Technisch-organisatorische Maßnahmen (TOM)

Art. 32 DSGVO · Version 2026-05-08 · gültig ab 2026-05-08

Verantwortlicher

IP Strategy UG (haftungsbeschränkt)
Niederrheinstraße 46f, 41472 Neuss
Amtsgericht Neuss, HRB 23546 · Vertreten durch Ilya Piontek

Anwendung: Immobilien Butler

1. Zweck dieses Dokuments

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) im Sinne von Art. 32 DSGVO, die der Auftragnehmer für den sicheren Betrieb der Software "Immobilien Butler" implementiert hat. Es ist Bestandteil des AVV (Anlage 1) sowie eigenständige Anlage zu den AVV-Verträgen mit allen Mandanten und dient als Nachweis zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO.

2. Bezug zum Stand der Technik

Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen sowie den Auftragsverarbeiter, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen. Da in "Immobilien Butler" personenbezogene Daten von Eigentümern und Mietern (einschließlich IBAN, SEPA-Mandatsdaten, Vertrags- und Buchungsdaten) verarbeitet werden, gilt für diese Software ein erhöhtes Schutzbedarfsniveau. Die nachfolgenden Maßnahmen orientieren sich an den Empfehlungen des BSI (Mindeststandards), an ISO/IEC 27001 sowie an den Veröffentlichungen der Aufsichtsbehörden der Länder.

3. Implementierte Maßnahmen

1. Zutrittskontrolle (physischer Zugang zu DV-Anlagen)

Kein unbefugter Zutritt zu Servern, auf denen personenbezogene Daten verarbeitet werden.

? Es werden keine eigenen Server-Räume betrieben. Hosting der Anwendung erfolgt durch Vercel Inc. (EU-Region "fra1" / Frankfurt am Main).

? Speicherung der Datenbank erfolgt durch Supabase Inc. auf AWS in Frankfurt (eu-central-1).

? Speicherung der Dokumente erfolgt durch Cloudflare, Inc. (R2-Speicher, EU-Jurisdiktion).

? Alle eingesetzten Subunternehmer sind nach ISO/IEC 27001 und/oder SOC 2 Type II zertifiziert; physische Zutrittskontrollen werden vertraglich gesichert.

? Arbeitsplätze des Auftragnehmers sind verschlüsselt (FileVault / BitLocker), gerätegebunden (MDM-fähig) und werden bei Verlust ferngelöscht.

2. Zugangskontrolle (logischer Systemzugang)

Verhinderung der Nutzung der Software durch Unbefugte.

? Anmeldung ausschließlich mit individueller E-Mail-Adresse und Passwort (keine Shared Accounts).

? Passwort-Hash gemäß bcrypt mit Cost-Factor >= 10; Klartext-Passwörter werden zu keinem Zeitpunkt persistiert oder protokolliert.

? Passwort-Mindestlänge 10 Zeichen, gemischter Zeichensatz empfohlen.

? Pflichtwechsel des Passworts bei initial vom Master-Administrator gesetzten Konten (mustChangePassword-Flag).

? Zwei-Faktor-Authentisierung (TOTP nach RFC 6238, 6-stellig, 30-Sekunden-Fenster, +/-1-Step-Toleranz) für alle Nutzer aktivierbar; Mandant-weite 2FA-Pflicht durch den Mandant-Administrator konfigurierbar.

? TOTP-Geheimnisse werden in der Datenbank ausschließlich AES-256-GCM-verschlüsselt abgelegt; der Verschlüsselungsschlüssel liegt außerhalb der Datenbank in den Vercel-Environment-Variablen.

? Wiederherstellungs-Codes (10 Stück) werden bei der 2FA-Einrichtung einmalig im Klartext angezeigt, in der Datenbank ausschließlich als sha256-Hashes gespeichert und sind nach einmaliger Verwendung verbraucht (single-use, Anti-Replay).

? 5-Versuch-Lockout über 15 Minuten für die Zwei-Faktor-Verifikation (BSI-Mindeststandard MFA, Anti-Brute-Force).

? Schutz gegen Selbstaussperrung: die Deaktivierung des eigenen 2FA ist gesperrt, wenn die Mandant-Pflicht aktiv ist.

? Brute-Force-Schutz auf der Anmelde-Route (Rate Limiting je IP/Konto).

