HASOMED®
Praxis. Therapie. Sicherheit.

Cyber- und Informations-sicherheit bei Elefant

Sicherheitsarchitektur, Betriebsmodell und Compliance-Rahmen

02/2026

Inhaltsverzeichnis

1 Einleitung

Einleitung

Gesundheitsdaten zählen zu den besonders schutzbedürftigen personenbezogenen Daten im Sinne der DSGVO. Ihre Verarbeitung erfordert ein besonders hohes Schutzniveau – insbesondere im psychotherapeutischen Kontext, in dem sie die Grundlage jeder Behandlung bilden. Für uns bedeutet das, dass Informationssicherheit und Datenschutz keine nachgelagerten Pflichten sind, sondern von Anfang an als grundlegende Designprinzipien in unsere Produkte integriert werden. Unser Ziel ist es, allen Beteiligten zu jeder Zeit das höchstmögliche Schutzniveau bereitzustellen.

Mit Elefant stellen wir seit vielen Jahren eine der führenden Praxissoftwarelösungen für tausende psychotherapeutische Praxen in Deutschland bereit.
Wir erleben seit einigen Jahren tiefgreifende Veränderungen im Gesundheitswesen und einen globalen technologischen Wandel, die gemeinsam eine grundlegende Modernisierung von Elefant erforderlich macht — sowohl, um ein dauerhaft hohes Schutzniveau sicherzustellen, als auch, um den sich wandelnden Erwartungen unserer Nutzer:innen gerecht zu werden.

→ **Diese Modernisierung wird insbesondere durch drei Entwicklungen getrieben:**

1. immer umfangreichere Anforderungen von Gematik und Kassenärztlicher Bundesvereinigung (KBV) an die Integration und den Betrieb von Fachmodulen wie Abrechnung, die Anbindung an Terminservicestellen und die Anwendungen der Telematikinfrastruktur,
2. neue Erwartungen unserer Kund:innen an orts- und geräteunabhängiges Arbeiten und die Integration mit modernen Softwareprodukten und Technologien, sowie
3. die technologische Notwendigkeit, unsere historisch in Delphi entwickelte Anwendung auf eine moderne Architektur zu überführen, da die zugrunde liegende Technologie weltweit abgelöst wird und perspektivisch nicht mehr tragfähig ist.

Vor diesem Hintergrund entwickeln wir Elefant konsequent von einer rein lokal installierten Anwendung hin zu einer modernen Anwendung, die lokale und Webkomponenten verbindet und plattformunabhängig genutzt werden kann. Dieser Wandel erweitert nicht nur die Möglichkeiten für Praxen, sondern erhöht auch unsere Verantwortung, die Sicherheit unserer Systeme transparent, nachvollziehbar und überprüfbar zu gestalten.

Dieses White Paper gibt einen strukturierten Einblick in unsere Sicherheitsarchitektur und unsere Grundsätze im Bereich Cyber- und Informationssicherheit. Es richtet sich an unsere Kund:innen, an Technologiepartner sowie an alle, die sich ein fundiertes und nachvollziehbares Bild davon machen möchten, wie wir Informationssicherheit bei HASOMED organisatorisch und technisch verankern.

Unser Anspruch ist klar: Sicherheit entsteht nicht durch Erklärungen oder Versprechen, sondern durch klar definierte Prozesse und Prinzipien, belastbare Maßnahmen und kontinuierliche Weiterentwicklung. Dieses Dokument versteht sich als Ausdruck dieser Haltung – und lädt ausdrücklich zur kritischen Betrachtung und zum fachlichen Dialog ein.

Hasomed®
Praxis. Therapie. Sicherheit.

2

Architektur & Betriebsmodell

2.1 Elefant – Das Produkt

Elefant ist eine lokal installierte Praxisverwaltungssoftware der HASOMED GmbH, die heute auf Windows-Systemen in psychotherapeutischen Praxen betrieben wird. Die Anwendung wurde initial in Delphi entwickelt und nutzt eine Firebird-Datenbank zur lokalen Speicherung. Elefant ist eine der am weitesten verbreiteten Lösungen im psychotherapeutischen Bereich. Die Software deckt zentrale Anforderungen des Praxisbetriebs ab – von Terminverwaltung und Dokumentation bis hin zur Abrechnung mit den Krankenkassen.
Durch ihre lange Einsatzgeschichte ist Elefant fest in den Arbeitsabläufen vieler Praxen verankert und bildet das digitale Fundament zahlreicher psychotherapeutischer Versorgungseinrichtungen in Deutschland.

2.2 Hybrid-Architektur (lokal + Cloud)

Zur Erweiterung und schrittweisen Modernisierung des Elefant-Systems setzt die HASOMED GmbH auf eine Kombination aus lokal installierter Anwendung und cloudbasierten Diensten. Ziel ist es, mittelfristig den Übergang zu einer vollständig browserbasierten Version zu ermöglichen, die unabhängig von lokalen Installationen genutzt werden kann – ohne dabei die Praxen zu abrupten Umstellungen zu zwingen.

