

[› VERTRAG NACH ART. 28 DSGVO](#)

Vertrag zur Auftragsverarbeitung

zwischen dem Kunden als Verantwortlichem und der dreifachDigital GmbH als Auftragsverarbeiter für den Dienst „Boxmove“ (Postfach-Umzüge und Zwischenlager).

Online: portal.boxmove.de/legal/avv

[› DOKUMENT](#)**AVV-BM-2026-09**[› STAND](#)

September 2026 · Version 1.0

[› MARKE](#)**Boxmove**

Ein Produkt der dreifachDigital GmbH

[› ANLAGEN](#)

- 1 Konkretisierung der Verarbeitung
- 2 Technische und organisatorische Maßnahmen
- 3 Subunternehmer

[› VERTRAGSPARTEIEN](#)

Auftraggeber · Verantwortlicher

Firma, Straße und Hausnummer, PLZ und Ort, vertreten durch – wie im Kundenkonto bei Boxmove hinterlegt –

– nachfolgend „Kunde“ oder „Verantwortlicher“ –

Auftragnehmer · Auftragsverarbeiter

dreifachDigital GmbH, Bozener Straße 41, 49082 Osnabrück, vertreten durch die Geschäftsführer Sebastian Kather, Marvin Kather und Raphael Pède, Amtsgericht Osnabrück, HRB 223038

– nachfolgend „dreifachDigital“ oder „Auftragsverarbeiter“ –

[› PRÄAMBEL](#)

Zwischen den Parteien besteht ein Hauptvertrag über die Nutzung des Dienstes „Boxmove“ (Postfach-Umzüge und Zwischenlager; Allgemeine Geschäftsbedingungen abrufbar unter boxmove.de/agb.html). Im Rahmen der Leistungserbringung verarbeitet dreifachDigital personenbezogene Daten im Auftrag des Kunden: Inhalte der Postfächer, die der Kunde von einem Quellsystem in ein Zielsystem kopieren lässt, sowie die dafür erforderlichen Zugangsdaten. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien gemäß Art. 28 DSGVO.

[› TEIL I · GEGENSTAND DER VERARBEITUNG](#)

§ 1 Gegenstand, Dauer und Zustandekommen

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch dreifachDigital im Auftrag des Kunden im Rahmen der Bereitstellung, des Betriebs und des Supports des Dienstes

[› UNTERNEHMEN](#)

dreifachDigital GmbH
Bozener Straße 41
49082 Osnabrück

[› KONTAKT](#)

support@boxmove.de
hallo@dreifach-digital.de
dreifach-digital.de

[› HANDELSREGISTER](#)

Amtsgericht Osnabrück, HRB 223038
USt-IdNr. DE461724855 · St-Nr. 66/200/78072
Geschäftsführer: Raphael Pède · Marvin Kather ·
Sebastian Kather

1 / 14

„Boxmove“: das Kopieren von Postfachinhalten (E-Mails, soweit unterstützt Kalender und Kontakte) von einem Quellsystem in ein Zielsystem, das tägliche Nachziehen neuer Elemente, der Abschluss des Umzugs und – auf Wunsch des Kunden – die vorübergehende Verwahrung der Inhalte im Zwischenlager.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Eine gesonderte Kündigung ist ausgeschlossen; die Pflichten aus §§ 4 und 11 bestehen über das Vertragsende hinaus fort.

(3) Dieser Vertrag gilt für Kunden, die Unternehmer im Sinne von § 14 BGB sind. dreifachDigital stellt ihn dem Kunden bei der Registrierung und dauerhaft im Kundenkonto sowie unter boxmove.de/avv.html zur Verfügung. Er wird Bestandteil des Vertragsverhältnisses, sobald der Kunde die erste entgeltliche Buchung (Umzug oder Zwischenlager) auslöst und dabei die Einbeziehung dieses Vertrags bestätigt; das elektronische Format genügt (Art. 28 Abs. 9 DSGVO). Auf Wunsch schließen die Parteien diesen Vertrag zusätzlich unterschrieben ab; Anfragen an info@dreifach-digital.de.

§ 2 Umfang, Art und Zweck der Verarbeitung

(1) Gegenstand, Art und Zweck der Verarbeitung, die Kategorien betroffener Personen sowie die Arten personenbezogener Daten sind in **Anlage 1 (Konkretisierung der Verarbeitung)** beschrieben.

(2) Die Verarbeitung findet in Mitgliedstaaten der Europäischen Union bzw. des Europäischen Wirtschaftsraums statt. Übermittlungen in Drittländer richten sich nach § 7.

(3) dreifachDigital verarbeitet die Postfachinhalte ausschließlich, um sie zu kopieren und – im Fall des Zwischenlagers – zu verwahren. Es findet keine inhaltliche Auswertung statt, insbesondere keine Auswertung durch Verfahren der künstlichen Intelligenz, keine Indexierung zu anderen Zwecken, keine Nutzung für Werbung und kein Mitlesen durch Mitarbeiter von dreifachDigital. Protokolle des Dienstes enthalten keine Nachrichteninhalte.

> TEIL II · PFLICHTEN DER PARTEIEN

§ 3 Verantwortlichkeit und Weisungsrecht

(1) Der Kunde ist im Verhältnis zu den betroffenen Personen Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen verantwortlich und stellt sicher, dass er zur Übertragung der Postfachinhalte berechtigt ist. Zieht der Kunde Postfächer für einen eigenen Auftraggeber um (etwa als IT-Dienstleister für dessen Unternehmen), stellt er sicher, dass er von diesem Auftraggeber zur Beauftragung von dreifachDigital als weiterem Auftragsverarbeiter befugt ist.

(2) dreifachDigital verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden. Einzige Ausnahme: Unionsrecht oder das Recht eines Mitgliedstaats verpflichtet dreifachDigital zu einer anderen Verarbeitung. In diesem Fall informiert dreifachDigital den Kunden vor der Verarbeitung über diese Pflicht, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

(3) Weisungen erteilt der Kunde in erster Linie durch die Nutzung und Konfiguration des Dienstes – etwa indem er Postfächer anlegt, Quell- und Zielsystem festlegt, Ordner ausschließt, Läufe startet, den Tag des Wechsels bestimmt, den Umzug abschließt, ein Zwischenlager bucht, verlängert oder löscht.

Darüber hinausgehende Weisungen bedürfen der Textform und sind an support@boxmove.de zu richten.

(4) Hält dreifachDigital eine Weisung für datenschutzrechtlich unzulässig, informiert dreifachDigital den Kunden unverzüglich. dreifachDigital darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.

§ 4 Vertraulichkeit

(1) Alle Personen, die für dreifachDigital personenbezogene Daten verarbeiten, sind zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO).

(2) Zugriff auf personenbezogene Daten des Kunden erhalten nur Personen, die diesen Zugriff zur Erfüllung ihrer Aufgaben benötigen. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der jeweiligen Tätigkeit und nach Vertragsende fort.

§ 5 Technische und organisatorische Maßnahmen

(1) dreifachDigital trifft die in **Anlage 2 (Technische und organisatorische Maßnahmen)** beschriebenen Maßnahmen gemäß Art. 32 DSGVO und hält diese während der Vertragslaufzeit aufrecht.

(2) Die Maßnahmen entwickeln sich mit dem Stand der Technik weiter. dreifachDigital darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das vereinbarte Schutzniveau darf dabei nicht sinken. Wesentliche Änderungen, die das Schutzniveau beeinträchtigen könnten, teilt dreifachDigital dem Kunden mit.

§ 6 Weitere Auftragsverarbeiter (Subunternehmer)

(1) Der Kunde erteilt die allgemeine Genehmigung zur Einschaltung weiterer Auftragsverarbeiter. Die bei Vertragsschluss eingesetzten Subunternehmer sind in **Anlage 3 (Subunternehmer)** aufgeführt.

(2) Die in Anlage 3 Teil B genannten Dienste kommen nur zum Einsatz, wenn der Kunde die jeweilige Funktion aktiv nutzt (Anmeldung mit Microsoft-Konto, Umzug von oder nach Microsoft 365). Ohne diese Nutzung werden keine Daten an diese Dienste übermittelt.

(3) Will dreifachDigital einen Subunternehmer hinzuziehen oder ersetzen, informiert dreifachDigital den Kunden mindestens vier Wochen vorher in Textform (per E-Mail an die im Konto hinterlegte Adresse oder als Hinweis im Dienst). Der Kunde kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Finden die Parteien dann keine einvernehmliche Lösung, kann der Kunde den Hauptvertrag außerordentlich zu dem Zeitpunkt kündigen, an dem die Änderung wirksam wird; laufende Umzüge werden bis dahin mit den bisherigen Subunternehmern fertiggestellt, soweit möglich.

(4) dreifachDigital verpflichtet jeden Subunternehmer vertraglich auf mindestens das Datenschutz- und Sicherheitsniveau dieses Vertrags und prüft die Einhaltung in angemessenen Abständen. Verletzt ein Subunternehmer seine Pflichten, haftet dreifachDigital dem Kunden dafür wie für eigenes Verhalten.

§ 7 Verarbeitung in Drittländern

(1) Hosting, Zwischenlager, Datensicherung und E-Mail-Versand erfolgen in der AWS-Region Frankfurt am Main (eu-central-1). dreifachDigital unterhält keine eigenen Server.

