



Vereinbarung für die Auftragsverarbeitung (Stand: Mai 2018)

zwischen

TM Logistik Gruppe

(TM Logistik Hamburg GbR, TM Logistik Hannover GbR, TM Logistik & Services GbR)

Rosenheimer Str. 37

28219 Bremen

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

und

ihren Kunden

- Verantwortlicher - nachstehend Auftraggeber genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand dieser Vereinbarung ist die über die zur Erbringung von Postdienstleistung erforderliche Datenverarbeitung hinausgehende Verwaltung von personenbezogenen Daten in den bereitgestellten Online-Systeme zur Versandvorbereitung. Diese Vereinbarung findet nur Anwendung, soweit "Verantwortliche" die vom Auftragsverarbeiter bereitgestellten Adressbuchfunktionen zur dauerhaften und sendungsunabhängigen Verwaltung ihrer Kundenadressen nutzen.

(2) Dauer

Diese Vereinbarung zur Auftragsverarbeitung gilt für einen unbegrenzten Zeitraum und kann vom Verantwortlichen jederzeit durch die Einstellung der Nutzung der Adressbuchfunktionen sowie Löschung aller gespeicherten Daten in den Adressbuchfunktionen beendet werden.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Nutzung der Adressbuchfunktionen ist optional und dient der dauerhaften und sendungsunabhängigen Verwaltung der Kundenadressen des Verantwortlichen. Die Eingabe, Änderung, Speicherung und Löschung erfolgt durch den Verantwortlichen selbst. Die Nutzung dieser Adressbuchfunktionen ist für die Erbringung von

Postdienstleistungen nicht erforderlich, sondern unterstützt lediglich den Verantwortlichen bei der Verwaltung seiner Versandadressen.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland ist ausgeschlossen.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

- Name
- Kontaktdaten
- Adresse

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden von TM Logistik
- Kunden von Kunden von TM Logistik
- Beauftragte von Kunden von TM Logistik
- Beauftragte von TM Logistik

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmer sind zulässig, soweit:
 - o der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

- o der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- o eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätig werden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

(6) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Nach angemessener Vorankündigung von mindestens 10 Geschäftstagen seitens des Verantwortlichen und um die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen sowie der aus dieser Vereinbarung erwachsenden Pflichten sicherzustellen und zu überprüfen, hat der Auftragsverarbeiter dem Verantwortlichen oder einem von dem Verantwortlichen beauftragten Prüfer die Durchführung regelmäßiger Prüfungen zu gestatten, wenn

- (a) der Verantwortliche die begründete Vermutung hat, dass der Auftragsverarbeiter nicht im Einklang mit den technisch-organisatorischen Maßnahmen und / oder den Verpflichtungen aus dieser Vereinbarung handelt;
- (b) sich ein Sicherheitsvorfall ereignet hat;
- (c) eine solche Prüfung durch die für den Verantwortlichen zuständige Aufsichtsbehörde gefordert wird.

(2) Ungeachtet des Vorstehenden kann der Nachweis für die Einhaltung der Vorschriften folgendermaßen erbracht werden:

- (a) Einhaltung der genehmigten Verhaltensregeln und/oder
- (b) Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO und/oder
- (c) aktuelle Zertifikate von Prüfern, Berichte oder Auszüge aus Berichten unabhängiger Stellen. Auf Verlangen des Verantwortlichen hat der Auftragsverarbeiter dem Verantwortlichen eine Abschrift des von dem externen Prüfer unterzeichneten Prüfungsberichts zur Verfügung zu stellen, sodass der Verantwortliche angemessen überprüfen kann, ob der Auftragsverarbeiter die technischen und organisatorischen Maßnahmen und Pflichten im Rahmen dieser Vereinbarung umsetzt bzw. erfüllt.

(4) Prüfungen werden zu den üblichen Geschäftszeiten, in angemessenem Umfang und ohne Störung des Betriebsablaufs durchgeführt. Für den Fall, dass der Verantwortliche die Prüfung durch einen von ihm beauftragten unabhängigen Prüfer durchführen lässt, hat dieser zuvor eine Verschwiegenheitserklärung zu unterzeichnen. Zudem darf der unabhängige Prüfer nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen.

(4) Sofern die Prüfung seitens des Auftragsverarbeiters oder eines anderen Auftragsverarbeiters Aufwendungen bedeutet, die über einen Geschäftstag hinausgehen, ist der Verantwortliche damit einverstanden, jeden darüber hinaus gehenden Tag zu erstatten.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
 - c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
 - d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
 - e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Schlussbestimmungen

- (1) Werden Daten des Verantwortlichen Gegenstand einer Durchsuchung und Beschlagnahme, eines Pfändungsbeschlusses, einer Einziehung im Rahmen eines Konkurs- oder Insolvenzverfahrens bzw. ähnlicher Ereignisse oder Maßnahmen Dritter, während sie im Verantwortungsbereich des Auftragsverarbeiters sind, so hat der Auftragsverarbeiter den Verantwortlichen hierüber unverzüglich in Kenntnis zu setzen. Der Auftragsverarbeiter hat sämtlichen Beteiligten dieser Maßnahme unverzüglich mitzuteilen, dass sich hiervon betroffene Daten ausschließlich im Eigentum des Verantwortlichen befinden und in dessen Verantwortungsbereich liegen, dass der Verantwortliche das alleinige Verfügungsrecht über diese Daten hat und dass der Verantwortliche für die Anwendung des Datenschutzrechts zuständig ist.
- (2) Sollte eine Bestimmung dieser Vereinbarung gleich aus welchem Grund für ungültig, rechtswidrig oder undurchsetzbar befunden werden, wird die betreffende Bestimmung ausgenommen und bleiben die übrigen Bestimmungen dieser Vereinbarung so in vollem Umfang in Kraft und rechtswirksam, als wäre diese Vereinbarung ohne die ungültige Bestimmung geschlossen worden.
- (3) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland