



TECHNISCHE DOKUMENTATION FÜR PRÜFER

Sicherheits- und Technikbericht

Architektur, Datenhaltung, Schutzmaßnahmen und Datenschutz des CRM ApexLead-pro.
Erstellt für IT-Abteilungen, Sicherheits- und Datenschutzbeauftragte, die den Einsatz der
Software prüfen.

2 Standorte

FRANKFURT & FALKENSTEIN

0 Drittland

FÜR CRM-DATEN

0 KI-Aufrufe

ZUR LAUFZEIT

STAND

15. Oktober 2026

DOKUMENTVERSION

1.1

PRODUKT

ApexLead-pro CRM (SaaS)

ANBIETER

ApexLead-pro, David Hörnlein-Ulrich

Alle Angaben beziehen sich auf den zum Stichtag ausgelieferten Produktionsstand.

§ Inhalt

Der Bericht ist so aufgebaut, dass die Kapitel 1 bis 3 für Entscheider genügen. Ab Kapitel 4 folgt die technische Tiefe, ab Kapitel 13 der Datenschutzteil. Kapitel 21 beantwortet die Fragen aus gängigen IT-Sicherheitsfragebögen in Kurzform, Kapitel 22 nennt die Ansprechpartner.

1	Kernaussagen auf einen Blick	2
2	Was geprüft wurde und wie	3
3	Das System in Zahlen	4
4	Architektur im Überblick	5
5	Technologie und warum sie gewählt wurde	6
6	Datenmodell und Datenbankzugriff	7
7	Mandantentrennung	8
8	Rollen und Berechtigungen	10
9	Authentifizierung und Sitzungen	11
10	Absicherung der Übertragung	15
11	Eingabeprüfung und Abwehr typischer Angriffe	16
12	Verschlüsselung gespeicherter Daten und Umgang mit Geheimnissen	18
13	Datenlandkarte: wo welche Daten liegen	19
14	Unterauftragsverarbeiter	21
15	Datenflüsse im Einzelnen	22
16	Keine Verarbeitung durch künstliche Intelligenz	24
17	Protokollierung und Nachvollziehbarkeit	25
18	Löschkonzept, Aufbewahrung und Betroffenenrechte	26
19	Betrieb, Verfügbarkeit und Notfallvorsorge	27
20	Entwicklung und Qualitätssicherung	29
21	Antworten auf die Fragen aus IT-Sicherheitsfragebögen	30
22	Ansprechpartner und weiterführende Unterlagen	32

1 Kernaussagen auf einen Blick

Wo liegen die Kundendaten?

Deutschland

Werden Daten in ein Drittland übermittelt?

Nein

Werden Kundendaten an eine KI übergeben?

Nein

ApexLead-pro ist ein gehostetes CRM für den Vertrieb und den Außendienst. Es wird als Software as a Service betrieben, also zentral vom Anbieter, ohne Installation beim Kunden. Dieser Bericht beschreibt den technischen Aufbau, die Schutzmaßnahmen und den Umgang mit personenbezogenen Daten in dem Detailgrad, den eine prüfende IT-Abteilung benötigt.

Die zehn Punkte, auf die es bei einer Prüfung ankommt

Prüfpunkt	Ist-Zustand	Kapitel
Serverstandort	Anwendung und Datenbank in Frankfurt am Main, Dateiablage und Videokonferenz in Falkenstein im Vogtland. Beide Standorte in Deutschland.	13
Mandantentrennung	Jeder Kunde ist ein eigener Mandant. Die Mandantenkennung wird serverseitig aus der Datenbank bestimmt, nicht aus dem Anmeldetoken übernommen, und in jede Abfrage eingesetzt.	7
Authentifizierung	Signiertes Sitzungstoken in einem für JavaScript unlesbaren Cookie, zusätzlicher Schutz gegen Anfragenfälschung, Passwörter nur als bcrypt-Hash.	9
Berechtigungen	Fünf Rollen, davon eine reine Leserolle, dazu Rechte je Bereich für Vertriebs- und Assistenzkonten im Vertrieb.	8
Verschlüsselung	TLS auf allen Wegen, HSTS erzwungen. Zugangsdaten verbundener Postfächer und Telefonanlagen zusätzlich mit AES-256 verschlüsselt gespeichert.	10, 12
Angriffsabwehr	Content Security Policy, Herkunftsprüfung, Ratenbegrenzung, Schutz vor SQL-Einschleusung, Skript-Einschleusung, Anfragenfälschung, Serveranfragen-Fälschung und Formel-Einschleusung in Exporten.	10, 11
Protokollierung	Getrenntes Änderungsprotokoll und Datenschutzprotokoll je Mandant, in der Anwendung einsehbar.	17
Löschung	30 Tage Schonfrist, Vorwarnung sieben Tage vorher, danach vollständige Löschung durch einen täglichen automatischen Lauf.	18
Künstliche Intelligenz	Kein Codepfad ruft ein KI-Modell auf. Es existiert kein KI-Anbieter als Unterauftragsverarbeiter.	16
Auftragsverarbeitung	Vertrag zur Auftragsverarbeitung liegt vor, Unterauftragsverarbeiter sind vollständig benannt.	14

Einordnung für Entscheider. Die Verarbeitung der eigentlichen CRM-Daten findet ausschließlich auf Servern in Deutschland statt. Dienste mit Sitz außerhalb der EU sind nur dort beteiligt, wo sie technisch unvermeidbar sind, nämlich bei der Zahlungsabwicklung und beim Zustellweg von Push-Benachrichtigungen. In beiden Fällen fließen keine CRM-Inhalte ab. Die Einzelheiten stehen in Kapitel 14.

2 Was geprüft wurde und wie

Dieser Bericht ist keine Marketingunterlage und keine Selbstauskunft aus dem Gedächtnis. Jede Aussage ist gegen den ausgelieferten Produktionsstand geprüft. Geprüft wurden:

Quelle	Was daraus entnommen wurde
Anwendungscode	Sämtliche Schnittstellen der Anwendung, die Zugriffsprüfungen, die Verschlüsselungsfunktionen und die Verarbeitungspfade.
Datenbankschema	Alle gespeicherten Felder, ihre Beziehungen und die Frage, welche Tabelle eine Mandantenkennung führt.
Betriebskonfiguration	Serverregion, Sicherheitskopfeilen, Zeitpläne der automatischen Läufe, Umgebungsvariablen dem Namen nach.
Rechtstexte	Auftragsverarbeitungsvertrag, Datenschutzerklärung und Allgemeine Geschäftsbedingungen, um technische und rechtliche Darstellung deckungsgleich zu halten.

Methodik

Die Prüfung erfolgte als vollständige Durchsicht des Quelltextes, nicht als Stichprobe. Zahlenangaben in diesem Bericht, etwa die Anzahl der Schnittstellen oder der Datenmodelle, sind ausgezählt und nicht geschätzt. Wo eine Aussage nur für die Betriebsumgebung gilt und nicht aus dem Code folgt, etwa der Tarif des Datenbankbetreibers, ist sie als Angabe des Betreibers gekennzeichnet.

Was dieser Bericht nicht ist

- Er ersetzt keinen externen Penetrationstest. Er beschreibt die umgesetzten Maßnahmen, nicht das Ergebnis eines Angriffsversuchs durch Dritte.
- Er ersetzt keine Zertifizierung. ApexLead-pro führt kein ISO-27001-Zertifikat und behauptet dies an keiner Stelle.
- Er trifft keine Aussage über Systeme, die der Kunde selbst anbindet, etwa sein eigenes Postfach oder seine Telefonanlage. Diese Abgrenzung ist in Kapitel 14 ausdrücklich beschrieben, weil sie datenschutzrechtlich entscheidend ist.

Hinweis zur Vertraulichkeit. Der Bericht nennt bewusst keine Zugangsadressen von Verwaltungsoberflächen, keine Namen von Geheimnissen mit ihren Werten und keine internen Netzdetails, die einem Angreifer nützen, ohne einem Prüfer zu helfen. Wo eine Prüfung mehr Tiefe verlangt, etwa eine vollständige Liste der technischen und organisatorischen Maßnahmen nach Artikel 32 DSGVO, wird diese auf Anfrage bereitgestellt.

3 Das System in Zahlen

Die folgenden Zahlen beschreiben den Umfang des Systems. Sie sind aus dem Produktionsstand ausgezählt und dienen der Einordnung: Es handelt sich um eine gewachsene, durchstrukturierte Anwendung, nicht um einen Prototyp.

Kennzahl	Wert	Bedeutung für die Prüfung
Zeilen Anwendungscode	168.198	Umfang der eigenen Entwicklung, ohne Fremdbibliotheken.
Schnittstellen (API-Routen)	365	Jede einzelne wurde auf ihre Zugriffsprüfung hin angesehen.
davon mit erzwungener Zugriffsprüfung	330	Kein Zugriff ohne gültige Anmeldung, Schlüssel oder Signatur.
davon bewusst öffentlich	35	Anmeldung samt zweitem Faktor und Passkey, Kontakt- und Bewerbungsformulare, öffentliche Terminbuchung. Keine dieser Routen liest fremde CRM-Daten. Siehe Kapitel 11.
Fachdienste (Service-Schicht)	79	Geschäftslogik liegt gebündelt in einer eigenen Schicht, nicht verstreut in den Schnittstellen.
Datenmodelle	104	Umfang des Datenmodells, siehe Kapitel 6.
Aufzählungstypen im Schema	75	Zustände sind im Schema festgelegt statt als freier Text gespeichert.
Datenbankmigrationen	55	Jede Schemaänderung ist versioniert und nachvollziehbar, siehe Kapitel 20.
Automatisierte Tests	33 Testdateien	Schwerpunkt auf den fehleranfälligen Bereichen Datenimport, Terminlogik, Anrufsteuerung sowie Zwei-Faktor-Authentifizierung und Passkeys.
Geplante Hintergrundläufe	8	Unter anderem die tägliche Ausführung der Löschrufen, siehe Kapitel 18.
Funktionsumfang	80+ Funktionen	Produktiv nutzbarer Stand, kein Beta-Produkt.

Reifegrad

Die Anwendung ist seit Juli 2026 zahlungspflichtig im Einsatz und wird laufend weiterentwickelt. Sicherheitsrelevante Korrekturen werden nicht gesammelt, sondern einzeln ausgeliefert. Mehrere der in diesem Bericht beschriebenen Maßnahmen sind das Ergebnis eigener Nachprüfungen, bei denen Lücken gefunden und geschlossen wurden. Zwei Beispiele, die zeigen, wie mit solchen Funden umgegangen wird:

- Die Dateiablage lieferte früher eine dauerhaft gültige Adresse je Datei aus. Wer die Adresse kannte, konnte die Datei ohne Anmeldung abrufen. Heute wird jede Datei durch eine angemeldete, mandantengeprüfte Route durchgereicht, und es existiert keine Funktion mehr, die eine dauerhafte öffentliche Adresse zurückgibt.
- Die zugesagte Löschung nach 30 Tagen war lange nur ein Datenbankfeld, das niemand auswertete. Heute läuft dafür jede Nacht ein Auftrag, der vorwarnt, anonymisiert und löscht.

4 Architektur im Überblick

ApexLead-pro ist eine Webanwendung mit klarer Schichtung. Es gibt keinen dicken Client, keine lokale Installation und keine Datenhaltung auf dem Endgerät außer dem, was der Browser für die Darstellung zwischenspeichert. Alle Verarbeitung findet auf Servern in Deutschland statt.

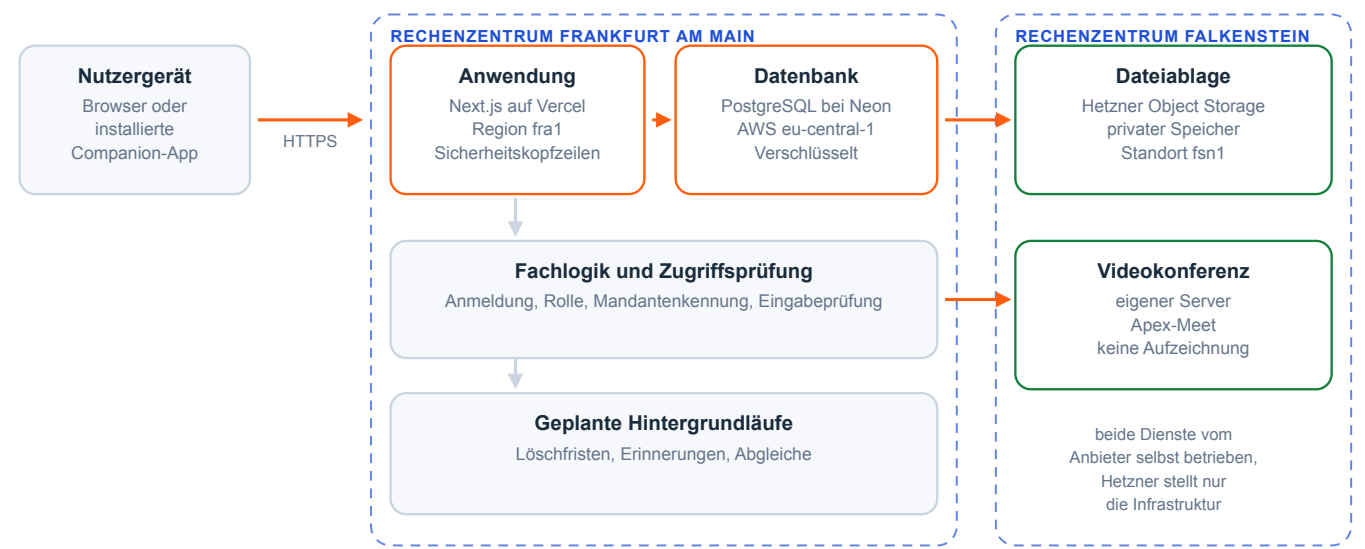


Abbildung 1: Systemübersicht mit den beiden Rechenzentrumsstandorten.