(2) Eine Übermittlung personenbezogener Daten in Länder außerhalb der EU bzw. des EWR erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind – entweder auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission (etwa des EU-US Data Privacy Framework) oder auf Grundlage der EU-Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO.

(3) Welche Dienste in Drittländern verarbeiten können und welche dieser Garantien jeweils gilt, ist in Anlage 3 ausgewiesen.

(4) Die Quell- und Zielsysteme des Kunden (Mailserver, Hosted Exchange, Microsoft 365) sind keine Subunternehmer von dreifachDigital. Wo diese Systeme stehen und ob dort ein Drittlandtransfer stattfindet, bestimmt der Kunde durch seine Wahl des Anbieters; Boxmove verbindet sich lediglich mit den vom Kunden benannten Servern.

§ 8 Unterstützung des Verantwortlichen

(1) dreifachDigital unterstützt den Kunden dabei, die Rechte betroffener Personen (Art. 12 bis 23 DSGVO) zu erfüllen. Dafür stellt der Dienst Funktionen bereit, die der Kunde selbst nutzen kann: Übersicht der umgezogenen Postfächer und Ordner, Bericht je Lauf, Löschung einzelner Postfächer, des Zwischenlagers und ganzer Umzüge.

(2) Wenden sich betroffene Personen direkt an dreifachDigital und betrifft die Anfrage erkennbar Daten des Kunden, leitet dreifachDigital die Anfrage unverzüglich an den Kunden weiter.

(3) dreifachDigital unterstützt den Kunden außerdem bei den Pflichten aus Art. 32 bis 36 DSGVO – Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörde –, soweit dreifachDigital über die dafür nötigen Informationen verfügt.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Wird dreifachDigital eine Verletzung des Schutzes personenbezogener Daten bekannt, die Daten des Kunden betrifft, meldet dreifachDigital sie dem Kunden unverzüglich – spätestens 48 Stunden nach Bekanntwerden.

(2) Die Meldung enthält, soweit die Informationen vorliegen: die Art der Verletzung, die betroffenen Systeme, Postfächer und Datenarten, die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen und vorgeschlagenen Abhilfemaßnahmen sowie einen Ansprechpartner. Später bekannt werdende Informationen reicht dreifachDigital unverzüglich nach.

(3) dreifachDigital unterstützt den Kunden bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

> TEIL III · KONTROLLE, BEENDIGUNG UND SCHLUSSBESTIMMUNGEN

§ 10 Nachweise und Kontrollrechte

(1) dreifachDigital stellt dem Kunden alle Informationen zur Verfügung, die dieser benötigt, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen. Als Nachweise dienen insbesondere dieser

Vertrag mit seinen Anlagen, die aktuelle TOM-Dokumentation, das Audit-Protokoll des Kundenkontos sowie Zertifizierungen und Prüfberichte der Rechenzentrumsbetreiber (für AWS u. a. ISO 27001 und SOC 1–3).

(2) Der Kunde darf die Einhaltung dieses Vertrags höchstens einmal pro Kalenderjahr kontrollieren – selbst oder durch einen Prüfer, der zur Vertraulichkeit verpflichtet ist und nicht im Wettbewerb zu dreifachDigital steht. Kontrollen sind 30 Tage vorher anzukündigen und finden während der üblichen Geschäftszeiten statt, ohne den Geschäftsbetrieb unangemessen zu beeinträchtigen. Bei einem konkreten, dokumentierten Datenschutzvorfall ist eine anlassbezogene Kontrolle mit kürzerer, angemessener Frist zulässig.

(3) Jede Partei trägt die ihr durch eine Kontrolle entstehenden Kosten selbst.

§ 11 Löschung und Rückgabe

(1) Boxmove kopiert Postfachinhalte; die Inhalte verbleiben im Quellsystem und liegen nach dem Umzug im Zielsystem des Kunden. Eine Rückgabe im Sinne einer Herausgabe von Datenbeständen ist daher nur für das Zwischenlager erforderlich: dessen Inhalte kopiert Boxmove auf Weisung des Kunden in das Zielsystem.

(2) Zugangsdaten zu Quell- und Zielsystemen löscht dreifachDigital automatisch mit dem Abschluss des Umzugs (letzter Lauf), spätestens mit der Löschung des Umzugs oder der Schließung des Kundenkontos. Der Kunde kann Zugangsdaten jederzeit selbst ersetzen oder entfernen.

(3) Das Zwischenlager wird gelöscht, sobald der Kunde den Weiterzug abgeschlossen hat und die Löschung auslöst, spätestens jedoch 30 Tage nach Ablauf der gebuchten Verwahrfrist von 30 Tagen (Karenzzeit, Hauptvertrag Ziffer 7). Der Kunde kann das Zwischenlager jederzeit selbst löschen. Gelöschte Inhalte können nicht wiederhergestellt werden.

