsklauseln laut DPA
Twilio Ireland Ltd., Dublin, Irland	Prüfung von Rufnummern (Lookup)	USA	Verbindliche interne Datenschutzvorschriften (BCR)
Bouncer Sp. z o.o., Breslau, Polen	Prüfung von E-Mail-Adressen	EU (Frankfurt am Main)	keine Übermittlung
Plus Five Five, Inc. (Resend), San Francisco, USA	Versand von System-E-Mails	EU	EU-US Data Privacy Framework, Standardvertragsklauseln
widdix GmbH (attachmentAV), Deutschland	Virenprüfung hochgeladener Dateien ohne Speicherung	EU	keine Übermittlung
Cloudflare, Inc., San Francisco, USA	Auslieferung und Schutz der Website (Content Delivery Network)	EU und weltweit	EU-US Data Privacy Framework, Standardvertragsklauseln
Microsoft Ireland Operations Ltd., Dublin, Irland	E-Mail-Kommunikation (Microsoft 365)	EU/EWR	EU Data Boundary; Standardvertragsklauseln laut Microsoft-DPA

Nicht aufgeführt ist der Zahlungsdienstleister: Er verarbeitet nur Rechnungs- und Zahlungsdaten des Auftraggebers in eigener Verantwortung und keine Abfragedaten. Ebenfalls keine Unterauftragsverarbeitung im Sinne des § 5.4 sind die Abfragen bei VIES und den nationalen Registern (Polen: Weiße Liste der Mehrwertsteuerpflichtigen und Lizenzverzeichnisse der GITD; Rumänien: ANAF; Tschechien: ARES und Mehrwertsteuerregister), bei OpenStreetMap Nominatim sowie Domainabfragen (WhoisXML API, WHOIS-Dienst von nic.at).