Derzeit erfolgt die Integration der neuen Funktionen über React-basierte Web-Komponenten, die innerhalb der bestehenden Windows-Anwendung eingebettet sind. Für die Nutzer:innen bleibt die gewohnte Arbeitsumgebung damit erhalten, während gleichzeitig moderne, cloudgestützte Erweiterungen verfügbar werden.

Zentrales technisches Bindeglied ist der installierte Relay-Dienst. Er stellt die Verbindung zwischen dem lokalen System und der Cloud her, greift bei Bedarf auf die Firebird-Datenbank zu, kommuniziert mit dem TI-Konnektor und überträgt Daten ausschließlich über verschlüsselte Kanäle.

Ein wesentlicher Baustein dieser Architektur ist die sichere Verlagerung der Datenhaltung. Immer mehr sensible Daten – darunter Dokumente, Formulare oder Kommunikationsobjekte aus der TI – werden über den Relay-Dienst in eine zentrale Serverinfrastruktur übertragen und dort verschlüsselt gespeichert. Die Ablage erfolgt logisch und kryptographisch mandantengetrennt in der Infrastruktur der HASOMED Tech GmbH, die als technologische Tochtergesellschaft den sicheren Betrieb dieser Systeme verantwortet.

2.3 Kernkomponenten

Die Architektur von Elefant umfasst sowohl lokal betriebene als auch cloudbasierte Komponenten. Gemeinsam bilden sie eine integrierte Plattform, die den Praxen einerseits Kontinuität in der täglichen Arbeit bietet und andererseits den Weg für moderne, webbasierte Funktionen öffnet.

- **Lokale Ebene**
  - **Elefant-Client (Delphi-Anwendung):**
    Die klassische Praxissoftware, die weiterhin auf Windows-Systemen betrieben wird.
  - **Firebird-Datenbank:**
    Lokaler Datenspeicher für Patientendaten, Dokumentationen und Konfigurationen.
  - **TI-Komponenten:**
    Konnektor und Kartenterminals, über die gesetzlich vorgeschriebene Fachanwendungen wie eAU, eRezept oder ePA ermöglicht werden.
- **Vermittlungsschicht**
  - **Relay-Dienst:**
    Lokaler Hintergrunddienst, der sowohl auf die Firebird-Datenbank zugreifen kann als auch mit dem TI-Konnektor kommuniziert. Er stellt eine verschlüsselte Verbindung zum Relay-Gateway her und ist damit die zentrale Schnittstelle zwischen Praxis und Cloud.
- **Cloud-Ebene**
  - **Web-Elefant:**
    Browserbasierte Oberfläche, die als eingebettete Komponente in der lokalen Anwendung sichtbar wird und schrittweise moderne Funktionen bereitstellt.
  - **Relay-Gateway::**
    Entgegennahme und Weiterleitung der verschlüsselten Anfragen aus den Praxen an die passenden Backend-Services.

Mandantenspezifische Datenhaltung:
Jede Praxis verfügt über einen eigenen, verschlüsselten Datenbereich in der AWS Cloud. Strukturierte Informationen – wie Patientendaten, Termine, Behandlungsinformationen oder technische Konfigurationen – werden in PostgreSQL-Datenbanken (AWS RDS) abgelegt. Dokumente – darunter medizinische Berichte, Formulare oder Dateien aus der elektronischen Patientenakte – werden verschlüsselt in S3-Buckets gespeichert, einem hochverfügbaren Objektspeicher von AWS, der für die sichere Ablage großer Datenmengen entwickelt wurde.

2.4 Geteiltes Verantwortungsmodell

Die sichere Verarbeitung sensibler Gesundheitsdaten erfordert nicht nur technische Maßnahmen, sondern auch eine klare organisatorische Verantwortungsverteilung. Im Fall von Elefant ergibt sich diese entlang der Rollen von HASOMED GmbH, HASOMED Tech GmbH und den nutzenden psychotherapeutischen Praxen.

Verantwortung der HASOMED GmbH
Die HASOMED GmbH ist Herstellerin von Elefant und alleinige Vertragspartnerin der Praxen. Sie trägt die Gesamtverantwortung für Konzeption, rechtliche Einordnung und Konformität des Produkts – insbesondere mit den Vorgaben aus SGB V, den Richtlinien der Kassenärztlichen Bundesvereinigung (KBV) und den Anforderungen der Telematikinfrastruktur (TI). Dazu gehört ausdrücklich auch die übergreifende Verantwortung für die Cyber & Informationssicherheit.

Ein Schwerpunkt liegt auf der Koordination im Datenschutz und Sicherheitskontext: Die HASOMED GmbH ist zentrale Kontaktstelle für Praxen, koordiniert die Kommunikation im Falle von Sicherheitsvorfällen und stimmt sich, falls notwendig, mit Aufsichtsbehörden ab. Auch die Auswahl und Steuerung aller Dienstleister – einschließlich HASOMED Tech als technologische Tochter – sowie der Abschluss und die Pflege der Auftragsverarbeitungsverträge (AVV) mit den Praxen fallen in diesen Verantwortungsbereich.