(4) Umzugsdaten (Postfachadressen, Ordnernamen, Anzahl und Größe der Elemente, Laufprotokolle ohne Inhalte, Berichte) kann der Kunde jederzeit durch Löschen des Umzugs entfernen. Mit der Schließung des Kundenkontos löscht dreifachDigital alle Umzugsdaten, Zugangsdaten und Zwischenlager des Kunden. In Sicherungskopien der Datenbank werden diese Daten mit den rollierenden Sicherungszyklen gelöscht, spätestens 90 Tage nach der Löschung im Produktivsystem; das Zwischenlager selbst ist nicht Teil der Sicherungen.

(5) Gesetzliche Aufbewahrungspflichten von dreifachDigital (insbesondere §§ 257 HGB, 147 AO) bleiben unberührt. Davon betroffene Daten (Rechnungsdaten) werden für die Dauer der Pflicht gesperrt und nur zu deren Erfüllung verarbeitet. Auf Verlangen bestätigt dreifachDigital die Löschung in Textform.

§ 12 Vergütung

Die Pflichten aus diesem Vertrag sind mit der Vergütung des Hauptvertrags abgegolten. Veranlasst der Kunde Unterstützungsleistungen, die über das gesetzlich geschuldete Maß hinausgehen (z. B. wiederholte Vor-Ort-Kontrollen ohne Anlass), kann dreifachDigital dafür nach vorheriger Ankündigung eine angemessene Vergütung verlangen.

§ 13 Haftung

Für die Haftung der Parteien gilt Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags (Allgemeine Geschäftsbedingungen, Ziffer 8).

§ 14 Schlussbestimmungen

(1) Weichen dieser Vertrag und der Hauptvertrag voneinander ab, gilt für die Verarbeitung personenbezogener Daten dieser Vertrag. Zwingendes Recht, insbesondere DSGVO und BDSG, bleibt unberührt.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Es gilt das Recht der Bundesrepublik Deutschland. Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags.

Unterschriften (nur bei zusätzlichem schriftlichem Abschluss nach § 1 Abs. 3)

Kunde (Verantwortlicher): Ort, Datum · Name in Druckbuchstaben · Unterschrift

dreifachDigital GmbH (Auftragsverarbeiter): Ort, Datum · Name in Druckbuchstaben · Unterschrift

Konkretisierung der Verarbeitung

Gegenstand, Dauer, Art und Zweck der Verarbeitung, betroffene Personen und Datenarten

1. Gegenstand der Verarbeitung

Bereitstellung und Betrieb des Dienstes „Boxmove“ zum Umzug von E-Mail-Postfächern: Verbindung zu den vom Kunden benannten Quell- und Zielsystemen (Mailkonten per IMAP, Hosted Exchange per IMAP/EWS, Microsoft 365 per Microsoft Graph), Kopieren der Postfachinhalte mit Ordnerstruktur, Markierungen und Datum, soweit unterstützt auch Kalender und Kontakte; tägliches Nachziehen neuer Elemente; Abschluss mit letztem Lauf und Bericht; auf Wunsch des Kunden Verwahrung der Inhalte im Zwischenlager, bis das Zielsystem sie aufnehmen kann; ferner Datensicherung der Steuerungsdaten, Support und Wartung.

2. Dauer der Verarbeitung

Je Umzug für die Umzugszeit von 30 Tagen ab dem ersten Kopieren, verlängerbar um jeweils 30 Tage; Zugangsdaten bis zum Abschluss des Umzugs; Zwischenlager für die gebuchte Frist von 30 Tagen je Postfach zuzüglich 30 Tage Karenz; Umzugsdaten bis zur Löschung durch den Kunden oder Schließung des Kontos. Einzelheiten in § 11 des Vertrags.

3. Art der Verarbeitung

Erheben (Abruf aus dem Quellsystem), Speichern (nur Zwischenlager und Steuerungsdaten), Auslesen, Übermitteln an das vom Kunden bestimmte Zielsystem, Abgleichen (Delta-Läufe), Sichern (Steuerungsdaten) und Löschen personenbezogener Daten – jeweils ausschließlich zur Erbringung der vertraglich vereinbarten Leistung. Postfachinhalte werden während der Übertragung nur im Arbeitsspeicher gehalten; eine dauerhafte Speicherung findet nur im Zwischenlager statt.

4. Zweck der Verarbeitung

Übertragung der Postfächer des Kunden bzw. seines Auftraggebers zu einem anderen Anbieter ohne Verlust von Inhalten und Struktur; vorübergehende Verwahrung bei Anbieterwechseln, bei denen das Zielsystem die Postfächer erst nach dem Domainumzug bereitstellt. dreifachDigital verfolgt keine eigenen Zwecke mit den Inhalten (§ 2 Abs. 3 des Vertrags).