Die Schichten und ihre Aufgaben

Schicht	Aufgabe	Umsetzung
Darstellung	Oberfläche im Browser, Eingabemasken, Darstellung der Daten. Enthält keine Geschäftsregeln, die über die Anzeige hinausgehen.	React mit Next.js App Router, TypeScript, Tailwind CSS
Schnittstelle	Nimmt Anfragen entgegen, prüft Anmeldung, Rolle und Mandant, validiert die Eingabe und gibt eine einheitlich geformte Antwort zurück.	290 Routen nach einheitlichem Muster
Fachlogik	Enthält die eigentlichen Regeln, etwa die Freigabe von Angeboten oder die Berechnung von Auswertungen. Setzt die Mandantenkennung in jede Abfrage ein.	63 Dienste in einer eigenen Schicht
Datenzugriff	Übersetzt Objekte in Datenbankabfragen. Alle Abfragen sind parametrisiert, freier SQL-Text kommt nicht vor.	Prisma als objektrelationaler Abbilder
Speicherung	Dauerhafte Ablage in einer relationalen Datenbank, Dateien getrennt davon in einem privaten Objektspeicher.	PostgreSQL, S3-kompatibler Speicher

Warum diese Trennung für die Sicherheit zählt

Weil die Fachlogik in einer eigenen Schicht liegt, gibt es je Vorgang genau eine Stelle, an der die Mandantenprüfung stattfindet. Eine neue Schnittstelle kann die Prüfung nicht versehentlich auslassen, denn sie ruft den Dienst auf, der sie enthält. Läge die Logik verstreut in den einzelnen Routen, müsste jede Route für sich korrekt sein, und genau dort entstehen in der Praxis die Lücken.

Kein Zugriff an der Anwendung vorbei. Die Datenbank ist nicht aus dem Internet erreichbar, sondern nur aus der Anwendungsumgebung heraus. Der Dateispeicher ist privat, ohne öffentliche Leseberechtigung. Jede Auslieferung einer Datei durchläuft eine angemeldete Route der Anwendung, die zuvor die Mandantenzugehörigkeit prüft.

5 Technologie und warum sie gewählt wurde

Die eingesetzten Bausteine sind bewusst etablierte, breit genutzte Standardtechnologien. Für eine prüfende IT-Abteilung ist das relevant, weil Sicherheitslücken in solchen Komponenten schnell bekannt werden und ebenso schnell Korrekturen erscheinen.

Baustein	Version	Rolle und Begründung
Next.js	14.2 (App Router)	Rahmenwerk für Oberfläche und Schnittstellen in einem. Serverseitige Ausführung ist der Normalfall, wodurch Geschäftslogik und Zugangsdaten das Rechenzentrum nicht verlassen. Einzige Ausnahme ist die ausdrückliche Übernahme eines eigenen Postfachs in eine angebundene Desktop-Anwendung, siehe Kapitel 9.
TypeScript	strikt konfiguriert	Typprüfung zur Übersetzungszeit. Ganze Fehlerklassen, etwa das Vergessen eines Feldes oder ein falscher Datentyp, treten gar nicht erst zur Laufzeit auf.
React	18	Oberflächenbibliothek. Maskiert eingebettete Werte beim Rendern selbsttätig, was die Grundlast an Skript-Einschleusung deutlich senkt.
Node.js	24.x	Laufzeitumgebung, in der Projektkonfiguration festgeschrieben, damit die Produktionsumgebung nicht unbemerkt auf eine ältere Fassung zurückfällt.
PostgreSQL	16	Relationale Datenbank mit Transaktionen und Fremdschlüsseln. Mehrstufige Vorgänge werden entweder vollständig oder gar nicht ausgeführt.
Prisma	5.22	Zugriffsschicht mit generiertem, typisiertem Client. Alle Abfragen sind parametrisiert, daher ist eine SQL-Einschleusung über die normalen Zugriffswege ausgeschlossen.
Zod	4.3	Prüft eingehende Daten gegen ein festgelegtes Schema, bevor sie die Fachlogik erreichen.
bcrypt	Kostenfaktor 12	Passwort-Hashverfahren mit Zufallssalz und einstellbarem Rechenaufwand.
sanitize-html, DOMPurify	aktuell	Bereinigen HTML aus fremder Quelle, insbesondere Inhalte empfangener E-Mails, vor der Anzeige.
Stripe	API v20	Zahlungsabwicklung. Zahlungsdaten werden ausschließlich dort verarbeitet und erreichen die Anwendung nicht.

Abhängigkeiten und ihre Pflege

- Fremdbibliotheken werden über die Paketverwaltung eingebunden und mit fest hinterlegter Auflösung installiert, sodass eine Auslieferung reproduzierbar ist.
- Sicherheitsmeldungen zu eingesetzten Paketen werden ausgewertet und abgearbeitet. Eine solche Bereinigung wurde zuletzt im August 2026 vollständig durchgeführt.
- Eine bekannt verwundbare Unterabhängigkeit wird, wo nötig, über eine erzwungene Mindestversion angehoben, statt auf die Korrektur des übergeordneten Pakets zu warten.

Bewusster Verzicht. Das Produkt bindet keine Werbe- oder Analysedienste ein, kein Google Analytics, keine Tracker Dritter, keine externen Schriftarten- oder Skriptquellen zur Laufzeit. Die Reichweitenmessung der öffentlichen Website erfolgt mit einer eigenen, cookiefreien Lösung, die keine IP-Adresse speichert. Einzelheiten in Kapitel 17.

6

Datenmodell und Datenbankzugriff

Die Daten liegen in einer relationalen PostgreSQL-Datenbank. Das Schema umfasst 104 Datenmodelle und 75 Aufzählungstypen. Es ist vollständig im Quelltext beschrieben und wird über versionierte Migrationen verändert, niemals von Hand an der laufenden Datenbank.

Die wichtigsten Datenbereiche

Bereich	Enthaltene Daten
Mandant und Konten	Team, Nutzerkonten, Rollen, Einladungen, Berechtigungen, Gerätekopplungen, Zugriff über Teamgrenzen hinweg.
Vertriebsdaten	Organisationen, Ansprechpartner, Verkaufschancen, Aufgaben, Aktivitäten, Statusverläufe, Gruppen und Projekte, Vertriebsgebiete.
Tickets	Vorgänge mit Arbeitsschritten und Fristen, Nachrichten, Metadaten der Anhänge, Mitleser und ein unveränderlicher Verlauf. Die Anhänge selbst liegen im Objektspeicher, siehe Kapitel 13.
Belege	Angebote mit Positionen, Rechnungen, Verträge, Artikelkatalog, Firmenstammdaten für die Beleggestaltung.
Kommunikation	Verbundene Postfächer, abgerufene Nachrichten, Metadaten der Anhänge, Vorlagen, Signaturen, Kalendertermine und deren Abgleich.
Planung	Touren, Terminbuchungsprofile, Buchungen, Anrufsitzungen und Anruflisten.
Datenschutz und Nachweis	Änderungsprotokoll, Datenschutzprotokoll, Einwilligungen, Löschanträge, Aufbewahrungsregeln, Löschprotokoll.
Vertragsverhältnis	Abonnementstatus, Plattformrechnungen, Supportvorgänge. Getrennt von den CRM-Daten des Kunden.

Wie auf die Daten zugegriffen wird

- **Ausschließlich über die Zugriffsschicht.** Jede Abfrage geht durch den generierten Datenbankclient. Dieser setzt Werte immer als Parameter ein, nie als zusammengesetzten Text. Damit ist die klassische SQL-Einschleusung über die Anwendungswege ausgeschlossen.
- **Mehrschrittige Vorgänge in Transaktionen.** Wenn ein Vorgang mehrere Tabellen berührt, etwa das Löschen eines Mandanten oder das Zurücknehmen eines Imports, läuft er in einer Transaktion. Bricht er ab, bleibt kein halber Zustand zurück.
- **Zustände als Aufzählungstyp.** Statuswerte, Rollen und Vorgangsarten sind im Schema als Aufzählung festgelegt. Ein ungültiger Wert kann nicht in die Datenbank gelangen, auch nicht über einen Fehler in der Oberfläche.
- **Keine ungeprüften Massenoperationen.** Lösch- und Änderungsbefehle über viele Datensätze enthalten die Mandantenbedingung fest im Code und sind nicht über Parameter aus der Anfrage steuerbar.

Schemaänderungen

Jede Änderung am Datenmodell wird als Migration abgelegt, aktuell 55 Stück. Eine Migration ist eine versionierte, geprüfte Datei, die beim Ausrollen ausgeführt wird. Dadurch ist jederzeit nachvollziehbar, wann welches Feld hinzugekommen ist. Änderungen unter Umgehung dieses Wegs sind im Betriebsablauf ausgeschlossen, seit die Migrationshistorie im September 2026 vollständig instand gesetzt wurde.

7 Mandantentrennung

Dies ist für die meisten prüfenden IT-Abteilungen die wichtigste Frage: Kann ein anderer Kunde unsere Daten sehen? Die Antwort ist nein, und der folgende Abschnitt beschreibt, wodurch das sichergestellt ist.

Das Prinzip

Jeder Kunde ist ein eigener Mandant, im System Team genannt. Jeder Datensatz, der zu einem Kunden gehört, trägt dessen Mandantenkennung, entweder direkt als Feld oder über seinen übergeordneten Datensatz. Die Kennung ist kein optionales Merkmal, sondern Bestandteil des Schemas und der Abfragen.

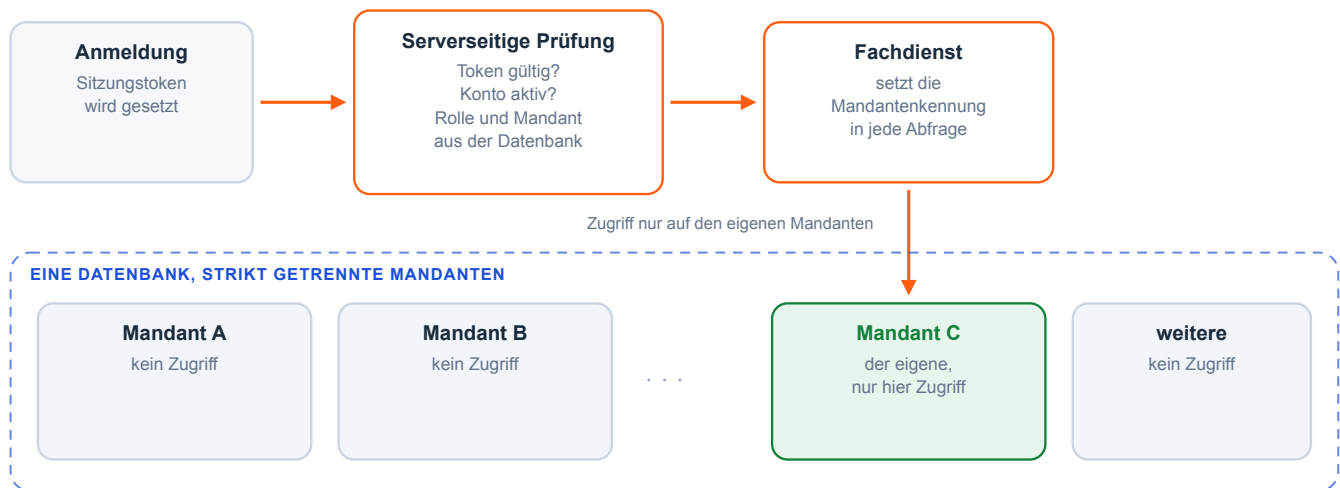


Abbildung 2: Weg einer Anfrage und Trennung der Mandanten in der Datenbank.

Die entscheidende Eigenschaft

Die Mandantenkennung stammt nicht aus dem Anmeldetoken, sondern aus der Datenbank. Bei jeder einzelnen Anfrage wird mit der Kennung des Nutzers aus dem Token ein Datenbankeintrag geladen, und Rolle sowie Mandantenzugehörigkeit werden aus diesem Eintrag übernommen. Ein manipuliertes oder veraltetes Token nützt einem Angreifer deshalb nichts: Selbst wenn es ihm gelänge, eine fremde Mandantenkennung hineinzuschreiben, würde sie nicht verwendet. Ebenso wirkt das Sperren oder Herabstufen eines Kontos sofort und nicht erst, wenn das Token abläuft.

Weitere Maßnahmen

Maßnahme	Wirkung
Prüfung in der Fachlogik	Die Dienste vergleichen die Mandantenkennung des angefragten Datensatzes mit der des Anfragenden und verweigern bei Abweichung den Zugriff, auch wenn die Kennung des Datensatzes erraten wurde.
Nicht erratbare Schlüssel	Datensätze tragen zufällig erzeugte Kennungen, keine fortlaufenden Nummern. Ein Durchprobieren fremder Datensätze scheitert bereits am fehlenden Schlüssel und zusätzlich an der Mandantenprüfung.
Gesonderte Prüfung bei Verkaufschancen	Bei Verkaufschancen wird zusätzlich geprüft, ob der Nutzer sie überhaupt sehen darf. Einfache Vertriebskonten sehen nur die ihnen zugewiesenen Datensätze, nicht alle des Mandanten.
Kontrollierter Zugriff über Mandantengrenzen	Unternehmen mit mehreren Standorten können Untermantanten führen. Ein Wechsel in einen anderen Mandanten ist nur möglich, wenn dafür ein ausdrücklicher, in der Datenbank hinterlegter Zugriffseintrag existiert und der Nutzer eine Leitungsrolle hat. Die Prüfung erfolgt serverseitig bei jeder Anfrage.
Löschung bleibt im Mandanten	Beim Löschen eines Mandanten werden ausschließlich Datensätze mit dessen Kennung entfernt. Der Vorgang läuft in einer Transaktion und ist im Löschprotokoll festgehalten.