Verantwortung der HASOMED Tech GmbH
Die HASOMED Tech GmbH ist eine hundertprozentige Tochtergesellschaft der HASOMED GmbH und übernimmt im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DSGVO die technische Bereitstellung, den sicheren Betrieb sowie die fortlaufende

Weiterentwicklung der zentral betriebenen Systemkomponenten von Elefant. Hierzu gehören insbesondere der Betrieb der AWS-Infrastruktur, die sichere Implementierung von Software, Verschlüsselungs- und Zugriffskontrollmechanismen, Schwachstellenmanagement sowie die Absicherung der Schnittstellen zwischen den lokalen Systemen der Praxen und der zentralen Serverinfrastruktur.

Die HASOMED Tech GmbH handelt dabei ausschließlich als Unterauftragsverarbeiter im Auftrag und nach dokumentierten Weisungen der HASOMED GmbH. Die HASOMED GmbH ist im Verhältnis zu HASOMED Tech datenschutzrechtlich Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO und behält die vollständige Kontrolle über alle Verarbeitungsvorgänge. Gegenüber den nutzenden Praxen agiert sie als Auftragsverarbeiter und ist für die Auswahl, Steuerung und Kontrolle ihrer Unterauftragsverarbeiter verantwortlich.

Im Rahmen ihres Informationssicherheits-Managementsystems (ISMS) führt die HASOMED GmbH regelmäßige interne Audits durch und stellt personell wie organisatorisch sicher, dass die Tätigkeiten der HASOMED Tech GmbH laufend überwacht und an die definierten Sicherheits- und Datenschutzanforderungen angepasst werden.

→ Verantwortung der nutzenden Praxen

Die Praxen selbst sind für die Sicherheit ihrer lokalen IT-Umgebung verantwortlich. Dazu zählen insbesondere der Schutz der Praxis-PCs, eine sichere Netzwerkkonfiguration, die Verwaltung von Zugangsdaten sowie der sachgerechte Betrieb der TI-Komponenten (Konnektor, Kartenterminal).

Diese Aufgaben liegen außerhalb des direkten Einflussbereichs der HASOMED GmbH und der HASOMED Tech GmbH. Die HASOMED GmbH unterstützt ihre Kund:innen jedoch aktiv mit praxisnahen Hinweisen und Hilfestellungen, um sicherzustellen, dass die lokalen Schutzmaßnahmen mit der Gesamtarchitektur zusammenspielen. Darüber hinaus tritt die HASOMED GmbH auch als Anbieter von IT-Sicherheitslösungen und Praxishardware auf und steht den Praxen bei der Auswahl, Implementierung und dem sicheren Betrieb lokaler IT-Infrastrukturen beratend zur Verfügung.

Hasomed®
Praxis. Therapie. Sicherheit.

3

Maßnahmen zur Risikominimierung

3.1 Unsere Grundprinzipien

Die Sicherheitsarchitektur von HASOMED beruht auf klar definierten Leitprinzipien. Sie bilden den verbindlichen Orientierungsrahmen für alle Entscheidungen im Bereich Informationssicherheit und schaffen damit die Grundlage für ein konsistentes, überprüfbares Sicherheitsmanagement.

Uns ist wichtig, Sicherheit nicht als eine Ansammlung technischer Einzelmaßnahmen zu begreifen, sondern als eine Managementaufgabe, die durch übergeordnete Werte, verbindliche Regeln und eine gelebte Sicherheitskultur getragen wird. Diese Prinzipien machen wir bewusst transparent, weil wir überzeugt sind, dass nachhaltige Sicherheit nur durch nachvollziehbare Entscheidungen und klare Verantwortlichkeiten entstehen kann.

- **Antizipieren statt Reagieren**

  Ein zentrales Prinzip unseres Sicherheitsprogramms ist es, Risiken vorausschauend und strategisch zu adressieren. Wir arbeiten mit Szenarien, die uns helfen, Bedrohungen greifbar zu machen und daraus konkrete Maßnahmen abzuleiten. Denn nur Risiken, die klar benannt sind, lassen sich auch wirksam mit Lösungen beantworten.

  Dabei betonen wir verschiedene Dimensionen, zum Beispiel:

  - **Informationen & Daten:**
    Welche Angriffsszenarien wirken auf die sensiblen Daten, die wir verarbeiten?
  - **Technologie-Stack:**
    Welche realistischen Bedrohungen ergeben sich für unsere Systeme und Infrastruktur?
  - **Markt & Kund:innen:**
    Welche Erwartungen an Sicherheit bestehen, und wie übersetzen wir sie in Maßnahmen?
  - **Eigener Risk Appetite:**
    Welche Initiativen und Maßnahmen folgen aus unserem Selbstverständnis und unserem definierten Risikorahmen?

  Diese mehrdimensionale Betrachtung macht Sicherheit für uns besprechbar, priorisierbar und planbar – und bildet damit die Grundlage, unser Sicherheitsprogramm kontinuierlich weiterzuentwickeln.