5. Kategorien betroffener Personen

- Mitarbeiter, Nutzer und Inhaber der umzuziehenden Postfächer (Beschäftigte des Kunden oder seines Auftraggebers),
- Kommunikationspartner dieser Postfächer: Kunden, Interessenten, Lieferanten, Geschäftspartner, Behörden, private Kontakte sowie alle weiteren Absender und Empfänger von E-Mails, Termineinladungen und Kontakteinträgen,
- in E-Mails, Anhängen, Terminen und Kontakten genannte Dritte,
- Nutzer des Kundenkontos bei Boxmove, soweit sie im Auftrag des Kunden handeln.

6. Arten personenbezogener Daten

E-Mail-Inhalte

Kopf- und Metadaten (Absender, Empfänger, Betreff, Datum, Message-ID, Markierungen wie gelesen/beantwortet, Ordnerzuordnung) sowie Nachrichtentexte und Anhänge in allen im Postfach enthaltenen Formaten. Der Inhalt ist vom Kunden bestimmt und kann alle Datenarten umfassen, auch besondere Kategorien nach Art. 9 DSGVO (siehe Nr. 8).

Kalender

Termine mit Titel, Zeitraum, Ort, Beschreibung, Teilnehmern und deren Antwortstatus, Erinnerungen, Serienregeln.

Kontakte

Name, Firma, Anschriften, Telefonnummern, E-Mail-Adressen, Notizen, Geburtstage und weitere vom Kunden gepflegte Felder.

Zugangsdaten

Postfachadressen und Anmeldenamen, Passwörter für IMAP/EWS (vom Kunden eingetragen oder vom Postfachinhaber über einen persönlichen Link eingegeben), OAuth-Token für Microsoft 365 (Anmeldung je Postfach) bzw. die Freigabe des Microsoft-365-Tenants durch dessen Administrator (Anwendungsberechtigung); Servernamen und Anschlüsse.

Steuerungs- und Protokolldaten

Postfachadressen, Ordnernamen, Anzahl und Größe der Elemente, Zeitpunkte und Ergebnisse der Läufe, Fehlermeldungen (ohne Nachrichteninhalte), Belegung des Zwischenlagers, Bericht je Umzug, Audit-Protokoll (Nutzer, Zeitpunkt, Aktion).

7. Zwischenlager

Im Zwischenlager werden E-Mails als einzelne Dateien im Nachrichtenformat sowie Termine und Kontakte, soweit die beteiligten Systeme sie im Postfach führen als strukturierte Dateien abgelegt, getrennt je Kunde und Postfach, verschlüsselt nach Anlage 2. Ein Index (Ordner, Message-IDs, Markierungen, Datum, Größe) liegt in der Datenbank des Dienstes. Passwörter werden nicht im Zwischenlager abgelegt.

8. Besondere Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nicht Gegenstand der Leistung, kann aber in den Postfachinhalten enthalten sein (etwa Gesundheitsdaten in E-Mails an eine Personalabteilung oder Arztpraxis). Boxmove behandelt alle Inhalte gleich und wertet sie nicht aus. Für die Zulässigkeit der Verarbeitung solcher Daten ist der Kunde verantwortlich; unterliegen Postfächer einem Berufsgeheimnis (§ 203 StGB), stellt der Kunde sicher, dass die Beauftragung zulässig ist.

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO · Stand 04.09.2026 · Dieses Dokument wird auf Anfrage auch eigenständig bereitgestellt.

Boxmove wird vollständig in der Cloud-Infrastruktur von Amazon Web Services in der Region Frankfurt am Main (eu-central-1) betrieben; dreifachDigital unterhält keine eigenen Server. Die Infrastruktur wird als Code (Terraform) verwaltet und ist dadurch dokumentiert, versioniert und reproduzierbar. Der Dienst läuft auf einer virtuellen Maschine (Amazon EC2) mit verschlüsseltem Datenträger (Amazon EBS), einer Datenbank (SQLite) und einem Objektspeicher (Amazon S3) für Zwischenlager und Sicherungen.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

- Betrieb ausschließlich in AWS-Rechenzentren mit zertifizierter physischer Sicherheit (u. a. ISO 27001, SOC 1–3): Zutrittskontrollsysteme, Überwachung, Sicherheitspersonal.
- Arbeitsplatzgeräte der Mitarbeiter mit Festplattenverschlüsselung, Bildschirmsperre und individueller Anmeldung.