Warum keine getrennten Datenbanken je Kunde

Die Trennung erfolgt logisch innerhalb einer Datenbank, nicht durch eine eigene Datenbank je Kunde. Das ist die übliche Bauweise für Software as a Service und hat einen sicherheitsrelevanten Vorteil: Es gibt genau einen Sicherungs-, Aktualisierungs- und Überwachungsvorgang, der für alle Mandanten gleichermaßen greift. Bei vielen getrennten Datenbanken entsteht die typische Lücke dadurch, dass eine davon bei einer Aktualisierung vergessen wird. Die Trennung selbst ist dadurch nicht schwächer, weil sie nicht an der Oberfläche, sondern in der Fachlogik und in jeder einzelnen Abfrage verankert ist.

8 Rollen und Berechtigungen

Das Berechtigungsmodell trennt zwischen der Rolle eines Kontos und den Rechten je Bereich, die die Leitung für Vertriebskonten festlegt. Die Rolle ist im Datenbankschema als Aufzählung festgelegt, die Rechte je Bereich werden je Konto gepflegt.

Rolle	Sichtbarkeit	Rechte
Leitung MASTER_USER	alle Daten des Mandanten	Vollzugriff. Verwaltet zusätzlich Abonnement, Konten, Rollen, Rechte je Bereich sowie die Sichtbarkeits- und Sicherheitsvorgaben des Mandanten.
Assistenz der Leitung MASTER_ASSISTANT_USER	alle Daten des Mandanten	Vollzugriff wie die Leitung, auch für Prüfungen und Freigaben. Abonnement, Konten, Rollen, Rechte und Vorgaben des Mandanten bleiben der Leitung vorbehalten.
Auswertung MANAGEMENT_USER	alle Daten des Mandanten	Reiner Lesezugriff. Jede verändernde Anfrage wird serverseitig abgewiesen. Ausgenommen ist nur, was das eigene Konto betrifft, etwa Passwort und zweiter Faktor.
Vertrieb STANDARD_USER	eigene Datensätze	Arbeitet mit den ihm zugewiesenen Datensätzen, je Bereich lesend oder schreibend, soweit die Leitung es erlaubt. Angebote unterliegen, sofern aktiviert, der Freigabe durch die Leitung.
Assistenz im Vertrieb STANDARD_ASSISTANT_USER	Datensätze der zugeordneten Person	Arbeitet für die zugeordnete Vertriebskraft, je Bereich soweit die Leitung es erlaubt und nie mit mehr Rechten als diese.

Die Rechte je Bereich umfassen Leads, Organisationen, Kontakte, Angebote, Rechnungen, Aufgaben, Aktivitäten, Kalender, E-Mail, Telefonie, Touren, Dateien, Import und Export sowie Verträge, jeweils getrennt nach Lesen und Schreiben.

Wie die Rechte durchgesetzt werden

- **Serverseitig, nicht in der Oberfläche.** Die Oberfläche blendet aus, was ein Konto nicht darf, aber die eigentliche Entscheidung fällt auf dem Server. Eine von Hand nachgebaute Anfrage nützt daher nichts.
- **Vor der Fachlogik.** Nur-Lesen und die Rechte je Bereich prüft dieselbe zentrale Zugangsprüfung, die jede Anfrage durchläuft, bevor die Fachlogik erreicht wird. Neue Schnittstellen sind dadurch ohne eigenes Zutun erfasst. Dasselbe gilt für den Zugang über den Apex-Mailer und über Schnittstellenschlüssel.
- **Rechte werden bei der Anfrage nachgeschlagen.** Das erteilte Recht für den betroffenen Bereich und die beabsichtigte Aktion, lesen oder schreiben, wird zum Zeitpunkt der Anfrage aus der Datenbank geprüft. Ein entzogenes Recht wirkt sofort.
- **Rollenwechsel wirkt sofort.** Da Rolle und Mandant bei jeder Anfrage aus der Datenbank gelesen werden, muss niemand auf den Ablauf einer Sitzung warten.

Das Leserecht steuert die Schnittstellen und Seiten eines Bereichs sowie die globale Suche. Kennzahlen auf der Startseite und im Reporting fassen mehrere Bereiche zusammen und sind keinem einzelnen Bereich zugeordnet.

Vier-Augen-Prinzip bei Angeboten

Der Mandant kann einstellen, dass Angebote einfacher Vertriebskonten vor dem Versand geprüft werden müssen. Ist die Einstellung aktiv, durchläuft ein Angebot die Zustände in Prüfung, freigegeben oder Korrektur erforderlich. Ein PDF-Export und ein Versand sind erst nach der Freigabe möglich. Für die prüfende Leitung wird automatisch eine Aufgabe erzeugt, damit kein Vorgang liegen bleibt. Das ist eine fachliche Kontrolle, die in Prüfungen häufig als organisatorische Maßnahme nach Artikel 32 DSGVO abgefragt wird.

Zugänge des Anbieters

Der Anbieter unterhält eine getrennte Betreiberoberfläche für Abrechnung und Support. Sie nutzt ein eigenes Anmeldeverfahren mit eigenem Geheimnis, ein eigenes Sitzungscookie und eine eigene Kontentabelle. Sie ist vollständig von den Kundenkonten getrennt, das heißt, ein Kundenkonto kann diese Oberfläche unter keinen Umständen erreichen, und ein Betreiberkonto meldet sich nicht am CRM eines Kunden an. Zugriffe des Anbieters auf Kundendaten erfolgen nur im Rahmen der Auftragsverarbeitung und auf Weisung, etwa zur Fehlerbehebung.

9 Authentifizierung und Sitzungen

Anmeldung

- Passwörter werden ausschließlich als bcrypt-Hash mit Zufallssalz und Kostenfaktor 12 gespeichert. Hashes aus früheren Beständen mit niedrigerem Kostenfaktor werden bei der nächsten erfolgreichen Anmeldung still auf den aktuellen Faktor gehoben. Im Klartext liegt ein Passwort zu keinem Zeitpunkt in der Datenbank, in einem Protokoll oder in einer Antwort der Schnittstelle.
- Bei falschen Zugangsdaten antwortet das System mit einer einheitlichen Meldung. Es wird nicht offengelegt, ob die Adresse überhaupt existiert.
- Die Anmeldung ist auf zehn Versuche je Absenderadresse in fünfzehn Minuten begrenzt. Danach folgt eine Abweisung mit Wartezeitangabe. Der Zähler liegt in der Datenbank und gilt für alle Serverinstanzen gemeinsam.
- Ein deaktiviertes Konto wird abgewiesen, ebenso ein Mandant ohne gültiges Abonnement.

Sitzung

Merkmal	Umsetzung
Verfahren	Signiertes Token nach JSON Web Token, Verfahren HS256. Beim Prüfen wird das zulässige Verfahren fest vorgegeben, damit ein Token mit abgeschwächtem oder fehlendem Signaturverfahren nicht akzeptiert wird.
Signaturgeheimnis	Wird aus der Betriebsumgebung gelesen. Die Anwendung startet den betroffenen Pfad nicht, wenn das Geheimnis fehlt oder kürzer als 32 Zeichen ist.
Ablage im Browser	Cookie mit den Merkmalen httpOnly, secure und SameSite Lax. Für JavaScript im Browser ist das Token nicht lesbar, ein Diebstahl über eingeschleusten Skriptcode scheidet damit aus.
Gültigkeit	Sieben Tage. Danach ist eine erneute Anmeldung nötig.
Widerruf	Sperren oder Löschen eines Kontos wirkt sofort, weil bei jeder Anfrage der Kontostatus aus der Datenbank geprüft wird.
Abmeldung	Löscht die Cookies serverseitig.

Schutz vor Anfragenfälschung

Zusätzlich zum Sitzungscookie wird beim Anmelden ein zweites, zufällig erzeugtes Merkmal gesetzt. Jede verändernde Anfrage, also alles außer reinem Lesen, muss diesen Wert in einer eigenen Kopfzeile mitsenden. Der Server vergleicht Kopfzeile und Cookie und weist die Anfrage ab, wenn sie nicht übereinstimmen. Eine fremde Website kann dieses Merkmal nicht auslesen und deshalb keine Aktion im Namen eines angemeldeten Nutzers auslösen.

Weitere Zugangswege und ihre Absicherung

Zugangsweg	Absicherung
Passwort zurücksetzen	Es wird ein Zufallswert mit 32 Byte erzeugt und nur dessen SHA-256-Hash gespeichert. Der Klartext erreicht ausschließlich das Postfach des Nutzers. Gültigkeit eine Stunde, Verwendung genau einmal.
Kopplung eines Smartphones	Der Kopplungscode wird ebenfalls nur als Hash gespeichert, gilt zwei Minuten und lässt sich genau einmal einlösen. Die Kopplung ist jederzeit widerrufbar.
Schnittstellenschlüssel für den Datenimport	Der Schlüssel wird nur als Hash gespeichert, angezeigt wird lediglich ein Namensanfang zur Wiedererkennung. Jeder Schlüssel ist einem Mandanten zugeordnet, trägt einen Berechtigungsumfang und lässt sich widerrufen.

Zugangsweg	Absicherung
Anmeldung einer angebundenen Desktop-Anwendung	Über den Browser nach dem Verfahren für native Anwendungen (RFC 8252) mit Proof Key for Code Exchange (PKCE). Der Nutzer meldet sich im CRM ganz normal an, einschließlich zweitem Faktor oder Passkey, und bestätigt das Gerät ausdrücklich. Daraus entsteht eine Einmal-Freigabe, zwei Minuten gültig, einmal einlösbar und nur als Hash gespeichert, die ausschließlich die Anwendung mit dem passenden geheimen Wert einlösen kann. Das Passwort des Nutzers gelangt nie in die Anwendung. Der dabei ausgestellte Gerätezugang wird nur als Hash gespeichert, gilt ausschließlich für Termine, Aufgaben, Tickets, Ansprechpartner, die Übergabe einzelner E-Mails zum Anlegen von Datensätzen, E-Mails mit im CRM hinterlegten Kontakten (zuerst nur Absender, Empfänger und Kennung; vollständig nur bei Treffer, ohne Anhang-Inhalte), E-Mail-Vorlagen, die eigenen Signaturen und Postfächer sowie die Auswahl verknüpfter Organisationen, jeweils mit den Rechten und der Sichtbarkeit des Nutzers, und wird von allen anderen Schnittstellen abgewiesen. Er erlischt bei Abmeldung im CRM oder in der Anwendung, bei Passwortänderung, beim Zurücksetzen des zweiten Faktors, bei deaktiviertem Konto und nach 90 Tagen ohne Nutzung. Ist das Abonnement des Mandanten gesperrt, weist das CRM jede Anfrage der Anwendung ab wie im CRM selbst. Die Anwendung ist ohne gültige Anmeldung insgesamt gesperrt und arbeitet ohne Verbindung höchstens sieben Tage nach der letzten Bestätigung weiter.
Übernahme eines Postfachs in die Desktop-Anwendung	Der einzige Weg, auf dem ein gespeichertes Postfach-Passwort das CRM verlässt. Nur für die eigenen, über IMAP und SMTP verbundenen Postfächer des Nutzers, nur auf ausdrücklichen Abruf eines einzelnen Postfachs, nie in einer Liste, über TLS und ohne Zwischenspeicherung der Antwort. Höchstens zehn Abrufe je Stunde und Nutzer, jeder Abruf steht im Änderungsprotokoll des Mandanten. Mit Google oder Microsoft angemeldete Postfächer sind ausgeschlossen, deren Zugang bleibt im CRM.
Geplante Hintergrundläufe	Werden nur ausgeführt, wenn die Anfrage das hinterlegte Geheimnis mitführt. Ein Aufruf von außen ohne dieses Geheimnis wird abgewiesen.
Zahlungsdienst	Eingehende Meldungen des Zahlungsdienstleisters werden anhand ihrer kryptografischen Signatur geprüft, bevor sie verarbeitet werden.
Videokonferenz	Der Zugang wird über ein kurzlebiges, serverseitig ausgestelltes Token geregelt und ist mengenmäßig begrenzt.
Meldungen des Konferenzservers	Der eigene Konferenzserver kann den Betreiber über eine Schnittstelle des CRM auf Störungen hinweisen. Sie nimmt nur Anfragen an, die das hinterlegte Geheimnis mitführen, und verschickt dann eine Nachricht an eine fest eingestellte Adresse des Betreibers. Der Aufrufer bestimmt nur den Text, nicht den Empfänger. Daten von Mandanten werden dabei weder gelesen noch übertragen.
Anmeldung mit Passkey	Die Aufgabe wird serverseitig abgelegt und beim Einlösen gelöscht, gilt also genau einmal. Geprüft werden Signatur, Herkunft der Anfrage, Bindung an die Domain und die erfolgte Freigabe durch den Nutzer.
Zweiter Faktor zurücksetzen	Der Notweg erzeugt einen Zufallswert mit 32 Byte, von dem nur der SHA-256-Hash gespeichert wird. Der Link wird erst nach 24 Stunden gültig, verfällt nach 72 Stunden und ist genau einmal verwendbar. Alle Master-Nutzer des Mandanten werden sofort benachrichtigt.

Zwei-Faktor-Authentifizierung

Jedes Nutzerkonto kann in den Einstellungen mit einem zweiten Faktor abgesichert werden. Verwendet wird das zeitbasierte Einmalkennwort nach RFC 6238, also das Verfahren, das jede gängige Authenticator-App beherrscht (Passwörter-App unter iOS, Google Authenticator, Microsoft Authenticator, 1Password, Bitwarden und andere). Ein Master-Nutzer kann den zweiten Faktor für sein gesamtes Team verpflichtend machen; Mitglieder ohne eingerichteten Faktor erreichen dann ausschließlich die Einrichtungsseite.

