# MediPrime
# Security Statement

v2022.1 – gültig ab 01.01.2022

## 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. Inzwischen gibt es zwei Firmenstandorte in Wien und Innsbruck. Wir beschäftigen uns mit der Konzeption, Entwicklung und dem Betrieb von Onlineanwendungen im Gesundheitswesen. Innerhalb der letzten Jahre wurde eine sichere, den österreichischen Gesetzen entsprechende Kommunikations- und Verwaltungsplattform für Ärzte (www.docsy.at) und Patienten (www.meinarztonline.at), sowie die Kommunikationsplattform (www.mediprime.app) geschaffen.

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

### MediPrime (MeinArztOnline, docsy) und mediprime.app

Als MediPrime Plattform wird die von uns konzipierte, entwickelte und betriebene technologische Basis bezeichnet, welches 2 User-Interfaces besitzt. 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).

Als mediprime.app wird die von uns konzipierte, entwickelte und betriebene Lösung bezeichnet, welche auch von anderen Patientenverwaltungssystemen über eine ebenfalls zur Verfügung gestellt API genutzt werden kann.

## Unser Sicherheitsverständnis

Egal ob Online-Ordinationssoftware (docsy), die von Patienten selbst verwaltete Gesundheitsakte mit Kommunikationsmöglichkeit (MeinArztOnline) oder die Kommunikations-App (mediprime.app) – 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 werden muss. Wir haben unsere Technologieplattformen 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, www.docsy.at/app oder www.mediprime.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 auf der MediPrime Plattform 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 der mediprime.app ist ausschließlich eine 2-Faktor-Authentifizierung mittels E-Mail-TAN, SMS TAN oder einer OTP-App 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 werden (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 (Internex GmbH) 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. Siehe auch: Anhang – TOMs unsere Hosters.

## Technische Details

### Datenspeicherung

Ein auf Funktionsniveau heruntergebrochenes Rechtesystem garantiert, dass nur berechtigte Nutzer auf sensible Daten (bzw. "besondere Kategorien personenbezogener Daten" lt. DSGVO) Daten zugreifen können.

Änderungen an Daten werden 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 Web-Anwendung, die mit Java 8, Kotlin, Spring Framework, Thymeleaf und React entwickelt wurde. Auf dem Server laufen Debian 9, Apache+Tomcat, MariaDB. 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.

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.

# Technisch organisatorische Maßnahmen unseres Hosting-Partners (nach Art. 32 EU-DSGVO)

Für den Betrieb unserer Plattform und Services, und somit auch zur Speicherung unserer Kundendaten greifen wir auf einen Hostingpartner zurück. Deswegen sind zur Datensicherung folgenden technisch organisatorischen Maßnahmen gültig. Diese werden von der internex GmbH, Lagerstraße 15, 3950 Gmünd gestellt.

## *1. Zutrittskontrolle*

Maßnahmen um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Rechenzentren erhalten, in welchen personenbezogene Daten verarbeitet werden.

**Gebäudesicherung**

- Gebäude- und Infrastruktur Monitoring
- Videoüberwachung
- Automatisches Zutrittskontrollsystem
- Absicherung von Gebäudeschächten außerhalb der Perimeter Abgrenzung
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal und Wachpersonal
- Schriftliche Zutrittsregelungen

**Sicherung der Räume**

- Biometrische Zutrittskontrolle zum Rechenzentrumsbereich
- Zutrittskarte für den Zutritt zu einem Rechenzentrumsraum

## *2. Zugangskontrolle*

Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können.

**Zugang zu den Serversystemen (Authentifizierung)**

- Server-Passwörter und Zugänge werden dem Auftraggeber bei der erstmaligen Inbetriebnahme übergeben. Der Auftraggeber ändert die Passwörter selbstständig sofort nach der Übernahme und wählt ein komplexes Passwort unter Berücksichtigung allgemeingültiger Standards.
- Auftraggeber verwaltet die Zugangsdaten selbstständig und ist für deren Sicherheit und periodische Änderungen verantwortlich.

## *3. Zugriffskontrolle*

Maßnahmen für berechtigte Administratoren zur Benutzung von internen Serversystemen zur Verwaltung.

- Berechtigungskonzept inkl. Rollendefinition
- Passwortpolicy (Mindestlänge, Sonderzeichen, periodischer Wechsel)
- Social Engineering Prevention
- Mehr-Weg-Authentifizierung

Die Verantwortung der Zugriffskontrolle von Kundensystemen obliegt dem Auftraggeber.

## *4. Weitergabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)*

Maßnahmen, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der beauftragten Leistung des Hauptauftrages zur Verfügung gestellt. Der Auftraggeber bewertet seine

betriebenen Datenverarbeitungsanwendungen und beauftragt auf Basis dessen erforderliche technische Maßnahmen.
- Alle Mitarbeiter sind unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

## *5. Eingabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)*

Maßnahmen bei internen Serversystemen um sicherzustellen, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

- Protokollierung über Logfiles
- Benutzeridentifikation

## *6. Auftragskontrolle (Art. 32 Abs. 1 lit. d DSGVO)*

Maßnahmen, dass personenbezogene Daten gemäß den Weisungen des Auftraggebers verarbeitet werden.