1.2 Zugangskontrolle

- Individuelle Benutzerkonten; Anmeldung ohne Passwort über einen einmaligen, 15 Minuten gültigen Anmelde-Link an die hinterlegte E-Mail-Adresse oder über das Microsoft-Konto des Nutzers (OpenID Connect mit PKCE). Konten entstehen nur durch Einladung des Kontoinhabers; eine Microsoft-Anmeldung legt nie ein Konto an.
- Ein Notfallzugang mit Passwort besteht nur für den Betreiber (mindestens zwölf Zeichen, nicht für Kunden).
- Sitzungen über signierte, nur per HTTPS übertragene Cookies. Anmeldeversuche sind ratenlimitiert (20 je 15 Minuten und Adresse), Anmelde-Links auf fünf Anforderungen je Adresse begrenzt.
- Administrativer Zugang zur Cloud-Infrastruktur ausschließlich über zentrales Single Sign-on mit Multi-Faktor-Authentifizierung; Zugriff auf die Instanz nur über AWS Systems Manager, kein offener SSH-Zugang; Metadatendienst der Instanz nur mit Token (IMDSv2).

1.3 Zugriffskontrolle

- Rollen im Kundenkonto (Inhaber, Mitarbeiter); Löschung des Zwischenlagers nur durch den Inhaber mit Bestätigung.
- Mitarbeiter von dreifachDigital greifen nicht auf Nachrichteninhalte zu; Fehlersuche erfolgt anhand von Protokollen, die keine Inhalte enthalten.
- Support-Zugriffe nur anlassbezogen über eine lesende Support-Sitzung, die vom Betreibersystem mit einem 60 Sekunden gültigen Einmal-Link eröffnet wird, 60 Minuten gilt und im Audit-Protokoll erscheint.
- Zugriff der Anwendung auf den Objektspeicher über die Instanzrolle mit minimalen Rechten; kein öffentlicher Zugriff auf Speicher (Public Access Block), Zugriff auf den Lager-Bucket nur über TLS

(Bucket-Richtlinie).

1.4 Trennungskontrolle

- Logische Mandantentrennung: jede Datenbankabfrage ist an das Kundenkonto gebunden und wird serverseitig autorisiert; Zwischenlager-Objekte liegen unter einem Pfad je Kunde und Postfach.
- Zugangsdaten werden mit einem Schlüssel je Kundenkonto verschlüsselt (siehe 1.5); Daten eines Kunden lassen sich mit dem Schlüssel eines anderen nicht entschlüsseln.
- Getrennte Umgebungen für Produktion und Staging mit eigener Datenbank, eigenen Schlüsseln und eigenem Speicherbereich; Produktivdaten werden nicht in Entwicklungs- oder Testumgebungen verwendet.

1.5 Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung (TLS) auf allen Verbindungen: zum Dienst (HTTPS mit HSTS), zu Quell- und Zielsystemen (IMAPS, EWS/Graph über HTTPS), zum Objektspeicher und zum E-Mail-Versand.
- Verschlüsselung gespeicherter Daten: Datenträger der Instanz (EBS), Zwischenlager und Sicherungen (S3, serverseitige Verschlüsselung AES-256).
- Zugangsdaten der Postfächer (Passwörter, OAuth-Token) werden zusätzlich anwendungsseitig mit AES-256-GCM verschlüsselt; der Schlüssel wird je Kundenkonto aus einem Hauptschlüssel und einem kontospezifischen Salt abgeleitet. Der Hauptschlüssel liegt nicht in der Datenbank, sondern in der Umgebung der Anwendung (AWS Systems Manager Parameter Store, verschlüsselt).
- Passwörter, die Postfachinhaber über den persönlichen Link eingeben, werden sofort gegen das Postfach geprüft, verschlüsselt gespeichert und nie im Klartext protokolliert.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Postfachinhalte werden ausschließlich an das vom Kunden benannte Zielsystem übertragen; es gibt keine Exportfunktion an Dritte und keine Weitergabe von Inhalten an das Betreibersystem (CRM) – dieses erhält nur Kundenstammdaten, Mengen und Belegung.
- Verbindungen zu Mailservern mit privaten oder internen Adressen werden in der Produktion abgelehnt (Schutz gegen Server-Side Request Forgery).
- Formularanfragen werden auf ihre Herkunft geprüft (Origin-Prüfung); Content-Security-Policy ohne Inline-Skripte.
- Ratenbegrenzung auf öffentlichen Endpunkten (persönliche Passwort-Links, Anmeldung, Support-Links, OAuth-Rücksprung: 60 Anfragen je 15 Minuten) und auf der Service-Schnittstelle des Betreibersystems (300 je Minute, Token mit konstantzeitigem Vergleich).
- Persönliche Links für Postfachinhaber und Einladungen sind kryptografisch zufällig, zeitlich begrenzt (15 Minuten bzw. 14 Tage) und einmalig einlösbar.

