MediPrime
Security Statement

v2018.5.1 – gültig ab 01.05.2018

Das Unternehmen / die Software

Über uns

Die MediPrime GmbH mit Sitz im 3. Wiener Gemeindebezirk wurde Anfang 2018 per Umbenennung und Umstrukturierung der 2015 gegründeten Stonebird IT Solutions GmbH eingetragen. Wir beschäftigen uns mit der Konzeption, Entwicklung und dem Betrieb von Onlineanwendungen im Gesundheitswesen. Innerhalb der letzten 3 Jahre wurde eine sichere, den österreichischen Gesetzen entsprechende Kommunikations- und Verwaltungsplattform für Ärzte (www.docsy.at) und Patienten (www.meinarztonline.at) geschaffen.

Die gesamte Konzeption und Entwicklung findet ausschließlich in Österreich und innerhalb unserers Unternehmens statt.

MediPrime, MeinArztOnline, Docsy & Whitelabelling

Als MediPrime wird die von uns konzipierte, entwickelte und in Instanzen betriebene technologische Basis bezeichnet. Docsy ist ein webbasiertes Ordinations- und Kommunikationssystem für Wahlärzte. MeinArztOnline ist ein Patientenportal zur Verwaltung eigener medizinischer Daten und zur Kommunikation mit den eigenen Ärzten (die Docsy verwenden).

Unsere Technologie ist als Whitelabel-Lösung verfügbar und kann auch selbst gehostet/betrieben werden.

Unser Sicherheitsverständnis

Egal ob Online-Ordinationssoftware (Docsy) oder die von Patienten selbst verwaltete Gesundheitsakte mit Kommunikationsmöglichkeit (MeinArztOnline) – Ärzte und Patienten vertrauen uns die sensibelsten Daten, die es gibt, an. Es ist offensichtlich, dass solch eine Anwendung über das an und für sich unsichere Internet gegen verschiedenste Arten von Angriffen abgesichert warden muss. Wir haben unsere Technologieplattform MediPrime von Beginn an dem Sicherheitsgedanken unterworfen. Unter Sicherheit verstehen wir

- geeignete Entwicklungs-, interne und Betriebsprozesse
- sichere Softwarearchitektur sowie sicheres Hosting
- gesetzeskonformer Betrieb (u.a. ÄrzteG, GTelG, DSGVO/DSG)
- Verfügbarkeit, Vertraulichkeit und Integrität unserer Plattform und Daten

Abläufe & Details

Verschlüsselung und Authentifizierung

Erst beim Aufruf von www.meinarztonline.at/app und www.docsy.at/app landet ein Besucher auf den eigentlichen MediPrime-Seiten. Die Verbindungen sind SHA-1-SSL-verschlüsselt, mit einem 2048 Bit RSA Public-/Private Key Exchange aufgebaut und mit 256 Bit verschlüsselt. Dies gilt nach heutigem Stand der Technik als vollständig sicher.

Aktuell ist der Login mittels Handysignatur oder Bürgerkarte, das Login mittels Benutzername und Passwort sowie eine Kombination möglich. Vor dem ersten Login mittels Handysignatur/Bürgerkarte muss der Account einmalig mit der eigenen Identität bestätigt werden. Dies kann in der "Profil"-Sektion von Docsy/MeinArztOnline nach dem Einloggen gemacht werden.

Bei Whitelabel-Lösungen ist eine verpflichtende Verwendung von Handysignatur/Bürgerkarte (GTelG-konforme GDA-Kommunikation) oder/und eine alternative 2-Faktor-Authentifizierung (z.B. für Patienten) möglich.

Brute-Force Schutz & Serversicherheit

Wenn Interessenten uns zur MediPrime-Sicherheit befragen, spielt das Thema Verschlüsselung eine große Rolle. Verständlicherweise ist die Möglichkeit, dass Dritte eine Verbindung einsehen oder sogar Daten abgegriffen werden können, gefürchtet. In der Praxis sind es dann aber oft ganz primitive Angriffe, die am gefährlichsten sind. Dieser Abschnitt gilt nur für den Zugriff per Benutzername und Kennwort, nicht durch die Handysignatur/Bürgerkarte (dieser ist über das A-Trust-System abgesichert).

Die Anzahl der möglichen Logins auf einen Account (eine Mailadresse) ist softwareseitig auf 10 Versuche limitiert, danach ist der Account gesperrt und muss durch einen Administrator wieder aktiviert warden (Kontaktaufnahme per Mail und Telefon möglich). Weiters werden IP-Adressen, die zu oft unerfolgreich auf Serverressourcen (Services, Ports) zugreifen, blockiert. Auf dem Server werden alle nicht für unsere Software bzw. die Verwaltung benötigten Ports gesperrt. Wir prüfen alle Serverdateien laufend auf Integrität.

Hosting & Datencenter

Die Verfügbarkeit als auch Sicherheit ist vom Standort des Servers abhängig. Die zentralen MediPrime-Server befinden in einem Rechenzentrum (Internexx) in Wien (Österreich), das nach ISO 27001 zertifiziert ist, und multiredundante Carrier-Anbindung und redundante Stromversorgung besitzt. Es wird ausschließlich Markenhardware eingesetzt. Es gibt personenbezogene Zutrittsüberwachung, Videokameras, Bewegungsmelder, 24/7-Überwachung und Vor-Ort-Sicherheitspersonal.

Technische Details

Datenspeicherung

Alle sensiblen Daten (bzw. "besondere Kategorien personenbezogener Daten" lt. DSGVO) werden per PBEWithHmacSHA256AndAES_256 verschlüsselt in der Datenbank gespeichert. Ein auf Funktionsniveau heruntergebrochenes Rechtesystem garantiert, dass nur berechtigte Nutzer auf Daten zugreifen können.