Keine Weitergabe an Dritte. Es ist kein SMS-Versand und kein externer Authentifizierungsdienst beteiligt. Es wird keine Telefonnummer erhoben. Die Prüfung ist eine reine Berechnung auf dem eigenen Server in Frankfurt am Main. Für die Zwei-Faktor-Authentifizierung entsteht daher kein zusätzlicher Unterauftragsverarbeiter (siehe Kapitel 14).

Eigenschaft	Umsetzung
Verfahren	Zeitbasiertes Einmalkennwort nach RFC 6238 auf Basis von RFC 4226. Eigene Umsetzung ohne Fremdbibliothek, aufbauend auf den kryptografischen Grundfunktionen der Laufzeitumgebung. Die Normgerechtigkeit ist durch die offiziellen Testvektoren der beiden Normen automatisiert belegt.

Eigenschaft	Umsetzung
Geheimnis	20 Byte aus dem kryptografischen Zufallsgenerator. Gespeichert wird es ausschließlich authentifiziert verschlüsselt (AES-256-GCM) mit einem je Verwendungszweck abgeleiteten Schlüssel. Es wird zu keinem Zeitpunkt im Klartext abgelegt.
Zeitfenster	30 Sekunden, Toleranz von genau einem Schritt nach vorn und hinten. Ein eingelöster Zeitschritt wird festgehalten und abgewiesen, ein abgefangener Code lässt sich innerhalb seiner Restgültigkeit also nicht erneut verwenden.
Ablauf der Anmeldung	Zweistufig. Nach korrektem Passwort wird bei aktivem zweitem Faktor keine Sitzung ausgestellt, sondern ein Zwischennachweis mit fünf Minuten Gültigkeit und eigenem Verwendungszweck. Er ist mit einem eigens abgeleiteten Schlüssel signiert und kann technisch nicht als Sitzung verwendet werden.
Missbrauchsschutz	Eigene, kontobezogene Begrenzung auf den zweiten Schritt: fünf Fehlversuche je Konto in 15 Minuten, danach Sperre für 15 Minuten. Der Zähler liegt in der Datenbank und nicht im Arbeitsspeicher, damit er sich nicht durch gleichzeitige Anfragen an mehrere Instanzen umgehen lässt.
Wiederherstellungscodes	Zehn Stück, einmalig angezeigt, gespeichert ausschließlich als SHA-256-Hash. Jeder Code ist genau einmal einlösbar; die Einmaligkeit wird von der Datenbank erzwungen und nicht von der Anwendung angenommen.
Vertrauenswürdige Geräte	Optional kann ein Gerät für 30 Tage gemerkt werden. Gespeichert werden nur der Hash des Merkmals und eine grobe Bezeichnung aus der Browserkennung, bewusst ohne IP-Adresse. Jederzeit einzeln widerrufbar.
Aussperrung	Ein Master-Nutzer kann den zweiten Faktor eines Teammitglieds zurücksetzen; der Vorgang wird im Änderungsprotokoll festgehalten und die betroffene Person per E-Mail informiert. Für den Fall, dass kein Master mehr einspringen kann, existiert ein Notweg per E-Mail, dessen Link erst nach 24 Stunden gültig wird und über den alle Master-Nutzer sofort benachrichtigt werden.
Dauerhafte Zugänge	Eine neue Gerätekopplung und ein neuer Schnittstellenschlüssel entstehen nur aus einer Sitzung, die den zweiten Faktor bestanden hat. Beide gelten anschließend ohne zweiten Faktor und dürfen deshalb nicht aus einer ungeprüften Sitzung hervorgehen.

Passkeys

Gleichwertig und wahlweise steht die Anmeldung mit einem Passkey nach dem Standard WebAuthn zur Verfügung. Ein Passkey ist kein zweiter Faktor neben dem Passwort, sondern ersetzt Passwort und Einmalkennwort zusammen: Er vereint den Besitz des Geräts und die Freigabe durch Biometrie oder Geräte-PIN. Ein Nutzer kann jederzeit zwischen beiden Verfahren wechseln oder beide parallel führen; das System lässt jedoch nicht zu, dass der letzte verbleibende Schutz eines Kontos entfernt wird.

Warum ein Passkey dem Einmalkennwort überlegen ist. Der Browser bindet ihn an die Domain und bietet ihn auf einer nachgebauten Anmeldeseite gar nicht erst an. Damit ist der häufigste erfolgreiche Angriff auf Zugangsdaten, das Abfischen über eine gefälschte Seite, konstruktiv ausgeschlossen. Ein abgelesenes sechsstelliges Kennwort lässt sich dagegen auf jeder Seite eingeben und vom Angreifer unmittelbar weiterverwenden.

Eigenschaft	Umsetzung
Standard	WebAuthn beziehungsweise FIDO2. Die Prüfung der Signaturen übernimmt eine etablierte, gepflegte Umsetzung; sie ist bewusst nicht selbst entwickelt, weil hier nicht ein Algorithmus zu rechnen, sondern ein Protokoll mit zahlreichen Prüfschritten abzunehmen ist.
Schlüsselmateriale	Der private Schlüssel verlässt das Gerät des Nutzers nie und ist für den Betreiber grundsätzlich nicht erreichbar. Gespeichert wird ausschließlich der öffentliche Teil, mit dem sich allein keine Anmeldung durchführen lässt.
Freigabe	Zwingend mit Nutzerprüfung (Biometrie oder Geräte-PIN). Ohne diese Vorgabe wäre der Passkey ein reiner Besitznachweis und kein vollwertiger Ersatz für Passwort und Einmalkennwort.
Bindung an die Domain	Die Kennung der vertrauenden Partei lautet auf die registrierbare Domain, nicht auf einen einzelnen Host. Die zulässigen Herkünfte sind serverseitig fest vorgegeben und werden bei jeder Anmeldung geprüft.
Einmal-Aufgaben	Jede Registrierung und Anmeldung erhält eine serverseitig abgelegte Aufgabe, die beim Einlösen gelöscht wird. Eine abgefangene Antwort wirkt daher genau einmal. Gültigkeit fünf Minuten.
Mehrere Geräte	Ein Nutzer kann beliebig viele Passkeys hinterlegen, benennen und einzeln widerrufen. Ob ein Schlüssel vom Betriebssystem auf weitere Geräte synchronisiert wird, wird angezeigt; bei einem nicht synchronisierten Schlüssel weist das System ausdrücklich auf den fehlenden zweiten Weg hin.
Aussperrung	Dieselben Wege wie beim Einmalkennwort: Wiederherstellungscodes, Zurücksetzen durch einen Master-Nutzer mit Eintrag im Änderungsprotokoll, ersatzweise der Notweg mit Wartefrist. Beim Zurücksetzen werden auch die Passkeys entfernt, da der Zugang sonst weiterhin als stark gesichert gälte und der Nutzer trotz Zurücksetzung ausgesperrt bliebe.

Betreiberseite. Sämtliche Betreiberkonten der eingesetzten Infrastruktur, also Hosting, Datenbank, Quellcodeverwaltung, Zahlungsdienst und Rechenzentrum, sind ebenfalls mit Zwei-Faktor-Authentifizierung geschützt. Damit ist auch der Weg abgesichert, über den ein Angreifer an die Daten aller Mandanten gelangen könnte.

10 Absicherung der Übertragung

Verschlüsselte Verbindungen

- Die Anwendung ist ausschließlich über HTTPS erreichbar. Die Verschlüsselung endet nicht vor dem Rechenzentrum, sondern erst an der Anwendung.
- Die Verbindung zur Datenbank ist verschlüsselt und läuft nicht über das offene Internet, sondern innerhalb der Umgebung des Datenbankbetreibers.
- Die Verbindung zum Dateispeicher erfolgt verschlüsselt über HTTPS mit signierten Anfragen.
- Videogespräche werden mit DTLS-SRTP verschlüsselt übertragen, die Steuerverbindung über TLS.

Erzwungene Sicherheitskopfeilen

Für jede ausgelieferte Seite setzt die Anwendung die folgenden Kopfeilen. Sie sind in der Konfiguration hinterlegt und gelten damit ausnahmslos, nicht nur für einzelne Seiten.

Kopfzeile	Wert	Wirkung
Strict-Transport-Security	zwei Jahre, inklusive Unterdomänen, zur Vorabaufnahme angemeldet	Der Browser verbindet sich künftig nur noch verschlüsselt, auch wenn ein Angreifer eine unverschlüsselte Adresse unterschreibt.
Content-Security-Policy	eigene Herkunft, eng gefasste Ausnahmen	Der Browser lädt Skripte, Stile, Bilder und Verbindungsziele nur aus den ausdrücklich erlaubten Quellen. Eingeschleuster Fremdcode findet kein Ziel, an das er Daten senden könnte.
frame-ancestors, X-Frame-Options	keine Einbettung erlaubt	Die Anwendung kann nicht in eine fremde Seite eingebettet werden. Angriffe durch untergeschobene Klickflächen scheiden aus.
X-Content-Type-Options	nosniff	Der Browser interpretiert Inhalte genau als das, was der Server angibt, und errät den Typ nicht.
Referrer-Policy	strict-origin-when-cross-origin	Beim Wechsel auf eine fremde Seite wird kein vollständiger Pfad übermittelt, der Rückschlüsse auf Datensätze zuließe.
Permissions-Policy	Kamera und Mikrofon nur für die eigene Anwendung, Standort gesperrt	Kamera wird für das Einlesen des Kopplungs-codes, Mikrofon für Telefonie und Videokonferenz benötigt. Der Standort wird nirgends abgefragt und ist deshalb vollständig gesperrt.

Herkunftsprüfung der Schnittstellen

Anfragen an die Schnittstellen werden nur von den eigenen Adressen des Produkts angenommen. Die Prüfung erfolgt gegen eine feste Liste zulässiger Herkünfte, nicht über eine pauschale Freigabe für alle. Eine fremde Website kann die Schnittstellen im Browser eines angemeldeten Nutzers damit nicht ansprechen.

Was ausdrücklich zugelassen ist und warum

Ein Prüfer wird in der Sicherheitsrichtlinie drei Ausnahmen finden. Sie sind bewusst gesetzt und hier vollständig erklärt:

- **Der eigene Konferenzserver** ist als Skript-, Rahmen- und Verbindungsziel freigegeben. Er läuft unter einer eigenen Unterdomäne auf eigener Infrastruktur in Falkenstein.
- **Microsoft und Google** sind als Verbindungsziele freigegeben, damit der Abgleich mit einem vom Kunden selbst verbundenen Postfach oder Kalender funktioniert. Ohne eine solche Verbindung wird kein Kontakt aufgebaut.
- **Eingebettete Stile und die Auswertung von Ausdrücken** sind zugelassen, weil die eingesetzte Diagrammbibliothek und das Rahmenwerk dies benötigen. Diese Zulassung bezieht sich ausschließlich auf die eigene Herkunft; fremde Skriptquellen bleiben ausgeschlossen.

11 Eingabeprüfung und Abwehr typischer Angriffe

Die folgende Tabelle ordnet die verbreiteten Angriffsklassen der jeweils umgesetzten Maßnahme zu. Die Reihenfolge folgt den gängigen Prüflisten für Webanwendungen.

Angriffsklasse	Status	Maßnahme
SQL-Einschleusung	abgedeckt	Alle Abfragen laufen über die parametrisierende Zugriffsschicht. Zusammengesetzter SQL-Text aus Nutzereingaben kommt nicht vor.
Skript-Einschleusung	abgedeckt	Die Oberflächenbibliothek maskiert eingebettete Werte selbsttätig. HTML aus fremder Quelle, insbesondere aus empfangenen E-Mails, wird vor der Anzeige bereinigt. Zusätzlich greift die Sicherheitsrichtlinie des Browsers.
Anfragenfälschung	abgedeckt	Doppeltes Merkmal aus Cookie und Kopfzeile bei jeder verändernden Anfrage, zusätzlich SameSite am Sitzungscookie.
Fehlende Zugriffskontrolle	abgedeckt	Zugriffsprüfung als Umhüllung jeder Route, Mandantenprüfung in der Fachlogik, Rollen- und Berechtsrechteprüfung serverseitig vor der Fachlogik.
Unsichere Direktverweise auf Objekte	abgedeckt	Zufällige Schlüssel statt fortlaufender Nummern, zusätzlich Mandantenprüfung bei jedem Zugriff.
Servieranfragen-Fälschung	abgedeckt	Der Bildabruf für empfangene E-Mails ist der einzige Pfad, auf dem der Server eine vom Nutzer beeinflusste Adresse abrufen. Dafür existiert eine eigene Prüfung, die Loopback, alle privaten Netze, den Übergangsbereich der Netzbetreiber, Multicast und insbesondere die Metadatenadresse der Cloudanbieter blockiert, und zwar für IPv4 und IPv6 einschließlich eingebetteter Adressen. Diese Prüfung ist durch automatisierte Tests abgedeckt.
Formel-Einschleusung in Exporten	abgedeckt	Werte, die in einer Tabellenkalkulation als Formel gelesen würden, werden beim Export maskiert und erscheinen als Text.
Gefährliche Dateiverarbeitung	abgedeckt	Für vom Kunden hochgeladene Belegvorlagen gibt es einen abgeschotteten Ausgabeweg: JavaScript ist abgeschaltet, alle Netzabrufe der Seite werden unterbunden, nur ausdrücklich freigegebene lokale Dateien dürfen geladen werden, und es gilt ein kurzes Zeitlimit.
Erraten von Zugangsdaten	abgedeckt	Ratenbegrenzung an der Anmeldung und an weiteren empfindlichen Endpunkten (zweiter Faktor, Passkeys, Gerätekopplung, Übernahme eines Postfachs). Der Zähler liegt in der Datenbank und gilt damit für alle Serverinstanzen gemeinsam; die Absenderadresse wird dafür nur als verschlüsselter Fingerabdruck gespeichert und nach Ablauf gelöscht.
Offenlegung durch Fehlermeldungen	abgedeckt	Nach außen gehen fachliche Meldungen in einheitlicher Form. Technische Einzelheiten bleiben im Serverprotokoll.
Unsichere Voreinstellungen	abgedeckt	Sicherheitskopfzeilen, Cookie-Merkmale und Rollenrechte sind in der Konfiguration bzw. im Schema festgeschrieben und nicht je Umgebung abweichend.
Veraltete Komponenten	laufend	Auswertung der Sicherheitsmeldungen zu Fremdbibliotheken, letzte vollständige Bereinigung im August 2026, bekannte verwundbare Unterabhängigkeiten werden über eine Mindestversion angehoben.