2.2 Eingabekontrolle

- Audit-Protokoll über sicherheits- und datenschutzrelevante Aktionen (Nutzer, Zeitpunkt, Aktion, Kundenkonto): Anlegen und Löschen von Umzügen, Postfächern und Zwischenlagern, Zugangsdaten, Läufe, Support-Sitzungen, Sperren.
- Jeder Lauf wird je Postfach protokolliert (Zeitpunkte, Ordner, Anzahl, Fehler); kopierte Termine und Kontakte werden je Element vermerkt, damit Delta-Läufe nichts doppelt anlegen.

- Serverseitige Validierung sämtlicher Eingaben gegen definierte Schemata; die Konfiguration des Servers wird beim Start geprüft, ein unvollständig konfigurierter Server startet nicht.
- Schreibende Aufrufe des Betreibersystems tragen einen Idempotenz-Schlüssel; wiederholte Aufrufe haben keine Seiteneffekte.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Tägliche konsistente Sicherung der Datenbank (Steuerungsdaten, Index des Zwischenlagers, verschlüsselte Zugangsdaten) in einen versionierten, verschlüsselten S3-Bucket in Frankfurt mit 90 Tagen Vorhaltung. Postfachinhalte verbleiben im Quellsystem und liegen nach dem Umzug im Zielsystem; das Zwischenlager ist nicht Teil der Sicherung und keine Datensicherung im Sinne eines Backups (Hauptvertrag Ziffer 6.3).
- Boxmove kopiert nur und löscht nie im Quellsystem; ein abgebrochener Lauf kann jederzeit wiederholt werden, bereits kopierte Elemente werden erkannt.
- Läufe werden in einer Warteschlange mit begrenzter Parallelität verarbeitet; bei Fehlern werden reservierte Leistungen freigegeben.
- Infrastruktur als Code ermöglicht den reproduzierbaren Wiederaufbau der Umgebung; feste IP-Adresse, automatische TLS-Zertifikate.
- Statusendpunkt für die Überwachung der Erreichbarkeit; Protokolle der Anwendung auf der Instanz.

4. Löschung und Aufbewahrung

- Zugangsdaten der Postfächer werden mit dem Abschluss des Umzugs (letzter Lauf) automatisch aus der Datenbank entfernt.
- Zwischenlager: Erinnerung 7 Tage und 1 Tag vor Ablauf, nach Ablauf 30 Tage Karenz (gesperrt, keine Läufe), danach automatische Löschung der Objekte mit Audit-Eintrag und Benachrichtigung; sofortige Löschung durch den Inhaber jederzeit möglich. Unvollständige Uploads werden nach 3 Tagen verworfen.
- Umzüge und Kundenkonten können vom Kunden gelöscht werden; mit der Schließung des Kontos werden Zugangsdaten, Zwischenlager und Umzugsdaten gelöscht; Sicherungen laufen nach 90 Tagen aus.

5. Regelmäßige Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Dokumentierter Prozess für Sicherheitsvorfälle einschließlich Meldung an betroffene Kunden (§ 9 des Vertrags, spätestens 48 Stunden nach Kenntnis).
- Auftragskontrolle: mit allen Subunternehmern bestehen Auftragsverarbeitungsverträge; regelmäßige Überprüfung der Liste und der Garantien (Subunternehmer-Liste, Anlage 3).
- Privacy by Design/Default: Region Frankfurt fest konfiguriert; keine KI-Auswertung, keine Analyse-Werkzeuge, keine Inhalte in Protokollen; das Zwischenlager ist nur nutzbar, wenn es ausdrücklich konfiguriert ist.
- Qualitätssicherung über Typprüfung, automatisierte Tests und Code-Reviews vor jeder Auslieferung; regelmäßige Aktualisierung der eingesetzten Komponenten und des Betriebssystems der Instanz.

6. Datenschutzorganisation

- Ein Datenschutzbeauftragter ist nach § 38 BDSG nicht zu benennen; die Datenschutzkoordination liegt bei der Geschäftsführung. Kontakt: info@dreifach-digital.de.
- Alle Mitarbeiter sind auf Vertraulichkeit und Datenschutz verpflichtet und werden entsprechend unterwiesen.
- Dokumentierte Vergabe und Entziehung von Zugängen bei Ein- und Austritt (On-/Offboarding).