Änderungen an Daten warden in Revisionstabellen gesichert, damit kann jede Datenmanipulation nachvollzogen werden.

Benutzer-Dokumente werden auf unseren Servern verschlüsselt abgelegt. Für die Verschlüsselung wird der password-based ByteEncryptor aus dem Spring Security Crypto Modul verwendet.

Webattacken / Login

SSL3 haben wir in der Apache2 Konfiguration deaktiviert. Die CSRF-Protection von Spring Security ist konfiguriert. HSTS-Token werden gesendet. Thymleaf's th:text bereinigt Text in den Views um XSS-Angriffe zu vermeiden. Wir bieten bewusst keine Remember-Me-Funktionalität an. Um starke Benutzer-Passwörter zu fördern, wird ein Password-Stärke-Meter angezeigt.

Verwendete Komponenten (Software-Stack)

Die MediPrime-Technologie ist eine MVC-basierte WebApp, die mit Java 8 und dem Spring Framework entwickelt wurde. Auf dem Server laufen Debian 8, Apache+Tomcat, MySQL. Mailtechnisch ist ausschließlich ein SSMTP-Agent installiert; unsere Mailserver sind managed in einem anderen österreichischen Rechenzentrum.

Weitere Details stehen nur nach persönlichem, projektbezogenen Kontakt zur Verfügung.

Rechtliche Details

DSG/DSGVO

Wir haben von Beginn an auf ein rechtlich gesichertes Datenschutzkonzept geachtet. Mit Dr. Knyrim (www.kt.at) haben wir hierzu einen starken Partner gewinnen können, mit dem wir die Grundlagen unserer Plattform auch publiziert haben: https://rdb.manz.at/document/rdb.tso.LIdako20160403.

Mit dem österreichischen DSG2000 haben wir bereits ein sehr starkes Datenschutzgesetz umgesetzt. Die Einführung der DSGVO ändert vergleichsweise wenig; es werden Informationspflichten, die Datenschutzerklärung, und Löschfristen eingeführt bzw. ergänzt sowie die erforderlichen internen Prozesse und Dokumentationen erstellt. Aus DSGVO-Sicht sind wir für die meisten (Patienten-)Daten Auftragsverarbeiter, sowohl aus Sicht der Ärzte als auch aus Sicht der Patienten. Verantwortliche im Sinne der DSGVO sind wir für selbst erhobene bzw. kombiniert weiterverarbeitete Daten.

ÄrzteG

Alle betroffenen Rechte und Pflichten des ÄrzteG sind auf Docsy bzw. MeinArztOnline ebenfalls umgesetzt. Unser Archiv- und Revisionssystem sorgt für eine sichere Dokumentation. Die Verantwortlichkeit für medizinische Beratung, der Annahme der digitalen Betreuung des Patienten, die Leistungsanbietung sowie die Haftung bleibt beim Arzt. Als Plattform stellen wir rein den sicheren Übertragungskanal zur Verfügung.

GTelG und Gesundheitstelematikverordnung (GTelVO)

Gemäß GTelVO muss die identität von Gesundheitsdiensteanbietern mittels elektronischer Signaturen (oder dem nicht existenten eHealth-Verzeichnisdienst) überprüft werden. Dies stellen wir durch die Verwendung der Bürgerkarte/Handysignatur sicher. Nach §1 (2) sowie insbesondere §6 ist die Verwendung einer elektronischen Signatur kein Muss, wir empfehlen die Verwendung aber dringend. Für Whitelabel-Lösungen gibt es die Möglichkeit, ausschließlich Login per Signatur anzubieten.

Vertraulichkeit und Integrität sind zwei fest verankerte Bausteine der IT-Sicherheit, diese werden explizit im Gesetzestext behandelt. §6 (3) GTelG erlaubt explizit die Datenspeicherung mittels “Cloud Computing”, sofern die Daten mit einem dem aktuellen Stand der Technik entsprechenden Verfahren verschlüsselt wurden. Die erlaubten Algorithmen werden angegeben. Unser Datensicherheits- und Verschlüsselungskonzept ist GTelVO-konform und wird weiter oben beschrieben. Die Integrität der Gesundheitsdaten wird durch Benutzerkennung, verschlüsselter Übertragung/Speicherung und dem Revisionssystem (Datum/Account/Version) sichergestellt.

Die Dokumentation des IT-Sicherheitskonzeptes ist sowohl im GTelG als auch in der DSGVO verankert.

Weitere Fragen?

Wir stehen Ihnen bei Fragen unter office@mediprime.eu sowie + 43 (0) 1 890 57 65 zur Verfügung.

Unser Ansprechpartner für Datensicherheit und Datenschutz ist:
Dr. Christoph Berdenich, BSc.
christoph.berdenich@mediprime.eu
+43 (0)1 890 5765

Unsere Produkte finden Sie online unter:
www.meinarztonline.at
www.docsy.at

Kontakt

MediPrime GmbH
Hetzgasse 12
1030 Wien

E-Mail: office@mediprime.eu *(Bevorzugt)*
Telefon: +43 (0) 1 890 57 65 *(Mo-Fr, 10-17 Uhr)*
Mobil: +43 (0) 699 13 113 200 *(Mo-Fr, 10-17 Uhr)*

Geschäftsführung: Dr. Christoph Berdenich, BSc | Dipl.-Ing. Domenik Muigg
Handelsgericht: Wien| Firmensitz: 1030 Wien | Firmenbuchnummer: FN 416669z | Steuernummer/UID: ATU68759211 | DVR-Nummer 4015612