? Session-Management: signierte HTTP-only Cookies mit SameSite=Strict, Secure-Flag.

? Automatische Abmeldung bei Inaktivität (5 / 10 / 15 / 30 / 60 Minuten oder deaktiviert), Standardwert 10 Minuten, pro Nutzer konfigurierbar; Cross-Tab-Synchronisation via localStorage-Events.

? Keine öffentliche Selbstregistrierung - Konten werden ausschließlich per Einladung durch den Master- bzw. Mandant-Administrator angelegt.

? Automatische Sperrung von Konten ausscheidender Nutzer durch den Mandant-Administrator.

3. Zugriffskontrolle (Berechtigungssteuerung)

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb der Anwendung.

? Drei-Stufen-Rollenmodell (master_admin, admin, user) mit feingranularen Permissions (z. B. property.read, beleg.review, journal.post).

? Mandantenscharfe Datenisolation: jede Datenbank-Abfrage wird auf die tenant_id des angemeldeten Nutzers eingeschränkt; durchgängige Implementierung wird durch eine Prisma-Erweiterung mit Laufzeit-Warner und schrittweise Postgres Row-Level-Security (RLS) zusätzlich abgesichert.

? Master-Administrator-Konten unterliegen verschärften Anforderungen (mandatorische 2FA, geringere Idle-Timeout-Standardwerte).

? Audit-Log aller geld-, daten- und sicherheitsrelevanten Vorgänge mit Vorher/Nachher-Werten, Nutzer-ID, IP-Adresse und Zeitstempel.

? Speicherung von Geheimnissen (API-Schlüssel, AES-Schlüssel, Tokens) ausschließlich in Vercel-Environment-Variablen - niemals im Quellcode oder Git-Repository.

? Datenschutzkonforme Vernichtung / Löschung über kaskadierende Foreign-Key-Löschungen sowie Soft-Delete-Marker, wo Aufbewahrungsfristen entgegenstehen.

4. Weitergabekontrolle (sicherer Transport)

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung.

? Sämtlicher Datenverkehr zwischen Browser, Anwendung (Vercel), Datenbank (Supabase), Dokumentenspeicher (Cloudflare R2), KI-Provider (Anthropic) und E-Mail-Provider (Resend) erfolgt ausschließlich über TLS 1.2 oder höher.

? Cloudflare R2 verschlüsselt sämtliche Objekte at-rest mit AES-256.

? Supabase verschlüsselt die Datenbank at-rest mit AES-256 und stellt automatische SSL-Verbindungen bereit.

? Dokumenten-Downloads erfolgen über zeitlich befristete, signierte URLs (Presigned URLs, TTL maximal 5 Minuten).

? E-Mail-Versand (Resend) und E-Mail-Empfang (Postmark Inbound) ausschließlich über TLS-verschlüsselte SMTP-Verbindungen.

? Outbound-Mail an Dritte (Mahnwesen, NK-Abrechnungen, Mietvertrags-Versand) erfordert immer eine explizite Freigabe-Aktion eines Nutzers - kein automatischer Massenversand ohne menschliche Prüfung.

5. Eingabekontrolle (Nachvollziehbarkeit)

Feststellung, ob und von wem personenbezogene Daten in der Anwendung eingegeben, verändert oder entfernt worden sind (Art. 5 Abs. 2 DSGVO - Rechenschaftspflicht).

? Audit-Log der Anwendung erfasst jede schreibende Aktion (insert / update / delete) mit dem auslösenden Nutzer-Konto, Tenant-ID, IP-Adresse und Zeitstempel.

? Vorher- und Nachher-Werte werden für sicherheitsrelevante Tabellen (User, Session, Tenant, Mietvertrag, Beleg, MietzahlungSoll, BankTransaction, Journal) vollständig protokolliert.

? Sicherheits-Events (auth.2fa.*, auth.mandant.2fa_policy_changed, user.totp.locked) werden mit erweiterten Metadaten (Versuchszähler, Lockout-Bis-Wann) erfasst.

? Einträge im Audit-Log sind für Mandant-Administratoren in der Anwendung einsehbar (Menüpunkt System - Audit-Log).

? Aufbewahrungsdauer Audit-Log: mindestens 12 Monate; Backups verlängern dies faktisch.

6. Verfügbarkeitskontrolle

Schutz gegen zufälligen oder mutwilligen Verlust personenbezogener Daten.