Prüfung eingehender Daten

Jede Schnittstelle prüft die empfangenen Daten gegen ein festgelegtes Schema, bevor die Fachlogik sie sieht. Geprüft werden Vorhandensein, Datentyp, Wertebereich und Format. Schlägt die Prüfung fehl, antwortet die Schnittstelle mit einer fachlichen Fehlermeldung und verarbeitet nichts.

Die öffentlich erreichbaren Schnittstellen

35 der 365 Schnittstellen sind ohne Anmeldung erreichbar. Weil ein Prüfer genau hier nachfragt, ist die Liste hier vollständig nach Zweck gegliedert:

Gruppe	Zweck und Absicherung
Anmeldung und Konto	Anmelden, Abmelden, Registrieren, Passwort vergessen und zurücksetzen, Einladung annehmen. Ratenbegrenzt, mit einmalig verwendbaren Tokens, keine Preisgabe vorhandener Konten.

Gruppe	Zweck und Absicherung
Zweiter Faktor und Passkey	Bestätigung des zweiten Schritts, Anmeldung mit Passkey sowie Anforderung und Einlösung des Notwegs. Sie sind naturgemäß ohne bestehende Sitzung erreichbar, verlangen aber alle einen Nachweis über den bestandenen ersten Schritt oder ein einmalig verwendbares Merkmal aus der bestätigten E-Mail. Eigene kontobezogene Ratenbegrenzung, siehe Kapitel 9.
Formulare der Website	Kontakt, Beratungsanfrage, Warteliste, Testzugang, Bewerbung, Angebotsanfrage, Partnerprogramm. Sie schreiben ausschließlich neue Anfragen und lesen keine bestehenden Daten.
Öffentliche Terminbuchung	Freie Zeiten anzeigen, Termin vormerken und buchen. Sichtbar ist nur, was der Kunde für seine Buchungsseite freigegeben hat. Das Ändern oder Absagen eines Termins ist nur mit einem persönlichen Einmal-Merkmal aus der Bestätigung möglich.
Abmeldung vom E-Mail-Empfang	Gesetzlich erforderlicher Abmeldeweg, erreichbar über ein Merkmal in der jeweiligen Nachricht.
Maschinelle Gegenstellen	Meldungen des Zahlungsdienstleisters und des Postfachanbieters. Beide werden anhand von Signatur bzw. hinterlegtem Geheimnis geprüft, bevor sie verarbeitet werden.
Anmeldung der Desktop-Anwendung	Tausch der im Browser bestätigten Einmal-Freigabe gegen den Gerätezugang. Die Anwendung hat hier naturgemäß noch keinen Zugang; Nachweis sind die Freigabe (zwei Minuten, einmal einlösbar) und der geheime Wert, den nur die Anwendung kennt, die die Anmeldung begonnen hat (PKCE). Zusätzlich ratenbegrenzt, siehe Kapitel 9.
Bilder in E-Mail-Signaturen	Liefert Bilder aus, die ein Nutzer für seine Signatur hinterlegt hat, damit Empfänger sie in ihrem Mailprogramm sehen. Nur Dateien aus dem Signaturordner eines Mandanten, Name ist eine zufällige Kennung, Pfad und Dateiendung werden streng geprüft. Hochgeladen werden nur geprüfte PNG-, JPEG-, GIF- oder WebP-Dateien bis 1 MB, kein SVG.
Reichweitenmessung	Nimmt einen Seitenaufruf der öffentlichen Website entgegen. Speichert keine IP-Adresse, ignoriert angemeldete Nutzer und erkannte Suchmaschinen.

Keine dieser Schnittstellen liest CRM-Daten eines Mandanten aus. Die Schnittstellen der Gerätekopplung, des Datenimports über Schlüssel und der Betreiberoberfläche erscheinen in dieser Aufstellung bewusst nicht, weil sie zwar keine Nutzeranmeldung, aber ein eigenes geprüftes Merkmal verlangen: ein Gerätetoken, einen Schlüssel oder eine Betreiberanmeldung.

12

Verschlüsselung gespeicherter Daten und Umgang mit Geheimnissen

Verschlüsselung durch die Infrastruktur

Datenbank und Dateispeicher verschlüsseln die abgelegten Daten auf Ebene des Datenträgers. Das schützt gegen den physischen Zugriff auf Speichermedien im Rechenzentrum. Diese Ebene wird von den jeweiligen Betreibern erbracht.

Zusätzliche Verschlüsselung durch die Anwendung

Für besonders empfindliche Felder verlässt sich die Anwendung nicht auf die Infrastruktur, sondern verschlüsselt selbst, bevor gespeichert wird. Betroffen ist alles, womit sich im Namen des Kunden an einem fremden System anmelden ließe:

Feld	Schutz
Zugriffs- und Erneuerungstoken verbundener Postfächer und Kalender	AES-256, eigener Zufallsvektor je Wert
Passwort eines über IMAP und SMTP verbundenen Postfachs	AES-256, eigener Zufallsvektor je Wert. Entschlüsselt wird es nur für die Verbindung zum Postfach und für die ausdrückliche Übernahme durch den Nutzer selbst, siehe Kapitel 9.
Passwort der Telefonanbindung des Softphones	AES-256, eigener Zufallsvektor je Wert

Der Schlüssel dafür liegt ausschließlich in der Betriebsumgebung und nicht in der Datenbank. Wer also nur eine Kopie der Datenbank hätte, könnte diese Felder nicht lesen. Die Anwendung verweigert den Dienst, wenn der Schlüssel fehlt oder die falsche Länge hat, statt unverschlüsselt weiterzuarbeiten.

Werte, die gar nicht erst gespeichert werden

- **Passwörter der Nutzer:** nur als bcrypt-Hash, nicht umkehrbar.
- **Zurücksetz-, Kopplungs- und Schnittstellenschlüssel:** nur als SHA-256-Hash. Der Klartext existiert einmalig bei der Ausgabe und danach nirgends im System.
- **Zahlungsdaten:** Kartennummern und Bankverbindungen werden ausschließlich beim Zahlungsdienstleister verarbeitet. Die Anwendung speichert nur dessen Kundenkennung und den Abonnementstatus.
- **Anhänge empfangener E-Mails:** Es werden nur Dateiname, Typ, Größe und die Kennung beim Postfachanbieter gespeichert. Der Inhalt wird erst beim Öffnen aus dem Postfach des Kunden geholt und nicht dauerhaft abgelegt.
- **Gesprächsinhalte und Gesprächsdauer:** werden nicht automatisch erfasst. Videogespräche werden nicht aufgezeichnet.

Verwaltung der Geheimnisse

- Geheimnisse liegen ausschließlich als Umgebungsvariablen in der Betriebsumgebung, nicht im Quelltext. Die lokalen Konfigurationsdateien sind von der Versionsverwaltung ausgeschlossen, im Quellcodebestand liegt nur eine Beispieldatei ohne Werte.
- Getrennte Geheimnisse für getrennte Zwecke: Sitzungen der Kundenkonten, Sitzungen der Betreibernoberfläche, Gerätesitzungen, Feldverschlüsselung, Hintergrundläufe, Zahlungsdienst und Konferenzserver verwenden jeweils eigene Werte. Ein kompromittiertes Geheimnis öffnet damit nicht alle Türen.
- Für Mindestlängen gibt es Prüfungen beim Start des jeweiligen Pfades statt stiller Ausweichwerte.

Warum das über den Standard hinausgeht. Viele Anwendungen speichern Zugangsdaten zu verbundenen Postfächern im Klartext oder nur schwach geschützt, weil sie zum Abrufen im Klartext benötigt werden. Hier sind sie zusätzlich zur Datenträgerverschlüsselung mit einem eigenen, außerhalb der Datenbank verwahrten Schlüssel gesichert. Der Aufwand lohnt, weil ein solcher Datensatz einem Angreifer sonst den Zugang zum gesamten E-Mail-Verkehr des Kunden eröffnen würde.

13 Datenlandkarte: wo welche Daten liegen

Die folgende Übersicht beantwortet die Frage, die in Prüfungen am häufigsten gestellt wird, für jede Datenart einzeln.

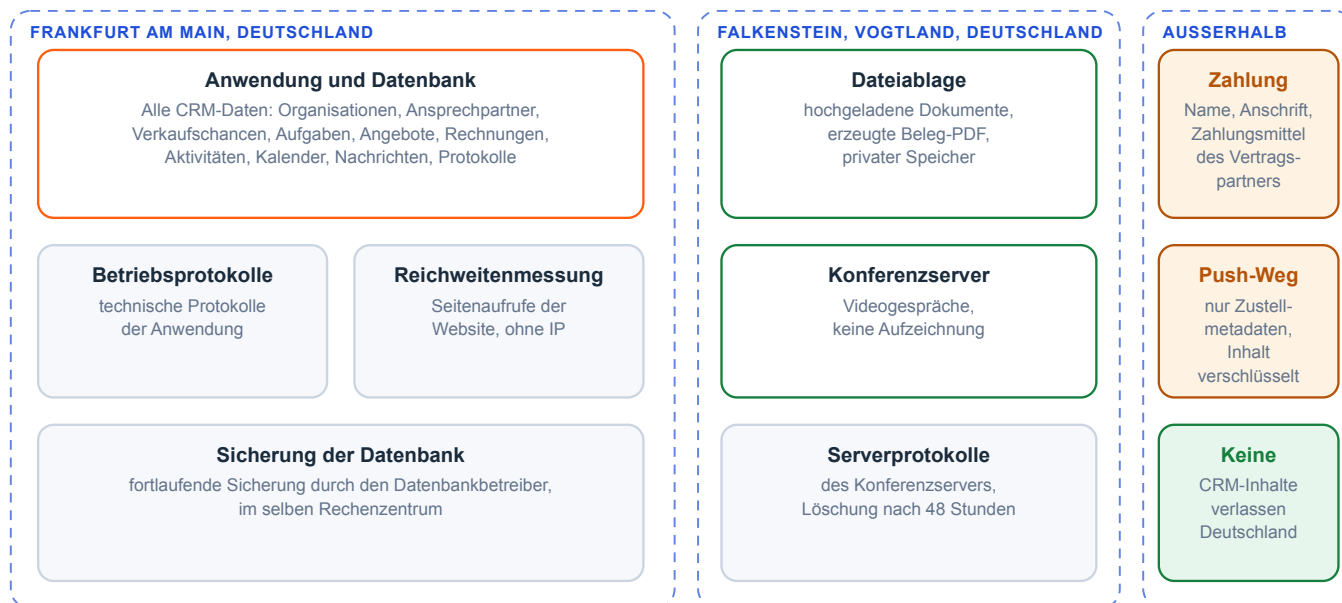


Abbildung 3: Ablageorte nach Datenart.

Datenart	Ablageort	Anmerkung
Sämtliche CRM-Stammdaten und Vorgänge	Frankfurt am Main	PostgreSQL bei Neon, AWS-Region eu-central-1. Verarbeitung durch die Anwendung in der Vercel-Region fra1, im Projekt fest eingestellt.
Nutzerkonten und Passwort-Hashes	Frankfurt am Main	Dieselbe Datenbank.
Inhalte abgerufener E-Mails	Frankfurt am Main	Nur wenn der Kunde ein Postfach verbindet (Posteingang und Gesendet-Ordner) oder die Desktop-Anwendung nutzt; aus der Desktop-Anwendung nur Mails, deren Absender oder Empfänger im CRM als Ansprechpartner oder Organisation hinterlegt ist oder deren Firmen-Domain eindeutig zu einer Organisation gehört. Anhänge werden nicht gespeichert, nur ihre Metadaten.
Hochgeladene Dokumente und erzeugte Beleg-PDF	Falkenstein im Vogtland	Privater Objektspeicher bei Hetzner, Standortkennung fsn1. Auslieferung nur über eine angemeldete Route.
Bilder in E-Mail-Signaturen	Falkenstein im Vogtland	Derselbe Objektspeicher. Öffentlich abrufbar, weil Empfänger das Bild in ihrem Mailprogramm laden, und nur das, was ein Nutzer ausdrücklich als Signaturbild hinterlegt hat.
Videogespräche	Falkenstein im Vogtland	Eigener Konferenzserver. Keine Aufzeichnung, Chatnachrichten werden nicht gespeichert, Serverprotokolle werden nach 48 Stunden gelöscht.
Sicherungen der Datenbank	Frankfurt am Main	Fortlaufende Sicherung durch den Datenbankbetreiber im selben Rechenzentrum.
Technische Protokolle der Anwendung	Frankfurt am Main	Beim Hostinganbieter, kurze Aufbewahrung, keine Ablage von CRM-Inhalten in Protokollen.
Vertrags- und Zahlungsdaten des Kunden	außerhalb der EU möglich	Betrifft die Geschäftsbeziehung zwischen Kunde und Anbieter, nicht die im CRM verwalteten Daten. Grundlage sind Standardvertragsklauseln bzw. das EU-US Data Privacy Framework.
Push-Benachrichtigungen	Zustellweg außerhalb der EU möglich	Nur Zustelladresse, Zeitpunkt und verschlüsselte Nutzlast. Der Inhalt ist für den Zustelldienst nicht lesbar. Nur bei ausdrücklich aktivierter Benachrichtigung.
Geocodierung von Anschriften	Heidelberg, Deutschland	Nur bei Nutzung von Tourenplanung oder Terminbuchung. Übermittelt wird die Geschäftsanschrift zur Umrechnung in Koordinaten.