Transparenz & Nachvollziehbarkeit

Sicherheit muss für uns immer auch nachvollziehbar sein – nicht nur ein Versprechen. Deshalb dokumentieren wir unser Sicherheitskonzept offen, schaffen Kontext und laden zur kritischen Überprüfung ein. Wir glauben, dass Vertrauen und Sicherheit aus Dialog entstehen. Hinweise zu Schwachstellen, Verbesserungsvorschläge oder technische Rückfragen greifen wir daher aktiv auf – unter anderem über unseren Security Contact Point und im Rahmen unseres Bug-Bounty-Programms.

Sicherheit als Standardprinzip

Sicherheit ist bei HASOMED kein optionaler Zusatz, sondern ein von Beginn an verpflichtend integrierter Bestandteil unserer Systemarchitektur. Grundlegende Schutzmechanismen wie Verschlüsselung, Zugriffskontrollen und Mandantentrennung werden standardmäßig implementiert und sind nicht abschaltbar oder von individuellen Entscheidungen abhängig.
Diese Grundhaltung ist Ausdruck unseres Verantwortungsbewusstseins gegenüber den nutzenden Praxen und den von ihnen verarbeiteten besonders schutzbedürftigen Gesundheitsdaten.

Orientierung an Standards und bewährten Prinzipien

Wir setzen auf bewährte Architekturprinzipien, klare Verantwortlichkeiten und den gezielten Einsatz moderner Sicherheitstechnologien. Dabei erfinden wir Sicherheit nicht neu, sondern orientieren uns an etablierten Standards und anerkannten Best Practices – unter anderem an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), dem C5-Anforderungskatalog sowie gängigen Cloud-Security-Frameworks.

Die HASOMED GmbH betreibt ein nach ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem (ISMS). Dieses ISMS definiert verbindliche Prozesse, Rollen und Kontrollmechanismen für alle sicherheitsrelevanten Tätigkeiten. Im Rahmen des ISMS durchlaufen wir regelmäßig interne und externe Audits, die die Wirksamkeit unserer Sicherheitsmaßnahmen überprüfen und deren kontinuierliche Weiterentwicklung sicherstellen.

Auf diese Weise schaffen wir eine belastbare und nachvollziehbare Sicherheitsarchitektur, deren Umsetzung nicht nur intern dokumentiert, sondern auch regelmäßig durch unabhängige Prüfer bestätigt wird.

3.2 Technische Maßnahmen

Envelope Encryption für Kundendaten mit externer Schlüsselverwaltung

In Elefant wird jeder sensible Inhalt mit eigenem Schlüsselmaterial geschützt. Das bedeutet: Patientendaten, Terminserien, Behandlungsdokumentationen oder auch hochgeladene medizinische Berichte werden jeweils separat verschlüsselt. Es gibt also nicht einen einzigen Generalschlüssel, sondern eine Vielzahl individueller Schlüssel, die eine klare Trennung zwischen den Datenobjekten sicherstellen.

Technisch geschieht dies nach dem Prinzip der Envelope Encryption:

- Jedes Datenobjekt erhält einen eigenen Data Key, der ausschließlich zur Verschlüsselung dieses einen Objekts genutzt wird.
- Diese Data Keys selbst werden nicht im Klartext gespeichert, sondern wiederum verschlüsselt – und zwar mit einem übergeordneten Master Key.

Die entscheidende Sicherheitsarchitektur liegt in der Verwaltung der Master Keys:

- Die Data Keys befinden sich innerhalb der AWS-Umgebung, wo sie die einzelnen Objekte absichern.
- Der Master Key jedoch liegt nicht bei AWS, sondern ausschließlich in einem Hardware-Sicherheitsmodul (HSM) der T-Systems. Über das AWS-Verfahren „External Key Store (XKS)“ kann AWS die Data Keys nur dann entschlüsseln, wenn der externe Keystore aktiv zustimmt.

Damit wird die tatsächliche Entschlüsselung technisch außerhalb von AWS vollzogen. Selbst im Fall einer hypothetischen Herausgabeverpflichtung könnte AWS nur verschlüsselte Datenblöcke bereitstellen – ohne Zugriff auf den Master Key bleiben diese unlesbar.

Für die Praxen bedeutet das: Die Daten sind nicht nur mandantenspezifisch getrennt, sondern auch durch ein zweistufiges Schlüsselkonzept abgesichert, bei dem die Kontrolle über die entscheidenden Schlüsselkomponenten vollständig bei HASOMED und einem europäischen Partner liegt.

→ **Absicherung der Schnittstellenkommunikation (Relay ↔ Relay-Gateway)**

Die Kommunikation zwischen den Praxen und der Cloud-Plattform erfolgt über den Relay-Dienst, der lokal auf den Praxisrechnern installiert ist. Er baut eine ausschließlich ausgehende Verbindung (Outbound) zum Relay-Gateway in der AWS-Region Frankfurt auf. Das bedeutet: Das Relay ist von außen nicht erreichbar und stellt damit keine Angriffsfläche für eingehende Verbindungen dar.