? Tägliche automatische Backups der Datenbank durch Supabase, einschließlich Point-in-Time Recovery (Wiederherstellung sekundengenau über die letzten 7 Tage).

? Cloudflare R2 speichert Dokumente mit eingebauter geo-verteilter Redundanz.

? Vercel betreibt die Anwendung mit automatischem Multi-Region-Failover.

? DDoS-Schutz und Bot-Mitigation durch Cloudflare.

? Regelmäßige Wiederherstellungstests gegen ein Restore-Environment.

? Sentry-Monitoring für Anwendungs-Fehler; SLO-Alerts bei Anstieg der Fehlerrate.

7. Trennungskontrolle (Mandantentrennung)

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

? Mandantenfähige Architektur ab Tag 1: jede Tabelle der Datenbank trägt eine tenant_id, jede Abfrage wird auf die tenant_id des Sitzungsbenutzers eingeschränkt.

? Dokumentenspeicher Cloudflare R2 verwendet pro Mandant einen eigenen Schlüsselpfad-Präfix (<tenant_id>/...).

? Postgres Row-Level Security (RLS) wird stufenweise eingeführt, um die Anwendungs-Schicht zusätzlich auf Datenbank-Ebene abzusichern.

? Eingehende Beleg-E-Mails werden über mandantenspezifische Subdomains (belege@<tenant>.immobilien-butler.com) eindeutig zugeordnet.

? Strikte logische Trennung von Test-, Staging- und Produktivumgebung - kein Datenabgleich zwischen Umgebungen.

8. Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers.

? Mit allen in Anlage 2 zur AVV genannten Subunternehmern bestehen schriftliche Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO.

? Bei Subunternehmern mit Sitz außerhalb der EU/EWR (insbesondere Anthropic für KI-gestützte Belegerkennung) erfolgt der Datentransfer auf Grundlage der EU-Standardvertragsklauseln (Durchführungsbeschluss 2021/914) sowie ergänzender technischer Maßnahmen (Zero Data Retention, kein Modelltraining mit Mandanten-Daten).

? Dokumentation aller Subunternehmer-Verträge; jährliche Überprüfung der Sicherheits-Zertifizierungen (ISO 27001, SOC 2).

? Aktualisierungen der Subunternehmer-Liste werden den Auftraggebern rechtzeitig vor dem Wirksamwerden mitgeteilt; ein Widerspruchsrecht aus berechtigtem Grund besteht.

4. Verfahren zur regelmäßigen Überprüfung

Datenschutz-Management mit dokumentierten internen Reviews mindestens einmal jährlich. Anlassbezogene Überprüfung zusätzlich bei: (a) Änderungen der Subunternehmer-Liste, (b) wesentlichen Architekturänderungen am Authentifizierungs- oder Speicher-Stack, (c) sicherheitsrelevanten Vorfällen, (d) neuen aufsichtsbehördlichen Vorgaben. Ergebnis-Dokumentation im internen Compliance-Ordner; sicherheitsrelevante Erkenntnisse fließen in eine neue TOM-Version ein und werden den Auftraggebern bei Wirksamwerden mitgeteilt.

5. Kontroll-Matrix

Mapping interner Control-IDs zu Art. 32 DSGVO, ISO/IEC 27001 und BSI-Mindeststandards.

AUTH-01 - Art. 32 Abs. 1 lit. b DSGVO - Vertraulichkeit

Passwort-Hashing (bcrypt), TOTP-Secret-Verschlüsselung at rest (AES-256-GCM), TLS 1.2+ in transit, AES-256 at-rest in DB & R2

AUTH-02 - Art. 32 Abs. 1 lit. b DSGVO - Integrität

Signierte Sessions, unveränderliches Audit-Log, Backup-Code-Hashing, Postgres-Constraints + Foreign Keys

AUTH-03 - ISO/IEC 27001 A.5.16 - Identitätsmanagement

Eindeutige User-IDs je Person, Mandant-Trennung, Lifecycle-Events im Audit-Log (invite, login, password-change, deactivate)

AUTH-04 - ISO/IEC 27001 A.5.17 - Authentifizierungsinformationen

bcrypt-Hashing, Mindest-Passwortlänge, sichere Speicherung, kein Klartext-Logging

