› ANLAGE 2 ZUM VERTRAG ZUR AUFTRAGSVERARBEITUNG

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO für den Dienst „Boxmove“. Dieses Dokument wird auch eigenständig veröffentlicht.
Online: portal.boxmove.de/legal/tom

› DOKUMENT

TOM-BM-2026-09

› STAND

September 2026 · Version 1.0

› MARKE

Boxmove
Ein Produkt der dreifachDigital GmbH

› AUFTRAGSVERARBEITER

dreifachDigital GmbH
Bozener Straße 41 · 49082 Osnabrück

› 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).