Die Verbindung wird durch mehrere Mechanismen abgesichert:

- **Transportverschlüsselung (TLS):**
  Alle Datenübertragungen zwischen Relay und Relay-Gateway erfolgen ausschließlich verschlüsselt.
- **Gegenseitige Authentifizierung (mTLS):**
  Jede Praxis verfügt über ein eigenes Zertifikat, mit dem sich der Relay-Dienst gegenüber dem Gateway ausweist. Umgekehrt überprüft das Relay die Identität des Gateways, sodass ein Zugriff durch Unbefugte ausgeschlossen wird.
- **Signierte Antworten:**
  Kommunikation, die vom Relay-Gateway zurück an das Relay gesendet wird, ist zusätzlich kryptografisch signiert. Damit wird die Integrität der Daten sichergestellt und Manipulationen im Übertragungsweg sind ausgeschlossen.

  Für die Praxen bedeutet das: Die Schnittstelle zwischen lokaler Anwendung und Cloud ist nicht nur verschlüsselt, sondern auch eindeutig authentifiziert und manipulationssicher.

→ **Gesicherte TI-Kommunikation über Konnektoren**

Die Anbindung an die Telematikinfrastruktur (TI) erfolgt bei unseren Kund:innen grundsätzlich über sogenannte TI-Konnektoren, die den sicheren Zugriff auf Fachanwendungen wie die ePA ermöglichen. Diese Konnektoren sind stets Teil der Praxisinfrastruktur und werden nicht zentral durch HASOMED betrieben.

Je nach Praxisumgebung kommen unterschiedliche Betriebsformen zum Einsatz:

- **Lokale Konnektoren (Einbox-Konnektoren):**
  Diese Hardwaregeräte sind physisch in den Praxen installiert und direkt mit dem Praxisnetz verbunden.

- **Rechenzentrums- oder TIaaS-Konnektoren:**
  Hier befindet sich der Konnektor im Rechenzentrum eines Dienstleisters, erreichbar über eine gesicherte VPN-Verbindung.
- **TI-Gateway-Konnektoren::**
  Diese neuere Architektur kombiniert virtuelle Hochleistungs-Konnektoren mit einer VPN-Anbindung und ermöglicht mehreren Praxen die Nutzung einer gemeinsam betriebenen, logisch getrennten Konnektor-Instanz.

Die Kommunikation zwischen Elefant und dem TI-Konnektor erfolgt immer innerhalb der jeweiligen Praxisinfrastruktur.

Wenn cloudbasierte Komponenten – etwa Web-Module von Elefant – Informationen austauschen, geschieht dies über den lokal installierten Relay-Dienst, der die Verbindung zwischen Cloud und Praxis vermittelt. Der Relay-Dienst kann in diesem Fall Anfragen aus der Cloud sicher an den lokalen Konnektor weiterleiten und deren Antworten verschlüsselt zurück übermitteln.

Dadurch ist gewährleistet, dass die Telematik-Kommunikation ausschließlich über die autorisierte Praxisinfrastruktur erfolgt und keine direkte Verbindung zwischen der Cloud-Plattform und der TI besteht.

Unabhängig davon, ob ein Konnektor lokal, im Rechenzentrum oder im TI-Gateway-Modell betrieben wird, bleibt die Kommunikation authentifiziert, verschlüsselt und manipulationssicher.

- **Mehrschichtiges Sicherheitskonzept für Arbeitsplatz-, Infrastruktur- und Anwendungsebene**

  Neben den spezifischen Schutzmechanismen innerhalb unserer Plattform betreiben wir ein mehrschichtiges Sicherheitskonzept, um sowohl unsere Unternehmens-IT als auch die zugrunde liegende technische Infrastruktur abzusichern. Unser Ansatz deckt alle relevanten Ebenen ab – vom Arbeitsplatz über die Server- und Netzwerkinfrastruktur bis hin zur Anwendungssicherheit – und wird im Rahmen unseres nach ISO/IEC 27001 zertifizierten Informationssicherheits-Managementsystems (ISMS) regelmäßig überprüft und weiterentwickelt. Die cloudbasierten Systemkomponenten werden zusätzlich nach dem C5-Standard (Cloud Computing Compliance Criteria Catalogue) des BSI auditiert.

Arbeitsplatz
Auf der Arbeitsplatzebene setzen wir auf einen abgesicherten Enterprise-Browser als zentralen Zugriffspunkt auf interne Systeme, einen zentralen Identity Provider (IdP) mit integriertem Passwort- und Gerätemanagement sowie auf sichere Kollaborations- und Kommunikationstools.

Diese Komponenten stellen sicher, dass der Zugriff auf interne Systeme kontrolliert, nachvollziehbar und an zentrale Authentifizierungs- und Autorisierungsvorgaben gebunden erfolgt.

Infrastruktur
Für die Absicherung unserer zentral betriebenen Systeme setzen wir auf spezialisierte Cloud-Sicherheitslösungen, darunter insbesondere Cloud Native Application Protection Platforms (CNAPP) sowie Cloud Infrastructure Entitlement Management (CIEM). Diese Lösungen überwachen kontinuierlich Konfigurationen, Berechtigungen und Ressourcenzugriffe, erkennen Abweichungen von definierten Sicherheitsrichtlinien frühzeitig und verhindern unautorisierte Zugriffe. So stellen wir sicher, dass unsere Systeme auch in dynamischen Betriebsumgebungen jederzeit auf einer belastbaren und regelkonformen Grundlage betrieben werden.