- Definition der Weisungsbefugnisse lt. Kundenanforderung
- Auftragsannahme nur in Schriftform oder von autorisierten Personen

## *7. Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. b DSGVO)*

Maßnahmen bei internen Serversystemen zur Verwaltung um sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

- Brandschutzmaßnahmen
- Überspannungsschutz
- Unterbrechungsfreie Stromversorgung
- Klimaanlage (Redundantes System)
- Luftfeuchtigkeit zwischen 40% und 60%
- 24/7 Monitoring der Serversysteme
- Separate Brandabschnitte
- Backupkonzept für interne Serversysteme zur Verwaltung

Auf Kundensystemen oder Serversystemen des Auftraggebers obliegt die Verantwortung der Verfügbarkeitskontrolle, insbesondere der Datensicherung, dem Auftraggeber, falls dies nicht schriftlich im Hauptvertrag anders vereinbart wurde.

## *8. Trennungsgebot*

Maßnahmen, dass personenbezogene Daten auf internen Serversystemen, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

- Getrennte Systemstrukturen der internen IT
- Getrennte Datenbanken

Die Trennungskontrolle bei Kundenservern oder Serversystemen des Auftraggebers obliegt dem Auftraggeber.

## *9. Abgrenzung*

Abgrenzung bei unsachgemäßer Handhabung der Hard- bzw. Software durch den Kunden. Insbesondere gilt dies bei folgenden Vorgängen:

- Datendiebstahl, welcher durch die Applikation/Webanwendung möglich wurde
- Datendiebstahl, welcher durch unachtsamen Umgang des Auftraggebers mit Zugangsdaten oder mit sonstigen sicherheitsrelevanten Schutzmechanismen möglich wurde
- Unbefugter Zugriff, welcher durch unachtsames Vorgehen vom Auftraggeber oder einem vom Auftraggeber dazu berechtigten Unternehmen ermöglicht wurde

- Für die Datenverarbeitung, Datensicherheit und Einhaltung der gesetzlichen Vorschriften auf Applikationsebene (z.B.: Webseite, Webanwendung, App,…) ist der Auftraggeber verantwortlich
- Vom Auftraggeber nicht autorisierte Veränderungen an Dateien oder Datenbanken, welche von einem berechtigten Unternehmen selbständig durchgeführt wurden
- Systeme, die nicht nach den Richtlinien des Herstellers betrieben und gewartet wurden

## Technisch organisatorische Maßnahmen MediPrime GmbH

Zusätzlich zu den technisch organisatorischen Maßnahmen unseres Hosters ergreifen wir folgende Maßnahmen.

**Authentifizierung**

- Account-Passwörter und Zugänge werden unseren Kunden bei der erstmaligen Inbetriebnahme übergeben. Der Kunde ändert die Passwörter selbstständig sofort nach der Übernahme und wählt ein komplexes Passwort unter Berücksichtigung allgemeingültiger Standards.
- Der Kunde verwaltet die Zugangsdaten selbstständig und ist für deren Sicherheit und periodische Änderungen verantwortlich.
- Es wird empfohlen, die Authentifizierung durch Handy-Signatur oder Bürgerkarte zu aktivieren, und die Authentifizierung durch Usernamen und Passwort zu deaktiveren.

**Zugriffskontrolle**
Dies beinhaltet Maßnahmen für Administratoren der MediPrime GmbH zur Verwaltung der Plattform.

- Berechtigungskonzept inkl. Rollendefinition
- Passwortpolicy (Mindestlänge, Sonderzeichen, periodischer Wechsel)
- Social Engineering Prevention
- verpflichtende Mehr-Weg-Authentifizierung (Handy-Signatur)
- Mitprotokollierung jedes Zugriffes

**Weitergabekontrolle**
Maßnahmen, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

- Die gesamte Verbindung inkl. Datenübertragung von und zur Plattform ist verschlüsselt
- Alle Mitarbeiter sind unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

**Eingabekontrolle**
Maßnahmen bei internen Serversystemen um sicherzustellen, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

- Protokollierung über Logfiles sowie Audit-Tables
- Benutzeridentifikation

**Auftragskontrolle**
Maßnahmen, dass personenbezogene Daten gemäß den Weisungen des Auftraggebers verarbeitet werden.

- Definition der Weisungsbefugnisse lt. Kundenanforderung
- Auftragsannahme nur in Schriftform oder von autorisierten Personen
- zusätzliche textuelle Protokollierung bei Zugriffen auf Kundenaccounts

**Abgrenzung**
Abgrenzung bei unsachgemäßer Handhabung der Software durch den Kunden. Insbesondere gilt dies bei folgenden Vorgängen:

- Datendiebstahl, welcher durch unachtsamen Umgang des Kunden mit Zugangsdaten oder mit sonstigen sicherheitsrelevanten Schutzmechanismen möglich wurde
- Unbefugter Zugriff, welcher durch unachtsames Vorgehen vom Kunden oder einem vom Kunden dazu berechtigten Personen oder Unternehmen ermöglicht wurde

## 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.
datenschutz@mediprime.eu
+43 (0)1 890 5765

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

## Kontakt

MediPrime GmbH
Mohsgasse 11/3-5
1030 Wien

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

Handelsgericht: Wien| Firmensitz: 1030 Wien | Firmenbuchnummer: FN 416669z | Steuernummer/UID: ATU68759211