Zusammengefasst. Die im CRM verwalteten Daten des Kunden, also der gesamte Bestand an Organisationen, Ansprechpartnern, Vorgängen, Belegen und Dokumenten, verlassen Deutschland nicht. Übermittlungen außerhalb der EU betreffen ausschließlich das Vertragsverhältnis zwischen Kunde und Anbieter sowie den technischen Zustellweg von Benachrichtigungen ohne lesbaren Inhalt.

14 Unterauftragsverarbeiter

Die folgende Liste ist deckungsgleich mit dem Vertrag zur Auftragsverarbeitung. Sie ist vollständig: Weitere Dienstleister mit Zugriff auf personenbezogene Daten werden nicht eingesetzt.

Dienstleister	Leistung	Standort der Verarbeitung	Umfang der Daten
Vercel Inc.	Betrieb der Webanwendung	Frankfurt am Main (Region fra1), Unternehmenssitz USA	Alle über die Anwendung verarbeiteten Daten während der Verarbeitung
Neon Tech, Inc.	Datenbankbetrieb	Frankfurt am Main (AWS eu-central-1)	Gesamter CRM-Datenbestand
Hetzner Online GmbH	Dateiablage und Konferenzserver	Falkenstein im Vogtland	Hochgeladene Dokumente, Beleg-PDF, Übertragung von Videogesprächen. Reine Infrastruktur, kein inhaltlicher Zugriff durch den Anbieter der Infrastruktur.
IONOS SE	Versand von System-E-Mails	Deutschland	Empfängeradresse und Inhalt der jeweiligen Nachricht
Stripe Payments Europe, Ltd.	Zahlungsabwicklung	EU, Konzernverarbeitung außerhalb der EU möglich	Vertrags- und Zahlungsdaten des Kunden, keine CRM-Inhalte
HeiGIT gGmbH	Umrechnung von Anschriften in Koordinaten, Fahrzeitberechnung	Heidelberg, Deutschland	Geschäftsanschrift, nur bei Tourenplanung oder Terminbuchung
Google LLC	Zustellweg für Benachrichtigungen an Android- und Chrome-Geräte	USA	Zustelladresse, Zeitpunkt, verschlüsselte Nutzlast. Inhalt nicht lesbar.
Apple Inc.	Zustellweg für Benachrichtigungen an Apple-Geräte	USA	wie vorstehend
Google LLC	Verbindungsaufbau für das Browser-Softphone	USA	Öffentliche IP-Adresse und Port des Nutzers. Nur bei eingerichtetem Softphone und nur, solange der Kunde keinen eigenen Server dafür hinterlegt. Diese Hinterlegung ist in den Einstellungen vorgesehen.

Abgrenzung: Dienste, die der Kunde selbst anbindet

Diese Unterscheidung ist datenschutzrechtlich entscheidend und wird in Prüfungen regelmäßig übersehen. Verbindet ein Kunde sein eigenes Postfach, seinen Kalender oder seine Telefonanlage, ist der jeweilige Anbieter kein Unterauftragsverarbeiter des CRM-Anbieters. Der Kunde wählt und beauftragt ihn selbst und unterhält dort sein eigenes Vertragsverhältnis. Das betrifft insbesondere:

- Microsoft 365 und Outlook einschließlich Microsoft Teams
- Google Workspace und Gmail einschließlich Google Meet
- Tabellendokumente als verbundene Datenquelle
- den Anbieter eines über IMAP und SMTP verbundenen Postfachs
- Automatisierungsdienste, die über die Schnittstelle Daten übermitteln
- den Telefonieanbieter des Browser-Softphones

Für diese Verbindungen gilt: Sie entstehen nur, wenn der Kunde sie einrichtet. Ohne Einrichtung baut das CRM keine Verbindung zu diesen Anbietern auf. Die datenschutzrechtliche Absicherung der eigenen Verbindung obliegt dem Kunden.

Prüfhinweis. Der Vertrag zur Auftragsverarbeitung, die Datenschutzerklärung und die Allgemeinen Geschäftsbedingungen sind öffentlich abrufbar und werden bei Änderungen an dieser Liste mitgeführt. Ein Wechsel eines Unterauftragsverarbeiters wird angekündigt.

15 Datenflüsse im Einzelnen

Alle folgenden Funktionen sind optional. Richtet ein Kunde sie nicht ein, entsteht der jeweilige Datenfluss nicht.

15.1 Anbindung eines Postfachs

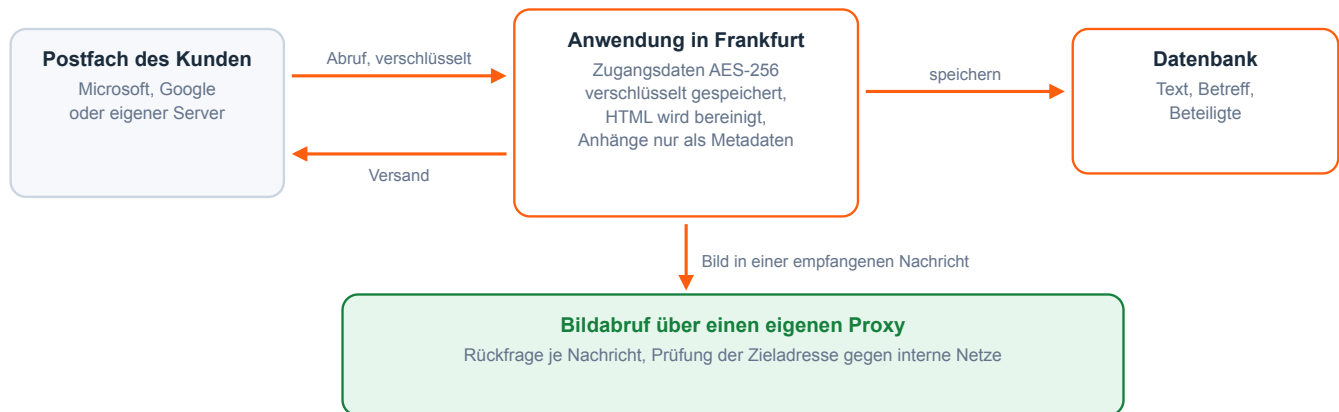


Abbildung 4: Weg einer E-Mail bei verbundenem Postfach.

- Die Verbindung erfolgt entweder über das Freigabeverfahren des Anbieters, also ohne Weitergabe des Passworts, oder über IMAP und SMTP mit Zugangsdaten, die AES-256-verschlüsselt gespeichert werden.
- Abgerufen werden Posteingang und Gesendet-Ordner. Je Ordner merkt sich das CRM, bis wohin es gelesen hat, und holt höchstens 150 Nachrichten je Lauf; der Rest folgt im nächsten Lauf. Der Abgleich läuft alle fünf Minuten und zusätzlich beim Öffnen eines Vorgangs.
- Abgerufene Nachrichten werden dem passenden Vorgang zugeordnet und in der Datenbank in Frankfurt abgelegt. Zugeordnet wird über die genaue Adresse eines Ansprechpartners oder einer Organisation, ersatzweise über die Firmen-Domain, wenn sie eindeutig zu genau einer Organisation gehört. Freemail-Domains und die eigene Domain des Kunden zählen dabei nie.
- Anhänge werden nicht gespeichert. Gespeichert werden Dateiname, Typ, Größe und die Kennung beim Anbieter; der Inhalt wird beim Öffnen frisch aus dem Postfach geholt.
- Eingebettete Bilder werden nicht ungefragt geladen. Der Nutzer entscheidet je Nachricht. Der Abruf läuft über einen eigenen Proxy mit Adressprüfung, damit weder der Absender den Empfänger nachverfolgen noch eine präparierte Adresse das interne Netz erreichen kann.
- HTML aus empfangenen Nachrichten wird vor der Anzeige bereinigt.

15.2 Telefonie



Abbildung 5: Trennung von Sprachverbindung und CRM-Daten.

Die Sprachverbindung läuft zwischen dem Browser des Nutzers und dem Telefonanbieter, den der Kunde selbst beauftragt. Das CRM ist an der Sprachverbindung nicht beteiligt und speichert weder Mitschnitte noch automatisch erfasste Gesprächsdauern. In der Datenbank landet nur, was der Nutzer als Ergebnis erfasst. Das Passwort der Telefonanbindung wird AES-256-verschlüsselt.

gespeichert. Der für den Verbindungsaufbau nötige Hilfsserver ist konfigurierbar, sodass ein Kunde mit eigener Infrastruktur auch diesen letzten externen Berührungspunkt vermeiden kann.

15.3 Dateien und Belege

- Hochgeladene Dokumente und erzeugte Beleg-PDF liegen im privaten Objektspeicher in Falkenstein.
- Der Speicher hat keine öffentliche Leseberechtigung. Es existiert keine Funktion, die eine dauerhaft gültige öffentliche Adresse ausgibt.
- Jede Auslieferung geht durch eine angemeldete Route, die zuvor die Mandantenzugehörigkeit prüft und die Datei anschließend durchreicht, statt auf den Speicher weiterzuleiten. Dadurch gelangt die Speicheradresse nicht in den Browser und kann nicht weitergegeben werden.

15.4 Videokonferenz

- Eigener Server in Falkenstein, betrieben vom Anbieter selbst. Es wird kein Dienst eines Videokonferenzanbieters genutzt.
- Verbindungen sind mit DTLS-SRTP verschlüsselt. Es wird nicht aufgezeichnet.
- Chatnachrichten zwischen den Teilnehmern laufen ausschließlich über den eigenen Server und werden weder dort noch im CRM gespeichert. Der Server hält keinen Nachrichtenverlauf vor, wer später beitrifft, sieht keine früheren Nachrichten. Nachrichtentexte erscheinen nicht in den Serverprotokollen.
- Der Server ist so eingestellt, dass er keine externen Hilfsserver kontaktiert und keine Anfragen an Dritte stellt. Diese Einstellung ist geprüft und wird nach Aktualisierungen erneut geprüft.
- Nach jeder Aktualisierung der Serversoftware prüft der Server automatisch, ob die eigenen Anpassungen noch greifen, und spielt sie bei Bedarf neu ein. Gelingt das nicht, meldet er es über eine durch ein Geheimnis geschützte Schnittstelle an den Betreiber, siehe Kapitel 9.
- Weichzeichnen oder Ersetzen des Hintergrunds wird vollständig im Browser des Teilnehmers berechnet. Das dafür nötige Modell und die mitgelieferten Hintergrundbilder kommen vom eigenen Server. Ein eigenes Hintergrundbild bleibt im Browser gespeichert und wird nicht hochgeladen.
- Raumnamen werden zufällig erzeugt und lassen keinen Rückschluss auf Anlass oder Teilnehmer zu. Serverprotokolle werden nach 48 Stunden gelöscht.

15.5 Benachrichtigungen auf das Smartphone

- Nur nach ausdrücklicher Aktivierung durch den Nutzer und nach Kopplung des Geräts.
- Der Inhalt der Benachrichtigung ist nach dem Web-Push-Verfahren verschlüsselt. Der Zustelldienst sieht die Zustelladresse und den Zeitpunkt, nicht den Inhalt.
- Die Zugangsdaten für die Zustellung werden sofort gelöscht, sobald der Nutzer die Verbindung trennt.

15.6 Datenimport und Schnittstelle

- Der Import läuft über den Assistenten in der Anwendung oder über eine Schnittstelle mit eigenem Schlüssel. Der Schlüssel ist mandantengebunden, trägt einen Berechtigungsumfang und wird nur als Hash gespeichert.
- Jeder Import wird als Vorgang festgehalten und ist innerhalb von 30 Tagen vollständig zurücknehmbar.
- Beim Export in Tabellenformate werden Werte maskiert, die sonst als Formel ausgeführt würden.

16 Keine Verarbeitung durch künstliche Intelligenz

Ruft die Anwendung zur Laufzeit ein KI-Modell auf?

Nein

Gelangen CRM-Daten zu einem KI-Anbieter?

Nein

Dienen Kundendaten dem Training von Modellen?

Nein

Diese Frage stellt inzwischen fast jede prüfende IT-Abteilung, und sie wird hier ausdrücklich beantwortet, weil die Antwort nicht selbstverständlich ist: Viele CRM-Anbieter übermitteln Inhalte an Sprachmodelle, ohne dass es dem Kunden auffällt.

Was geprüft wurde

- Die Liste der Fremdbibliotheken enthält kein Entwicklungspaket eines KI-Anbieters.
- Eine Suche über den gesamten Anwendungscode nach den Adressen und Aufrufmustern der gängigen KI-Dienste liefert keinen Treffer.
- Funktionen, die anderswo mit KI umgesetzt werden, etwa die Bewertung von Verkaufschancen, die Zuordnung eingehender Nachrichten oder die Auswertung, arbeiten hier nach festen, nachvollziehbaren Regeln. Das Ergebnis ist bei gleicher Eingabe immer dasselbe und damit prüfbar.

