

Datenschutzerklärung für Patienten

(Stand Mai 2018)

Letzte Aktualisierung **15.05.2018**.

Die MediSoftware bietet für die Arztpraxis-Software PRAXIS-PROGRAMM die zusätzliche Web-Software MediDate zur Datenverarbeitung an, die ausschließlich über Web-Browser zu erreichen ist und als PlugIn in den Webaufruf der nutzenden Arztpraxis eingebunden wird. Die Anwendungen werden von der jeweiligen Arztpraxis angeboten und können von natürlichen Personen (Nutzer) kostenlos genutzt werden.

Die persönlichen und medizinischen Daten, die durch die Eingabe in die Anwendungen erfasst werden, sind sehr sensibel und werden daher mit höchster Effektivität und Sicherheit bereits unmittelbar bei der Eingabe durch asymmetrische, zertifikatsbasierte Verschlüsselungsverfahren geschützt. Die Datenschutzgesetze von Deutschland (wie das Telemediengesetz (TMG), das Bundesdatenschutzgesetz (BDSG), die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (TKG)) und die gesetzgeberischen Vorgaben auf EU-Ebene (Europäische Datenschutz-Grundverordnung (EU-DSGVO)) sollen dabei sicherstellen, dass das Selbstbestimmungsrecht auch beim Umgang mit den Daten der Nutzer zur Geltung kommt und die Privatsphäre jedes Einzelnen gewahrt bleibt. MediSoftware als Hersteller der Web-Software MediDate sorgt für die Einhaltung dieser Datenschutzgesetze und unterliegt der Kontrolle und Aufsicht des schleswig-holsteinischen Unabhängigen Landeszentrum für den Datenschutz (ULD).

So werden aufgrund der speziellen Sensibilität der Nutzerdaten diese grundsätzlich mit vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in den Technischen Richtlinien TR-02102 (https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_hm.html) empfohlenen Verfahren kryptografisch gesichert und damit mit einem optimalen Sicherheitsstandard geschützt. MediSoftware hat zu keinem Zeitpunkt Einblick in die Nutzerdaten sowie ein umfassendes Datenschutz- und Sicherheitskonzept über den (1) Datenzugang, (2) Datenverarbeitung, (3) Datentransfer und (4) Datenspeicherung erstellt, welches der Sensibilität der Daten gerecht wird.

1 Datenzugang in MediDate

Sämtliche Daten werden von dem jeweiligen Nutzer selbst angelegt und aktualisiert. Zur eindeutigen Identifizierung der Nutzer wird lediglich ein Hash-Wert seiner E-Mail-Adresse in MediDate gespeichert. Diese Daten benötigt MediDate, um die Kommunikation zwischen Arztpraxis und Nutzer zuordnen zu können (z.B. Terminbestätigung, Terminabsage, Terminverschiebung). Die Nutzer haben zudem die Möglichkeit, je nach von der Arztpraxis freigeschalteter Anwendungen, zusätzliche Informationen zu hinterlegen. Die Nutzer von MediDate entscheiden allein, welche Daten sie eingeben und speichern. Der Nutzer/Kunde ist allerdings selber für die Sicherheit seines eigenen Computers und seiner eigenen Software verantwortlich und für den entsprechenden Schutz zu sorgen.

Alle vom Nutzer erfassten Daten bleiben solange verschlüsselt auf Systemen von MediSoftware als Betreiber der MediDate-Plattform zwischengespeichert, bis die Arztpraxis, die die Anwendungen anbietet,

die (Buchungs-)Daten abgeholt und in das praxisinterne EDV-System übernommen sowie die Buchung bestätigt hat.

Wenn der Nutzer das Nutzungsverhältnis mit der Arztpraxis beenden möchte – was jederzeit möglich ist – , wird das zugehörige Nutzerprofil innerhalb der Praxis (im Rahmen der geltenden gesetzlichen Dokumentationspflichten des Heilberufers) einschließlich aller in MediDate hinterlegten Daten vollständig und unwiderruflich gelöscht. Informationen (wie Termine oder Nachrichten), die der Nutzer an die Arztpraxis versendet hat, bleiben als Eingangsnachrichten beim Arzt erhalten, da diese Informationen in den Besitz des Arztes übergegangen sind.

2 Generelle Datenverarbeitung

Weder Angestellte der MediSoftware noch Dritte können aufgrund der asymmetrischen Verschlüsselung (Public-/Private-Key-Verfahren) Zugriff auf Daten, die auf den Servern von MediSoftware zwischengespeichert sind, erhalten.

Um bei einem Zugriff auf die Daten die Datumsangaben des letzten Zugriffs für den Nutzer anzuzeigen und gegebenenfalls nach einer längeren Zeit der Nicht-Nutzung Erinnerungs- und Löschungsrouinen einleiten zu können, werden diese Datumsangaben durch MediSoftware verarbeitet. Es werden aber dazu keine betreffenden Nutzungs- bzw. Kundenprofile erstellt, sondern dem Nutzer nur eine Art generelles Logbuch über seine vergangenen Anmeldungen angezeigt. Dabei wird nicht gezeigt und/oder gespeichert, was der Nutzer/Kunden konkret getan oder verändert hat, sondern es wird nur generell angezeigt, ob er im persönlichen Benutzerkonto aktiv war.

Darüber hinaus verwendet MediDate 'Session-Cookies'. Session-Cookies sind kleine Dateien, die im Speicher des Rechners vom Nutzer/Kunden gespeichert werden, um das Sitzungs-Konzept der MediDate-Plattform zu unterstützen. Es handelt sich dabei nur um so genannte temporäre Dateien, die automatisch wieder gelöscht werden, nachdem der Nutzer die aktuelle MediDate-Sitzung beendet hat. In keinem Fall erhält eine dritte Partei die Möglichkeit, über die Internet-Seiten von MediDate Cookies bei den Nutzern/Kunden zu hinterlegen.