AUTH-05 - ISO/IEC 27001 A.8.5 - Gesicherte Authentifizierung

Mehr-Faktor-Authentifizierung (TOTP), optional WebAuthn/Passkeys (Roadmap), Mandant-weite Erzwingung

AUTH-06 - BSI Mindeststandard MFA

TOTP nach RFC 6238, Backup-Codes single-use, Anti-Replay, 5-Versuch-Lockout / 15 Min

DATA-01 - Art. 32 Abs. 1 lit. a DSGVO - Pseudonymisierung & Verschlüsselung

TOTP-Secrets AES-256-GCM, DB at-rest AES-256 (Supabase), Object-Storage at-rest AES-256 (R2), TLS 1.2+ in transit

DATA-02 - Art. 32 Abs. 1 lit. c DSGVO - Wiederherstellbarkeit

Tägliche automatische Backups, Point-in-Time Recovery (7 Tage), R2 geo-verteilte Redundanz, Vercel Multi-Region-Failover

DATA-03 - Art. 32 Abs. 1 lit. d DSGVO - Wirksamkeitsprüfung

Vitest-Testabdeckung der Auth-Pfade (>200 Tests), CI-Gate bei jedem Deploy, jährliche Penetrationstest-Empfehlung

ACC-01 - Art. 5 Abs. 2 DSGVO - Rechenschaftspflicht

Audit-Log mit Vorher/Nachher-Werten für jede schreibende Aktion auf sicherheitsrelevanten Tabellen, einsehbar je Mandant

TENANT-01 - Art. 32 - Trennungsgebot

tenant_id in jeder Tabelle, Prisma-Erweiterung mit Laufzeit-Warner, schrittweise Postgres RLS, R2-Schlüsselpfad-Präfixe

SUB-01 - Art. 28 DSGVO - Auftragsverarbeitung

AVV mit jedem Subunternehmer, Liste in Anlage 2 zur AVV, jährliche Sicherheits-Audits, SCC 2021/914 für Drittland-Transfers

6. Verbleibende Risiken und kompensierende Maßnahmen

Phishing-Resistenz von TOTP

TOTP ist nicht inhärent phishing-resistent (im Gegensatz zu Passkeys). Kompensation: kurze Session-Timeouts, IP- und User-Agent-Erfassung im Audit-Log, geplante Einführung von WebAuthn/Passkeys.

Verlust des zweiten Faktors durch den Nutzer

10 Backup-Codes als Recovery-Pfad. Bei Verlust sowohl des Geräts als auch der Backup-Codes: manueller Reset durch den Mandant-Administrator nach Identitätsprüfung; Vorgang im Audit-Log dokumentiert.

Insider-Risiko durch DB-Zugriff

TOTP-Secrets sind bei reinem DB-Zugriff nicht nutzbar - der AES-Schlüssel liegt außerhalb der DB. Backup-Codes sind sha256-gehasht und nicht reversibel. Passwort-Hashes (bcrypt) sind ebenfalls nicht reversibel.

Drittlandtransfer USA (Anthropic für KI-Belegerkennung)

EU-Standardvertragsklauseln (SCC 2021/914), Zero Data Retention beim Provider, vertraglicher Verzicht auf Modelltraining mit Mandanten-Daten. Mandant kann KI-Belegerkennung deaktivieren - Ausweichpfad ist die manuelle Beleg-Erfassung.

Session-Hijacking bei kompromittiertem Endgerät

HTTP-only + SameSite=Strict + Secure Cookies, TLS 1.2+ überall, automatische Idle-Abmeldung (Standard 10 Min), IP-Erfassung im Audit-Log zur Anomalie-Erkennung.

7. Versionsstand und Pflege

2026-05-08 · 2026-05-08

Erstfassung als eigenständiges TOM-Dokument; Konsolidierung der bisher in AVV Anlage 1 gepflegten Maßnahmen mit Aufnahme der vollständigen Authentifizierungs-Maßnahmen (TOTP-Verschlüsselung at rest, Mandant-weite 2FA-Pflicht, 5-Versuch-Lockout, 10 Backup-Codes), Kontroll-Matrix zu DSGVO/ISO/BSI sowie Dokumentation verbleibender Risiken und kompensierender Maßnahmen.

Das Dokument wird mindestens jährlich sowie anlassbezogen überprüft und fortgeschrieben.