Die cloudbasierten Komponenten werden zusätzlich nach dem C5-Standard (Cloud Computing Compliance Criteria Catalogue) des BSI auditiert, um die Einhaltung höchster Sicherheits- und Compliance-Anforderungen regelmäßig durch unabhängige Prüfer bestätigen zu lassen.

Applikationssicherheit
Die Anwendungssicherheit wird durch ein systematisches Schwachstellenmanagement, automatisierte sicherheitsrelevante Tests (z. B. IAST), regelmäßige Penetrationstests sowie ein Bug-Bounty-Programm sichergestellt. Diese Maßnahmen ermöglichen es, potenzielle Schwachstellen frühzeitig zu erkennen und Sicherheitsanforderungen laufend in die Entwicklungsprozesse einfließen zu lassen.

3.3 Organisatorische Maßnahmen

Professionelles Sicherheitsprogramm mit CISOIQ

Sicherheit ist für uns nicht nur eine technische Frage, sondern ein fester Bestandteil unserer Organisation. Von Beginn an haben wir ein eigenständiges Sicherheitsprogramm etabliert, das über die Rolle eines Chief Information Security Officers (CISO) fest in unserer Unternehmensstruktur verankert ist.

Für die Planung, Umsetzung und laufende Betreuung unseres Sicherheitsprogramms arbeiten wir mit CISOIQ, einem spezialisierten Berliner Cyber-Security-Unternehmen. CISOIQ übernimmt nicht nur beratende Aufgaben, sondern wirkt mit eigenem Fachpersonal operativ an der Umsetzung unseres Sicherheitsprogramms mit — etwa bei der Gestaltung von Richtlinien, dem Aufbau sicherheitsrelevanter Prozesse, dem operativen Schwachstellenmanagement und der Vorbereitung auf interne wie externe Audits.

Das Sicherheitsteam von CISOIQ ist eng in unsere Organisation eingebunden, arbeitet in kontinuierlicher Abstimmung mit dem Management der HASOMED GmbH und berichtet direkt an die Geschäftsführung. Dadurch stellen wir sicher, dass Cyber & Informationssicherheit bei HASOMED nicht als begleitendes Thema verstanden wird, sondern als kontinuierlicher Prozess, der eng mit der technologischen Entwicklung des Produkts verzahnt ist.

Sicherheitsbewusstsein & Kultur im Team

Für uns ist klar: Sicherheit ist nicht allein Aufgabe einzelner Spezialist:innen, sondern eine gemeinsame Verantwortung aller Mitarbeitenden. Jede und jeder trägt dazu bei, dem Vertrauen gerecht zu werden, das uns Kund:innen und Marktteilnehmer entgegenbringen.

Deshalb ist Awareness und Verantwortungskultur von Beginn an eine tragende Säule unseres Security-Programms. Wir fördern dies durch regelmäßige Awareness-Trainings, klare Leitlinien im Umgang mit sensiblen Daten und praxisnahe Übungen, etwa zu Phishing oder Passwortsicherheit.

So stellen wir sicher, dass Security nicht nur ein technisches Thema bleibt, sondern ein gelebter Teil unserer Unternehmenskultur ist – und in allen Bereichen, von der Produktentwicklung bis zur täglichen Zusammenarbeit, selbstverständlich berücksichtigt wird.

Vier-Augen-Prinzip bei sicherheitskritischen Änderungen

In der Softwareentwicklung von Elefant, ebenso wie bei allen anderen Systemen und Infrastrukturen, gilt für uns: Keine sicherheitsrelevante Änderung darf von einer einzelnen Person unkontrolliert durchgeführt werden.

Daher kombinieren wir moderne Entwicklungs- und Betriebsprinzipien wie konsequente Versionierung, das verbindliche Vier-Augen-Prinzip bei sicherheitskritischen Änderungen und dedizierte Security-Reviews durch qualifizierte Teammitglieder. Jede Änderung an Code, Infrastruktur oder Konfiguration durchläuft damit mehrere Kontrollschritte, bevor sie produktiv wirksam wird.

Wir vertrauen unseren Teams – und gleichzeitig folgen wir dem Grundsatz, dass es gute Praxis ist, wichtige Schritte gemeinsam abzusichern. So stellen wir sicher, dass Fehler oder Schwachstellen nicht unbemerkt bleiben und dass immer mehrere Perspektiven in sicherheitsrelevante Entscheidungen einfließen.

Kontinuierliche Penetrationstests

Um mögliche Schwachstellen frühzeitig zu identifizieren, kombinieren wir verschiedene Prüfmethoden, anstatt uns ausschließlich auf standardisierte Verfahren zu verlassen.

Zum einen führen wir regelmäßig strukturierte Penetrationstests durch, die anhand definierter Prüfkategorien bewerten, ob öffentlich erreichbare Systeme oder Anwendungen potenzielle Verwundbarkeiten aufweisen. Diese Tests liefern uns ein systematisches und belastbares Bild über den aktuellen Sicherheitsstand unserer Systeme.