Subunternehmer

Weitere Auftragsverarbeiter nach Art. 28 Abs. 2 und 4 DSGVO · Stand 04.09.2026

Teil A · Für den Betrieb des Dienstes eingesetzte Subunternehmer

UNTERNEHMEN	SITZ	LEISTUNG	VERARBEITUNGSORT · GARANTIE
Amazon Web Services EMEA SARL	Luxemburg	Cloud-Infrastruktur: virtuelle Maschine und Datenträger (EC2, EBS), Objektspeicher für Zwischenlager und Sicherungen (S3), Konfigurationsspeicher (Systems Manager), Versand von System-E-Mails über Amazon SES (Anmelde-Links, Benachrichtigungen zu Läufen und Zwischenlager)	Region Frankfurt (eu-central-1). Für etwaige Support-Fernzugriffe: EU-US Data Privacy Framework und EU-Standardvertragsklauseln (AWS Data Processing Addendum)
Mollie B.V.	Amsterdam, Niederlande	Zahlungsabwicklung über das Betreibersystem der dreifachDigital GmbH; erhält ausschließlich Zahlungsdaten des Kunden (Betrag, Zahlungsart, Name, E-Mail-Adresse), keine Postfachinhalte	EU; Mollie ist für die Zahlungsabwicklung eigenständig Verantwortlicher, ergänzend Data Processing Agreement von Mollie

Teil B · Nur bei aktiver Nutzung der jeweiligen Funktion durch den Kunden

UNTERNEHMEN	SITZ	LEISTUNG · ÜBERMITTELTE DATEN	VERARBEITUNGSORT · GARANTIE
Microsoft Ireland Operations Ltd.	Dublin, Irland	Anmeldung mit Microsoft-Konto (Microsoft Entra ID): Name, E-Mail-Adresse, Kontokennung des Nutzers. Zugriff auf Microsoft 365 im Auftrag des Kunden (Microsoft Graph): Lesen und Schreiben der für den Umzug ausgewählten Postfächer über die vom Administrator des Kunden erteilte Freigabe	EU (EU Data Boundary); für Zugriffe aus Drittländern EU-US Data Privacy Framework und EU-Standardvertragsklauseln (Microsoft Products and Services Data Protection Addendum)

Für die in Teil B genannten Dienste gilt: Ohne aktive Nutzung der jeweiligen Funktion findet keine Übermittlung statt (§ 6 Abs. 2 des Vertrags). Bei Microsoft 365 als Quell- oder Zielsystem ist Microsoft zugleich Auftragsverarbeiter des Kunden aus dessen eigenem Vertrag; die Freigabe für Boxmove kann der Administrator jederzeit im Microsoft-Verwaltungsportal widerrufen.

Teil C · Keine Subunternehmer: vom Kunden bestimmte Quell- und Zielsysteme

Die folgenden Systeme werden nicht von dreifachDigital beauftragt, sondern vom Kunden als Quelle oder Ziel benannt. Sie sind daher keine Subunternehmer von dreifachDigital; maßgeblich sind die Vereinbarungen des Kunden mit dem jeweiligen Anbieter:

› UNTERNEHMEN

dreifachDigital GmbH
Bozener Straße 41
49082 Osnabrück

› KONTAKT

support@boxmove.de
hallo@dreifach-digital.de
dreifach-digital.de

› HANDELSREGISTER

Amtsgericht Osnabrück, HRB 223038
USt-IdNr. DE461724855 · St-Nr. 66/200/78072
Geschäftsführer: Raphael Pedé · Marvin Kather · Sebastian Kather

- Mailserver beliebiger Anbieter, die der Kunde per IMAP anbindet (z. B. IONOS, Strato, All-Inkl, QualityHosting),
- Hosted-Exchange-Systeme, die der Kunde per IMAP oder EWS anbindet,
- Microsoft-365-Tenants des Kunden oder seines Auftraggebers,
- das Betreibersystem der dreifachDigital GmbH (CRM) für Kundenstammdaten, Rechnungen und Zahlungen – es ist Teil des Verantwortlichen und kein Dritter.

Stand: 4. September 2026, Version 1.0 (AVV-BM-2026-09). Auftragsverarbeiter: dreifachDigital GmbH, siehe Impressum. Zugehörig: AGB, Datenschutzerklärung.

> ABSCHLUSS

Dieser Vertrag wird dem Kunden bei der Registrierung, im Kundenkonto und unter boxmove.de/avv.html bereitgestellt. Er wird mit der ersten entgeltlichen Buchung Bestandteil des Vertragsverhältnisses (Art. 28 Abs. 9 DSGVO, elektronisches Format). Auf Wunsch stellen wir eine unterzeichnete Fassung zur Verfügung.

Ort, Datum · Kunde (Verantwortlicher)

Osnabrück, Datum · dreifachDigital GmbH (Auftragsverarbeiter)

> UNTERNEHMEN

dreifachDigital GmbH
Bozener Straße 41
49082 Osnabrück

> KONTAKT

support@boxmove.de
hallo@dreifach-digital.de
dreifach-digital.de

> HANDELSREGISTER

Amtsgericht Osnabrück, HRB 223038
USt-IdNr. DE461724855 · St-Nr. 66/200/78072
Geschäftsführer: Raphael Pede · Marvin Kather ·
Sebastian Kather