Die personenbezogenen Angaben der Nutzer werden nicht an Dritte weitergegeben, wenn der Nutzer dazu nicht ausdrücklich sein Einverständnis erteilt hat oder MediSoftware zur Herausgabe verpflichtet ist, beispielsweise aufgrund einer gerichtlichen oder behördlichen Anordnung.

3 Verschlüsselung des Datentransfers bzw. der Kommunikation

Der Transfer der Daten vom Computer des Nutzers zum MediDate-Server wie auch umgekehrt das Herunterladen von Daten vom MediDate-Server auf den Computer des Nutzers ist verschlüsselt. MediDate benutzt hierfür den aktuellen Verschlüsselungsstandard SSL (Secure Socket Layer, Version 3.0). Dieses bewährte kryptographische Verfahren wird weltweit als Standard für hochsensible Transaktionen im Internet verwendet, wie beispielsweise im Online-Banking und bei sensiblen Internet-Anwendungen im Gesundheitsbereich. Es kombiniert einen 2048 Bit langen öffentlichen Schlüssel mit einem symmetrischen Schlüssel in der Länge von 256 Bit. Am Schlosssymbol im Browser-Fenster ist erkennbar, ob die Informationen geschützt übermittelt werden und welche Verschlüsselungslänge im Browser unterstützt

wird. Die Authentizität des Verschlüsselungscodes von MediDate wird durch das SSL-Zertifikat bestätigt. Über einen Doppelklick auf das Schlüsselsymbol am unteren Bildrand erfährt der Nutzer mehr über das Zertifikat.

4 Verschlüsselung der Datenspeicherung

Die Daten der Nutzer werden nicht nur verschlüsselt übermittelt, sondern auch ausschließlich verschlüsselt gespeichert. Dadurch wird der Zugriff auf die Nutzerdaten durch Dritte nicht nur organisatorisch, sondern auch technisch verhindert. Die Daten des Patienten werden bereits lokal auf dem Rechner des Patienten verschlüsselt und erst danach zu den MediDate-Servern übertragen. Dafür wird ein mehrstufiges System aus symmetrischen und asymmetrischen Verschlüsselungsalgorithmen verwendet, so dass weder Administratoren und Mitarbeiter von MediSoftware noch Dritte diese Daten im Klartext lesen können. Zum Entschlüsseln der dafür nötigen Schlüssel ist es zwingend nötig, den privaten Schlüssel der Arztpraxis zu kennen. Sämtliche verwendeten Kryptographierungs-Algorithmen entsprechen der Technischen Richtlinie TR-02102 („Kryptographische Verfahren: Empfehlungen und Schlüssellängen“) des Bundesamtes für Sicherheit in der Informationstechnik.

Zur sicheren, physischen Verwahrung der Nutzer/Kunden Daten arbeitet MediSoftware mit einem externen, großen Internet-Provider (derzeit: Microsoft Deutschland GmbH, Siemensstraße 27 · 61352 Bad Homburg). Die genutzten Server befinden sich ausschließlich in Europa. Nur besonders autorisierte Personen (etwa von Service-Unternehmen zu Wartungsarbeiten) haben Zugang zu den gesicherten Räumen. Aufgrund der verschlüsselten Datenspeicherung können diese Personen nicht auf die Kunden-/Nutzerdaten zugreifen. Der Provider gewährleistet den Einsatz moderner Firewall-Technologie und physikalisch gesicherter Einrichtungen.

Der Aufgabenbereich des Providers beinhaltet lediglich die Sicherstellung der Verfügbarkeit der Infrastruktur des Rechenzentrums (Strom, Internet, Routing) sowie der gemieteten Hardware (z.B. Austausch defekter Komponenten). Auf die Server selbst haben nur Administratoren von MediSoftware Zugriff.

5 Auskunfts- und Widerrufsrecht

Der Nutzer erhält jederzeit ohne Angabe von Gründen kostenfrei Auskunft über seine bei MediSoftware gespeicherten Daten. Er kann jederzeit seine bei MediSoftware erhobenen Daten sperren, berichtigen oder löschen lassen. Auch kann er jederzeit die etwaig ggü. MediSoftware erteilte Einwilligung zur Datenerhebung und Verwendung ohne Angaben von Gründen widerrufen.

Sollten Sie weitere Fragen haben, so können Sie sich gerne an uns wenden: MediSoftware, Steinstraße 1, 24118 Kiel, Tel. +49 (0)431 88687-0, E-Mail: medidate@medisoftware.de.

MediSoftware überprüft regelmäßig und durchgängig die Einhaltung dieser Datenschutzbestimmungen und lässt sich hierzu von einer externen, unabhängigen Firma prüfen (derzeit: ATOS, <https://atos.net/de/deutschland>). Erhält MediSoftware formale Beschwerdeschriften, wird sie mit dem Verfasser bezüglich seiner Bedenken Kontakt aufnehmen, um eventuelle Beschwerden hinsichtlich der

Verwendung von persönlichen Daten zu lösen. MediSoftware verpflichtet sich, dazu kooperativ mit den entsprechenden Behörden, einschließlich lokaler Datenschutzbehörden, zusammenzuarbeiten.

Ein Angebot der MediSoftware

Steinstraße 1,
24118 Kiel,
Deutschland

Telefon: +49 (0)431 88687-0

Fax: +49 (0)431 88687-88

E-Mail: medidate@medisoftware.de

Website: www.medisoftware.de

Vertretungsberechtigt: Dipl.Phys.Jan Meincke

UStID: DE134835986