Darüber hinaus betreiben wir ein Bug-Bounty-Programm. Dabei wird unsere Plattform kontinuierlich von einer Vielzahl unabhängiger Sicherheitsforscher:innen geprüft, die mit unterschiedlichen Ansätzen und Fachperspektiven potenzielle Schwachstellen aufdecken, die in klassischen Tests nicht erfasst werden.

Ergänzend setzen wir automatisierte Analysetools ein, die laufend nach sicherheitsrelevanten Mustern und Abweichungen suchen und so unsere Angriffsfläche kontinuierlich überwachen.

Uns ist bewusst, dass sich Fehler nie vollständig ausschließen lassen. Durch die Kombination dieser Verfahren stellen wir jedoch sicher, potenziellen Angriffen frühzeitig begegnen zu können — sowohl durch strukturierte interne Prüfungen als auch durch den kontinuierlichen Einbezug externer Perspektiven.

Sicherheitsaudits für Lieferanten, Drittparteien und Unterauftragsverarbeiter

Für den Betrieb komplexer Systeme ist der Einsatz externer Unterauftragsverarbeiter (z. B. für Hosting und Betrieb) sowie weiterer Drittparteien, etwa Hersteller von Softwarekomponenten, Frameworks oder Bibliotheken, technisch notwendig. Diese Einbindung erfordert jedoch, dass wir uns auf das Sicherheitsniveau aller beteiligten Parteien uneingeschränkt verlassen können.

Unterauftragsverarbeiter im Sinne von Art. 28 DSGVO werden von der HASOMED GmbH vor ihrem Einsatz sorgfältig geprüft und in Auftragsverarbeitungsverträge eingebunden. Dazu gehören insbesondere die Bewertung ihres Informationssicherheitsniveaus, die Prüfung relevanter Zertifizierungen (z. B. ISO/IEC 27001, C5) sowie regelmäßige Audits im Rahmen unseres Informationssicherheits-Managementsystems (ISMS).

Wir begrenzen die Anzahl der eingesetzten Unterauftragsverarbeiter auf das notwendige Minimum und informieren unsere Kund:innen transparent über alle Änderungen. Eine stets aktuelle Liste aller Unterauftragsverarbeiter wird öffentlich zugänglich bereitgestellt.

Für sonstige Lieferanten und Drittparteien, bei denen keine Verarbeitung im Auftrag erfolgt (z. B. bei Softwarebibliotheken oder Hardwarelieferanten), führen wir strukturierte Due-Diligence-Prüfungen durch. Dabei betrachten wir nicht nur formale Nachweise, sondern auch organisatorische Aspekte, etwa:

- Welche Sicherheitsorganisation ist etabliert?
- Wie sehen die Prozesse im Bereich Incident Response oder Schwachstellenmanagement aus?
- Wie transparent kommunizieren die Anbieter über Schwachstellen oder Sicherheitsvorfälle?
- Entspricht das Gesamtbild den Anforderungen an eine belastbare Sicherheitskultur?

So stellen wir sicher, dass wir in der gesamten Lieferkette einen einheitlich hohen Maßstab anlegen — unabhängig davon, ob es sich um Auftragsverarbeiter oder sonstige Drittparteien handelt.

Strukturierte Incident-Response- und Kommunikationsabläufe

Auch bei bestmöglicher Vorbereitung lassen sich Sicherheitsvorfälle nie vollständig ausschließen. Entscheidend ist daher, wie schnell und koordiniert reagiert wird. Aus diesem Grund haben wir bei HASOMED klare Incident-Response-Prozesse etabliert, die technische Analyse, interne Koordination und externe Kommunikation systematisch miteinander verbinden.

Unsere Abläufe folgen definierten Schritten – von der ersten Erkennung über die Bewertung und Eindämmung bis hin zur nachhaltigen Behebung und Dokumentation. Dabei ist festgelegt, welche Rollen zu welchem Zeitpunkt eingebunden werden und wie die Eskalationswege verlaufen. Ein besonderer Schwerpunkt liegt auf der klaren Kommunikation: Sowohl intern zwischen den beteiligten Teams als auch extern gegenüber betroffenen Kund:innen und – falls erforderlich – gegenüber Aufsichtsbehörden.

Darüber hinaus betrachten wir auch sogenannte „near miss situations“ – also Ereignisse, die potenziell kritisch hätten werden können, aber frühzeitig erkannt und entschärft wurden. Diese Fälle fließen systematisch in unsere Lernprozesse ein. Unser Ziel ist nicht nur, Vorfälle effizient zu bearbeiten, sondern die Organisation dadurch langfristig stärker und resilienter zu machen.

Damit folgt unser Sicherheitsansatz dem Prinzip der Anti-Fragilität: Jede Störung oder Herausforderung ist für uns eine Gelegenheit, Strukturen und Abläufe zu verbessern. So entsteht ein System, das nicht nur widersteht, sondern sich kontinuierlich an neue Bedrohungen anpasst und daran wächst.

Für unsere Kund:innen bedeutet das: Im unwahrscheinlichen Fall eines Sicherheitsvorfalls können sie sich darauf verlassen, dass HASOMED schnell, strukturiert und offen reagiert – und dass jeder Vorfall zu noch mehr Stärke im Gesamtsystem führt.