Die eine Schnittstelle, nach der ein Prüfer fragen wird

Das Produkt enthält eine Schnittstelle, über die ein Kunde sein CRM an ein eigenes Assistenzwerkzeug anbinden könnte. Sie ruft selbst kein KI-Modell auf, sondern würde Daten an ein vom Kunden betriebenes Programm ausliefern. Sie ist zentral abschaltbar und im Auslieferungszustand aus. Ein Zugriff setzt zusätzlich einen gültigen, mandantengebundenen Schlüssel voraus. Eine Aktivierung ist eine bewusste Entscheidung des Betreibers und keine stille Voreinstellung.

Abgrenzung zur Entwicklung

Bei der Entwicklung der Software werden KI-gestützte Werkzeuge eingesetzt, wie heute in nahezu jedem Softwareprojekt. Das betrifft ausschließlich Quelltext auf den Rechnern der Entwicklung und niemals Produktionsdaten von Kunden. Ein Zugriff dieser Werkzeuge auf die Produktionsdatenbank besteht nicht. Diese Trennung ist bewusst gezogen und wurde in einem eigenen Prüfbericht im Juli 2026 gesondert verifiziert.

Bedeutung für die Prüfung. Weil kein KI-Dienst beteiligt ist, entfallen die Fragen nach dem Vertrag mit einem KI-Anbieter, nach der Ausschlussmöglichkeit vom Training und nach der Kennzeichnungspflicht KI-erzeugter Ausgaben. Sollte künftig eine KI-gestützte Funktion eingeführt werden, wird sie als solche gekennzeichnet, in die Liste der Unterauftragsverarbeiter aufgenommen und angekündigt.

17 Protokollierung und Nachvollziehbarkeit

Das System führt zwei getrennte fachliche Protokolle je Mandant. Beide sind in der Anwendung einsehbar, gehören dem Mandanten und werden mit ihm gelöscht.

Protokoll	Grundlage	Inhalt
Änderungsprotokoll	Artikel 5 Absatz 2 DSGVO, Rechenschaftspflicht	Anlegen, Ändern und Löschen von Datensätzen mit Zeitpunkt, handelndem Konto, betroffenem Datensatz und den einzelnen geänderten Feldern samt vorherigem und neuem Wert.
Datenschutzprotokoll	Artikel 30 DSGVO, Verzeichnis von Verarbeitungstätigkeiten	Datenschutzrelevante Vorgänge: Auskunft, Export, Löschung, Erteilung und Widerruf einer Einwilligung, Löschantrag und dessen Ausführung oder Ablehnung.

Eigenschaften der Protokollierung

- **Sie ist Bestandteil der Fachlogik** und nicht der Oberfläche. Ein Vorgang, der über eine andere Route ausgelöst wird, wird ebenso protokolliert.
- **Sie unterbricht den Vorgang nie.** Schlägt das Schreiben eines Protokolleintrags fehl, läuft der eigentliche Vorgang weiter. Das ist eine bewusste Entscheidung: Ein Fehler in der Protokollierung darf nicht dazu führen, dass eine berechtigte Änderung scheitert.
- **Nur die geänderten Felder** werden festgehalten, nicht der gesamte Datensatz. Das hält das Protokoll lesbar und vermeidet unnötige Kopien personenbezogener Daten.

Weitere Nachweise

- **Einwilligungen** werden je Organisation oder Ansprechpartner mit Zweck, Status und Zeitpunkt geführt, sodass ein Widerruf belegbar ist.
- **Statusverläufe** von Verkaufschancen werden gesondert festgehalten, wodurch nachvollziehbar bleibt, wann ein Vorgang welche Stufe erreicht hat.
- **Löschvorgänge** werden in einem eigenen Protokoll festgehalten, das die Löschung eines Mandanten überdauert, damit die Ausführung einer Löschpflicht auch danach belegbar ist.
- **Importvorgänge** werden mit ihren Datensätzen festgehalten, damit ein Import zurückgenommen werden kann.

Technische Protokolle

Die Betriebsprotokolle der Anwendung liegen beim Hostinganbieter in Frankfurt und dienen der Fehlersuche. In sie werden keine CRM-Inhalte geschrieben; Fehlermeldungen enthalten die technische Ursache, nicht die verarbeiteten Daten. Die Serverprotokolle des Konferenzservers werden nach 48 Stunden gelöscht, was durch die Konfiguration der Protokollrotation sichergestellt und überprüft ist.

Reichweitenmessung der öffentlichen Website

Die Website nutzt keinen externen Analysedienst. Stattdessen wird ein Seitenaufruf mit einem tageweise wechselnden, gesalzenen Prüfwert gezählt. Dieser Wert wird aus IP-Adresse und Browserkennung berechnet; die IP-Adresse selbst wird nicht gespeichert und der Wert ist nicht umkehrbar. Am Folgetag entsteht für dasselbe Gerät ein anderer Wert, eine geräteübergreifende oder längerfristige Wiedererkennung ist damit ausgeschlossen. Angemeldete Nutzer werden nicht gezählt, erkannte Suchmaschinen ebenfalls nicht. Cookies werden dafür nicht gesetzt. Ein zuvor eingesetzter externer Analysedienst wurde aus Datenschutzgründen entfernt.

18 Löschkonzept, Aufbewahrung und Betroffenenrechte

Löschung eines Kundenkontos

Kündigt ein Kunde sein Konto, läuft ein festgelegter, automatisierter Ablauf. Er wird jede Nacht ausgeführt und ist nicht von einer manuellen Handlung abhängig.

Zeitpunkt	Vorgang
sofort	Das Löschmodatum wird auf 30 Tage in der Zukunft gesetzt. Die Daten bleiben vollständig erhalten, damit ein versehentlich ausgelöster Vorgang zurückgenommen werden kann.
nach 23 Tagen	Vorwarnung an den Kunden, genau einmal, sieben Tage vor der endgültigen Löschung.
nach 30 Tagen	Endgültige Löschung aller Daten des Mandanten in einer Transaktion, einschließlich der zugehörigen Dateien im Objektspeicher und der Beendigung des Abonnements beim Zahlungsdienstleister.

Ausgeschiedene Mitarbeiter eines weiterbestehenden Mandanten werden nach derselben Systematik behandelt: Vorwarnung sieben Tage vorher, danach Entfernung des Personenbezugs, während die von ihnen erzeugten Geschäftsvorgänge dem Mandanten erhalten bleiben.

Was bewusst nicht gelöscht wird. Die Rechnungen des Anbieters an den Kunden bleiben bestehen, weil § 147 der Abgabenordnung eine zehnjährige Aufbewahrung verlangt. Ihre Verknüpfung zum gelöschten Mandanten wird dabei aufgehoben. Das ist die gesetzlich vorgeschriebene Ausnahme von der Löschung und keine Zurückhaltung von CRM-Daten.

Eingefrorene Zugänge sind nicht gelöschte Zugänge

Läuft ein Testzugang ab oder endet ein Abonnement, wird der Zugang gesperrt, die Daten bleiben jedoch unverändert erhalten. Der Kunde behält Zugriff auf genau die Funktionen, die er braucht, um seinen Status zu sehen, ein Abonnement zu buchen, seine Stammdaten zu pflegen, den Support zu erreichen und sich abzumelden. Diese Ausnahmen sind als Erlaubnisliste umgesetzt, nicht als Sperrliste, damit eine vergessene Zeile zu viel sperrt statt zu wenig.

Betroffenenrechte

Recht	Umsetzung im Produkt
Auskunft, Artikel 15	Der Mandant kann die zu einer Person gespeicherten Daten in der Anwendung einsehen und exportieren. Der Vorgang wird im Datenschutzprotokoll festgehalten.
Berichtigung, Artikel 16	Änderung direkt im Datensatz, mit Eintrag im Änderungsprotokoll.
Löschung, Artikel 17	Löschanträge werden als eigener Vorgang geführt, mit Entscheidung und Ausführung. Für Kundenkonten gilt zusätzlich der oben beschriebene automatisierte Ablauf.
Datenübertragbarkeit, Artikel 20	Export in gängige Tabellenformate mit wählbaren Spalten.
Widerspruch und Widerruf, Artikel 21	Einwilligungen werden je Person mit Zweck und Zeitpunkt geführt und lassen sich widerrufen. Für E-Mail-Empfänger gibt es zusätzlich einen eigenen Abmeldeweg.
Aufbewahrungsregeln	Der Mandant kann eigene Aufbewahrungsfristen hinterlegen, um seine Löschroutine abzubilden.

Rollenverteilung nach DSGVO

Der Kunde ist Verantwortlicher für die von ihm im CRM verarbeiteten Daten. Der Anbieter ist Auftragsverarbeiter und handelt auf Weisung. Ein Vertrag zur Auftragsverarbeitung nach Artikel 28 DSGVO liegt vor, ist öffentlich abrufbar und enthält die Unterstützungspflichten bei Betroffenenanfragen, bei Datenschutz-Folgenabschätzungen und bei der Meldung von Verletzungen des Schutzes personenbezogener Daten.

19 Betrieb, Verfügbarkeit und Notfallvorsorge

Betriebsmodell

- Die Anwendung läuft in einer verwalteten Umgebung ohne eigene, dauerhaft laufende Server, die gepflegt werden müssten. Betriebssystem- und Laufzeitaktualisierungen der Ausführungsumgebung obliegen dem Anbieter dieser Umgebung.
- Die Ausführungsregion ist im Projekt fest auf Frankfurt am Main eingestellt und damit versioniert, nicht nur im Verwaltungsportal gesetzt. Eine unbemerkte Verlagerung in eine andere Region ist dadurch ausgeschlossen.
- Für den selbst betriebenen Konferenzserver gilt eine eigene Betriebsdokumentation mit Härnungen, einer eingeschränkten Firewall, automatisch erneuerten Zertifikaten und einer Prüfliste für Aktualisierungen.
- Den Fünf-Minuten-Takt für den Postfach-Abgleich gibt der selbst betriebene Server in Deutschland vor. Er ruft nur einen durch ein Geheimnis geschützten Endpunkt auf und sieht dabei weder Zugangsdaten noch Nachrichten.
- Acht geplante Hintergrundläufe erledigen wiederkehrende Aufgaben, darunter die Löschrufen, Erinnerungen an fällige Aufgaben, den Abgleich verbundener Datenquellen und die Auswertung abgelaufener Testzugänge.

Verfügbarkeit

Punkt	Angabe
Zugesagte Verfügbarkeit	99 Prozent im Jahresmittel für die Kernanwendung, entsprechend dem veröffentlichten Service-Level-Vertrag.
Ausgenommene Zusatzfunktionen	Softphone, Videokonferenz und Push-Benachrichtigungen. Sie hängen von Diensten und Geräten ab, die außerhalb des Einflussbereichs des Anbieters liegen. Diese Ausnahmen sind in den Geschäftsbedingungen ausdrücklich benannt.
Wartungsarbeiten	Auslieferungen erfolgen ohne Abschaltung. Eine neue Fassung wird bereitgestellt und der Verkehr anschließend darauf umgestellt.
Rücknahme einer Auslieferung	Jede frühere Fassung bleibt verfügbar und kann innerhalb von Minuten wieder aktiviert werden.

Sicherung und Wiederherstellung

- **Datenbank:** Der Datenbankbetreiber führt eine fortlaufende Sicherung, die eine Wiederherstellung auf einen frei wählbaren Zeitpunkt innerhalb der letzten 24 Stunden erlaubt. Die Sicherung liegt im selben Rechenzentrum in Frankfurt. Angabe des Betreibers, abhängig vom gebuchten Tarif des Datenbankanbieters.
- **Dateien:** Die Dateiablage ist redundant ausgelegt. Gelöschte Dateien werden mit dem zugehörigen Mandanten entfernt.
- **Quellcode und Konfiguration:** Vollständig versioniert. Eine Wiederherstellung der Anwendung aus dem Quellcode ist jederzeit möglich, da keine von Hand eingerichteten Serverzustände existieren.
- **Pflicht des Kunden:** Die Geschäftsbedingungen weisen den Kunden ausdrücklich auf eine eigene Datensicherung hin. Dafür steht der Export in gängige Tabellenformate bereit.

Vorgehen bei einem Sicherheitsvorfall

1. **Erkennen und eingrenzen.** Betroffene Zugänge werden gesperrt, betroffene Geheimnisse ausgetauscht. Da Rolle und Mandant bei jeder Anfrage aus der Datenbank gelesen werden, wirkt eine Sperre sofort.
2. **Bewerten.** Anhand der Protokolle wird bestimmt, welche Mandanten und welche Datenarten betroffen sind.
3. **Melden.** Der Anbieter meldet dem betroffenen Kunden als Verantwortlichem eine Verletzung des Schutzes personenbezogener Daten unverzüglich, damit dieser seine Frist von 72 Stunden nach Artikel 33 DSGVO einhalten kann. Diese Pflicht ist im Vertrag zur Auftragsverarbeitung festgehalten.
4. **Beheben und nacharbeiten.** Die Ursache wird beseitigt und die Korrektur ausgeliefert. Eine entsprechende Prüfung wird, wo möglich, durch einen automatisierten Test dauerhaft abgesichert.

Zugänge des Anbieters zur Infrastruktur

- Sämtliche Betreiberkonten der eingesetzten Infrastruktur, also Hosting, Datenbank, Quellcodeverwaltung, Zahlungsdienst und Rechenzentrum, sind mit Zwei-Faktor-Authentifizierung geschützt.
- Der Zugang zum selbst betriebenen Konferenzserver erfolgt über ein Schlüsselpaar, nicht über ein Passwort.
- Der Kreis der Personen mit Zugang zur Produktionsumgebung ist auf den Betreiber beschränkt.

20 Entwicklung und Qualitätssicherung

Ein Prüfer schließt aus der Arbeitsweise der Entwicklung darauf, wie zuverlässig die beschriebenen Maßnahmen über die Zeit erhalten bleiben. Deshalb ist dieser Abschnitt Teil des Berichts.