Hasomed®
Praxis. Therapie. Sicherheit.

4

Rechtliche Zulässigkeit & Compliance

Umgang mit (US-)Behördenanfragen

Auch wenn wir für den Betrieb unserer Systeme auf AWS setzen, behalten wir zu jedem Zeitpunkt die vollständige Hoheit über die für die Entschlüsselung erforderlichen Schlüssel. Diese Schlüssel liegen ausschließlich in einem externen Hardware-Sicherheitsmodul (HSM) in Deutschland, betrieben von unserem Partner T-Systems, und sind für AWS nicht zugänglich.

Die öffentliche Diskussion über mögliche Zugriffe ausländischer Behörden auf in der Cloud gespeicherte Daten – etwa im Kontext des US CLOUD Act – zeigt, wie wichtig technische und organisatorische Souveränität in Cloud-Architekturen ist. Der US CLOUD Act sieht vor, dass US-Behörden Cloud-Anbieter mit US-Eigentumsverhältnissen in bestimmten Fällen zur Herausgabe von Daten verpflichten können. Ein solcher Zugriff erfordert einen richterlichen Beschluss eines US-Bundesgerichts und kommt in der Praxis nur in sehr seltenen Ausnahmefällen vor. Gleichwohl berücksichtigen wir dieses Risiko in unserer Sicherheitsarchitektur ausdrücklich:

Alle Daten werden mandantenspezifisch verschlüsselt abgelegt. Da AWS keinen Zugriff auf die zentralen Master Keys hat, könnte der Anbieter selbst im Falle eines rechtlichen Herausgabeverlangens jedoch keine gespeicherten Daten entschlüsseln oder an US-Behörden weitergeben.

Sollten deutsche Behörden rechtmäßige Auskunfts- oder Herausgabeverlangen an uns richten, werden diese Anfragen durch unsere Rechtsabteilung geprüft, mit den zuständigen Aufsichtsbehörden abgestimmt und – sofern personenbezogene Daten betroffen sind – unter Einbeziehung der betroffenen Kund:innen bearbeitet.
So stellen wir sicher, dass ein behördlicher Zugriff ausschließlich auf Grundlage des geltenden deutschen und europäischen Rechts erfolgt und die Rechte unserer Kund:innen jederzeit gewahrt bleiben.

Zertifizierungen & Standards

Unsere Sicherheitsarchitektur und unsere organisatorischen Maßnahmen sind an etablierten internationalen Standards ausgerichtet und werden regelmäßig extern überprüft.

- Die HASOMED GmbH ist nach ISO/IEC 27001 zertifiziert – dem international anerkannten Standard für Informationssicherheits-Managementsysteme (ISMS). Diese Zertifizierung belegt, dass Informationssicherheit bei uns systematisch geplant, umgesetzt und kontinuierlich verbessert wird.

Die HASOMED Tech GmbH erfüllt den C5-Standard (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik (BSI). C5 stellt sicher, dass Cloud-Dienste nach nachvollziehbaren, hohen Sicherheitskriterien betrieben werden.

Wir sehen uns verpflichtet, diese Zertifizierungen dauerhaft aufrechtzuerhalten und regelmäßig zu erneuern. Für unsere Kund:innen bedeutet das, dass unsere Sicherheitsmaßnahmen nicht nur intern definiert, sondern durch unabhängige externe Prüfer bestätigt sind.

DSGVO-Konformität

Die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) ist für uns selbstverständlich – sie bildet die rechtliche Grundlage für jede Verarbeitung personenbezogener Daten. Wichtig ist uns dabei, die Anforderungen der DSGVO nicht nur formal zu erfüllen, sondern ”by design” in unsere Architektur und Prozesse einzubauen.

Zentrale Prinzipien wie Datenminimierung, Zweckbindung, Transparenz, Integrität, Vertraulichkeit und die Wahrung der Betroffenenrechte verstehen wir nicht nur als gesetzliche Vorgaben, sondern als praktische Leitlinien für unseren täglichen Umgang mit sensiblen Gesundheitsdaten.

Damit ist die DSGVO für uns mehr als ein regulatorischer Rahmen: Sie ist ein Gestaltungsprinzip, das wir konsequent in Technik, Organisation und Prozesse übersetzen.

Hasomed®
Praxis. Therapie. Sicherheit.

5

Zusammenarbeit & Ausblick

Sicherheit ist für uns kein abgeschlossener Zustand, sondern eine gemeinsame Aufgabe, die sich ständig weiterentwickelt. Dieses White Paper soll deshalb nicht nur Einblick in unsere aktuellen Prinzipien und Maßnahmen geben, sondern auch zur Diskussion einladen.

Wir möchten offenlegen, wie wir Sicherheit bei HASOMED verstehen, und freuen uns über Rückmeldungen, Kritik und Anregungen. Denn wir sind überzeugt: Nur im konstruktiven Austausch mit unseren Nutzer:innen, Partner:innen und der Fachöffentlichkeit können wir unser Sicherheitsniveau kontinuierlich verbessern und gemeinsam eine verlässliche digitale Gesundheitsversorgung gestalten.