Wie Änderungen entstehen und ausgeliefert werden

Schritt	Umsetzung
Versionsverwaltung	Jede Änderung ist ein nachvollziehbarer Eintrag mit Begründung. Es gibt keine Änderung direkt am laufenden System.
Typprüfung	Die Übersetzung schlägt bei einem Typfehler fehl. Eine Auslieferung mit Typfehler ist nicht möglich.
Statische Prüfung	Regelwerk zur Codequalität ist eingerichtet und läuft bei jeder Auslieferung mit.
Automatisierte Tests	25 Testdateien, bewusst dort angesetzt, wo Fehler teuer werden: Datenimport in allen Formaten, Erkennung von Dubletten, Verfügbarkeits- und Zeitonenlogik der Terminbuchung, Regelwerk und Warteschlange des Anrufmodus sowie die Adressprüfung gegen Serveranfragen-Fälschung.
Datenbankmigrationen	Jede Schemaänderung ist eine versionierte Datei und wird beim Ausrollen ausgeführt. Die Migrationshistorie wurde im September 2026 instand gesetzt, seither läuft ausschließlich der geprüfte Weg.
Auslieferung	Automatisch aus der Versionsverwaltung. Jede Fassung ist einzeln erreichbar und kann zurückgenommen werden.
Trennung von Konfiguration und Code	Alle umgebungsabhängigen Werte liegen als Umgebungsvariablen vor. Derselbe Code läuft in Entwicklung und Produktion.

Umgang mit sicherheitsrelevanten Funden

Sicherheitsrelevante Korrekturen werden einzeln ausgeliefert und nicht bis zum nächsten Funktionspaket gesammelt. Nach jedem Fund wird gefragt, ob dieselbe Ursache an anderer Stelle ebenfalls vorliegt. Mehrere der in diesem Bericht beschriebenen Maßnahmen entstanden auf diese Weise, unter anderem:

- eine vollständige Überprüfung der Mandantentrennung über alle Abfragen hinweg,
- eine vollständige Sicherheitsdurchsicht der Anwendung,
- eine gesonderte Durchsicht des Weges für hochgeladene Belegvorlagen,
- die Bereinigung gemeldeter Schwachstellen in Fremdbibliotheken,
- die Prüfung, ob zur Laufzeit KI-Dienste angesprochen werden.

Dokumentation

- Ein Benutzerhandbuch und ein Einführungsleitfaden stehen als PDF bereit.
- Ein Hilfebereich ist in die Anwendung integriert; das Handbuch wird daraus erzeugt, sodass beide nicht auseinanderlaufen können.
- Ein Einrichtungsassistent führt neue Mandanten durch die ersten Schritte, einschließlich der Rollenvergabe.

21 Antworten auf die Fragen aus IT-Sicherheitsfragebögen

Die folgenden Fragen stammen aus den gängigen Lieferanten- und Sicherheitsfragebögen. Die Antworten sind so knapp gehalten, dass sie sich direkt übernehmen lassen; die Spalte rechts verweist auf das Kapitel mit der ausführlichen Begründung.

Frage	Antwort	Kap.
In welchem Land werden die Daten gespeichert?	Ausschließlich Deutschland. Anwendung und Datenbank in Frankfurt am Main, Dateien und Videokonferenz in Falkenstein im Vogtland.	13
Werden Daten in ein Drittland übermittelt?	Für CRM-Daten nein. Außerhalb der EU liegen nur die Zahlungsabwicklung des Vertragsverhältnisses und der Zustellweg von Push-Benachrichtigungen, dessen Inhalt verschlüsselt und für den Zustelldienst nicht lesbar ist.	13, 14
Liegt ein Vertrag zur Auftragsverarbeitung vor?	Ja, nach Artikel 28 DSGVO, öffentlich abrufbar, mit vollständiger Liste der Unterauftragsverarbeiter.	14, 18
Wie erfolgt die Mandantentrennung?	Logisch innerhalb einer Datenbank über eine Mandantenkennung an jedem Datensatz. Die Kennung wird bei jeder Anfrage serverseitig aus der Datenbank bestimmt, nicht aus dem Anmeldetoken übernommen.	7
Wie werden Passwörter gespeichert?	Als bcrypt-Hash mit Zufallssalz, Kostenfaktor 12. Keine Speicherung im Klartext, an keiner Stelle.	9, 12
Gibt es Zwei-Faktor-Authentifizierung?	Ja. Für Endnutzerkonten wahlweise als zeitbasiertes Einmalkennwort nach RFC 6238 oder als Passkey nach WebAuthn, von einem Master-Nutzer für das gesamte Team verpflichtend schaltbar. Kein SMS-Versand, kein externer Dienst, keine Telefonnummer. Für sämtliche Betreiberkonten der Infrastruktur ebenfalls ja.	9, 19
Wie ist die Zwei-Faktor-Authentifizierung gegen Durchprobieren geschützt?	Fünf Fehlversuche je Konto in 15 Minuten, danach Sperre. Der Zähler liegt in der Datenbank, nicht im Arbeitsspeicher einzelner Instanzen. Ein eingelöster Code wird gegen Wiedereinspielung gesperrt.	9
Werden Passkeys unterstützt?	Ja, nach dem Standard WebAuthn. Ein Passkey ersetzt Passwort und Einmalkennwort zusammen und ist gegen gefälschte Anmeldeseiten geschützt, weil der Browser ihn an die Domain bindet. Nutzer können zwischen beiden Verfahren wechseln oder beide parallel führen.	9
Was passiert, wenn ein Nutzer sein Gerät verliert?	Zehn einmalig nutzbare Wiederherstellungscodes, ersatzweise Zurücksetzen durch einen Master-Nutzer mit Eintrag im Änderungsprotokoll. Für den Fall, dass kein Master mehr einspringen kann, ein Notweg per E-Mail mit 24 Stunden Wartefrist und Benachrichtigung aller Master-Nutzer.	9
Wie lange gilt eine Sitzung?	Sieben Tage. Sperrung oder Rollenänderung eines Kontos wirkt sofort, unabhängig von der Sitzungsdauer.	9
Wie wird die Übertragung geschützt?	Ausschließlich HTTPS, HSTS über zwei Jahre einschließlich Unterdomänen, Content Security Policy, Einbettung in fremde Seiten unterbunden, Herkunftsprüfung der Schnittstellen gegen eine feste Liste.	10
Werden Daten im Ruhezustand verschlüsselt?	Ja, auf Datenträgerebene durch Datenbank- und Speicherbetreiber. Zugangsdaten verbundener Postfächer und Telefonanlagen zusätzlich mit AES-256, wobei der Schlüssel außerhalb der Datenbank liegt.	12
Gibt es ein Rollen- und Rechtekonzept?	Ja, fünf Rollen einschließlich einer reinen Leserolle, dazu feingranular erteilbare Einzelrechte je Assistenzkonto. Durchsetzung serverseitig.	8
Werden Zugriffe und Änderungen protokolliert?	Ja, getrenntes Änderungsprotokoll und Datenschutzprotokoll je Mandant, in der Anwendung einsehbar.	17
Wie werden Daten gelöscht und nach welchen Fristen?	30 Tage Schonfrist nach Kündigung, Vorwarnung sieben Tage vorher, danach vollständige Löschung durch einen nächtlichen automatischen Lauf, einschließlich der Dateien. Ausnahme sind die Rechnungen des Anbieters wegen § 147 AO.	18
Können wir unsere Daten exportieren?	Ja, jederzeit in gängige Tabellenformate mit wählbaren Spalten, ohne Mitwirkung des Anbieters.	18

Frage	Antwort	Kap.
Wie wird gesichert und wiederhergestellt?	Fortlaufende Sicherung der Datenbank durch den Datenbankbetreiber mit Wiederherstellung auf einen frei wählbaren Zeitpunkt innerhalb der letzten 24 Stunden, im selben Rechenzentrum. Dateiablage redundant. Anwendung jederzeit aus dem versionierten Quellcode wiederherstellbar.	19
Welche Verfügbarkeit wird zugesagt?	99 Prozent im Jahresmittel für die Kernanwendung, so auch im veröffentlichten Service-Level-Vertrag. Softphone, Videokonferenz und Push-Benachrichtigungen sind ausdrücklich ausgenommen.	19
Wie werden Sicherheitsvorfälle gemeldet?	Unverzüglich an den betroffenen Kunden als Verantwortlichen, damit dessen Frist von 72 Stunden nach Artikel 33 DSGVO eingehalten werden kann. Die Pflicht ist im Auftragsverarbeitungsvertrag festgehalten.	19
Gibt es Zertifizierungen oder externe Penetrationstests?	Nein. Es besteht kein ISO-27001-Zertifikat und es wurde kein externer Penetrationstest beauftragt. Stattdessen liegen mehrere dokumentierte eigene Sicherheitsdurchsichten vor, unter anderem zur Mandantentrennung, zur Gesamtanwendung, zur Verarbeitung hochgeladener Dateien und zu den Fremdbibliotheken.	2, 20
Welche Subunternehmer sind beteiligt?	Neun, vollständig benannt mit Leistung, Standort und Datenumfang. Sieben davon verarbeiten in Deutschland oder der EU.	14
Werden unsere Daten für KI oder Modelltraining genutzt?	Nein. Die Anwendung ruft zur Laufzeit kein KI-Modell auf, es besteht kein KI-Anbieter als Unterauftragsverarbeiter, und es findet kein Training mit Kundendaten statt.	16
Wer beim Anbieter hat Zugriff auf unsere Daten?	Der Kreis beschränkt sich auf den Betreiber. Der Zugriff erfolgt im Rahmen der Auftragsverarbeitung, etwa zur Fehlerbehebung. Die Betreiberoberfläche ist von den Kundenkonten technisch vollständig getrennt.	8, 19
Wie ist die Programmierschnittstelle abgesichert?	Über mandantengebundene Schlüssel mit Berechtigungsumfang, die nur als Hash gespeichert und jederzeit widerrufbar sind.	9, 15
Wie wird gegen die verbreiteten Angriffsklassen geschützt?	Zwölf Angriffsklassen einzeln bewertet und abgedeckt, darunter SQL-Einschleusung, Skript-Einschleusung, Anfragenfälschung, fehlende Zugriffskontrolle und Serveranfragen-Fälschung.	11
Wie erfolgt die mobile Nutzung?	Als installierbare Webanwendung mit demselben Nutzerkonto. Ein Gerät wird über einen einmalig verwendbaren, nur als Hash gespeicherten Code gekoppelt und kann jederzeit widerrufen werden. Auf dem Gerät werden keine CRM-Daten dauerhaft abgelegt.	9, 15
Was geschieht bei Vertragsende?	Die Daten bleiben 30 Tage vollständig erhalten und exportierbar, danach werden sie gelöscht. Ein gesperrter Zugang ist kein gelöschter Zugang.	18

22 Ansprechpartner und weiterführende Unterlagen

Ansprechpartner für Rückfragen der IT

Für technische Rückfragen, für eine vertiefte Auskunft zu den technischen und organisatorischen Maßnahmen nach Artikel 32 DSGVO oder für ein Gespräch mit Ihrer IT- und Datenschutzabteilung steht der Anbieter persönlich zur Verfügung. Ein Rückruf lässt sich kurzfristig vereinbaren.

Anliegen	Kontakt
Technische und datenschutzrechtliche Rückfragen	info@apexlead-pro.de, Telefon +49 30 700 169 16
Vertragliche Fragen und Vorstellung im Unternehmen	vertrieb@apexlead-pro.de, gern auch als Rückruf oder Videotermin
Anbieter	David Hörnlein-Ulrich, ApexLead-pro, Kolonie 2, 14798 Havelsee, Deutschland. USt-IdNr. DE462238980

Unterlagen, die diesen Bericht ergänzen

Unterlage	Inhalt und Bezug
Vertrag zur Auftragsverarbeitung	Rechtsverbindliche Fassung der Kapitel 14 und 18, einschließlich der Unterauftragsverarbeiter und der Unterstützungspflichten. Öffentlich abrufbar.
Datenschutzerklärung	Verarbeitungszwecke, Rechtsgrundlagen und Speicherdauern, auch für die öffentliche Website. Öffentlich abrufbar.
Allgemeine Geschäftsbedingungen	Leistungsumfang, Verfügbarkeitszusage, Mitwirkungspflichten und Abgrenzung der vom Kunden selbst angebotenen Dienste. Öffentlich abrufbar.
Kurzübersicht zum Datenschutz	Zusammenfassung für den schnellen Überblick, als PDF erhältlich.
Benutzerhandbuch und Einführungsleitfaden	Bedienung und Einrichtung, als PDF erhältlich.
Vollständige Liste der technischen und organisatorischen Maßnahmen	Auf Anfrage, in der von Ihrer Prüfstelle gewünschten Gliederung.

Gültigkeit dieses Berichts

Der Bericht beschreibt den Stand vom 15. Oktober 2026. Er wird fortgeschrieben, sobald sich Architektur, Standorte oder die Liste der Unterauftragsverarbeiter ändern. Bei einer Änderung eines Unterauftragsverarbeiters werden die Kunden gesondert unterrichtet.

Schlussbemerkung. ApexLead-pro ist von Grund auf für den deutschen Mittelstand gebaut worden, mit der Datenhaltung in Deutschland als Ausgangspunkt der Architektur und nicht als nachträglicher Zusatz. Die in diesem Bericht beschriebenen Maßnahmen sind vollständig umgesetzt und im ausgelieferten Produktionsstand nachprüfbar. Für eine Prüfung mit größerer Tiefe, etwa eine Begehung der Maßnahmen gemeinsam mit Ihrer IT, steht der Anbieter bereit.