Datenschutzrichtlinie medatixx

Diese Datenschutzrichtlinie gilt für die Software „medatixx" der medatixx GmbH & Co. KG. Der Schutz Ihrer persönlichen Daten liegt uns sehr am Herzen. An dieser Stelle möchten wir Sie daher über den Datenschutz in unserem Unternehmen informieren. Selbstverständlich beachten wir die gesetzlichen Bestimmungen des Datenschutzgesetzes (BDSG), des Telemediengesetzes (TMG) und andere datenschutzrechtliche Bestimmungen.

Gegenstand des Datenschutzes

Gegenstand des Datenschutzes sind personenbezogene Daten. Diese sind nach § 3 Abs.1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hierunter fallen z. B. Angaben wie Name, Post-Adresse, E-Mail-Adresse oder Telefonnummer, ggf. aber auch Nutzungsdaten wie Ihre IP-Adresse.

Erhebung und Speicherung von Nutzungsdaten

Zur Lizenzprüfung der erworbenen Software, zur Kundendatenpflege sowie zur Prüfung, ob Updates der Software medatixx notwendig sind, sammeln und speichern wir personenbezogene Daten. Diese Daten werden ausschließlich für den internen Gebrauch gespeichert. In der Folge finden Sie jene Daten, welche durch die Nutzung der Software medatixx an uns übermittelt werden (sofern die entsprechenden Felder in Ihrer Software ausgefüllt sind):

Betriebsstättenbezogene Daten:

1. Bezeichnung
2. Betriebsstättenart (Haupt- oder Nebenbetriebsstätte)
3. (N)BSNR
4. KV-Bezirk
5. PLZ, Straße, Ort
6. Telefonnummer
7. Faxnummer
8. Homepage

Daten der zugeordneten Ärzte:

9. Anzahl der zugeordneten Ärzte
10. Nachname
11. Vorname
12. Namenszusatz
13. Titel
14. LANR

15. E-Mail
16. Geburtsdatum
17. Berechtigt bis

Weitere Daten:

18. Name Arbeitsplatz mit Rechner- und Netzwerkname
19. Versionsnummer des medatixx-Servers bzw. Updatestand (mit Einspieldatum)
20. Verwendete Cloud-Version (verwendete URL)
21. Letzte Einträge der Error-Logdatei
22. Letzte Anmeldung in medatixx
23. Anzahl der Arbeitsplätze
24. Anzahl der angelegten Mitarbeiter
25. Hardwarekomponenten des medatixx-Servers
    - CPU-ID
    - Host-ID
    - Grafikkarten-Beschreibung
    - Computermodell-ID
    - Arbeitsspeichergröße
    - Seriennummer des C-Laufwerks
    - Netzwerkadapter
        - MAC-Adresse
        - Beschreibung
        - Status
        - Adaptertyp (Ethernet, Wifi etc.)
        - IP-Adresse

Cookies

Wir verwenden keine Cookies.

Zweckgebundene Datenverwendung

Wir beachten den Grundsatz der zweckgebundenen Datenverwendung und erheben, verarbeiten und speichern Ihre personenbezogenen Daten nur für die Zwecke, für die Sie sie uns mitgeteilt haben. Eine Weitergabe Ihrer persönlichen Daten an Dritte erfolgt nicht ohne Ihre ausdrückliche Einwilligung, sofern dies nicht zur Erbringung der Dienstleistung oder zur Vertragsdurchführung notwendig ist. Auch die Übermittlung an auskunftsberechtigte staatliche Institutionen und Behörden erfolgt nur im Rahmen der gesetzlichen Auskunftspflichten oder wenn wir durch eine gerichtliche Entscheidung zur Auskunft verpflichtet werden.

Auch den unternehmensinternen Datenschutz nehmen wir sehr ernst. Unsere Mitarbeiter und die von uns beauftragten Dienstleistungsunternehmen sind von uns zur Verschwiegenheit und zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet worden.

Haftungsausschluss

Die Inhalte der Software medatixx werden mit größter Sorgfalt recherchiert und implementiert. Fehler im Bearbeitungsvorgang sind dennoch nicht auszuschließen. Hinweise und Korrekturen senden Sie bitte an uns.

Neben unserer Software liefern wir unter Umständen Fremdkomponenten aus, welche für den Betrieb von medatixx notwendig sind, z.B. Betriebssystemkomponenten. Für diese trägt der jeweilige Hersteller das Haftungsrisiko.

Sofern wir Ihnen weitere, für den Betrieb von medatixx nicht notwendige Komponenten ausliefern, welche von Ihnen optional verwendet werden können, wie z.B. Gerätetreiber, so liegt das Haftungsrisiko beim Hersteller (z.B. beim Druckerhersteller für Druckertreiber).

Auskunft- und Widerrufsrecht

Sie erhalten jederzeit ohne Angabe von Gründen kostenfrei Auskunft über Ihre bei uns gespeicherten Daten. Sie können jederzeit Ihre bei uns erhobenen Daten sperren, berichtigen oder löschen lassen. Auch können Sie jederzeit die uns erteilte Einwilligung zur Datenerhebung und Verwendung ohne Angaben von Gründen widerrufen. Wir stehen Ihnen jederzeit gern für weitergehende Fragen zu unseren Hinweisen zum Datenschutz und zur Verarbeitung Ihrer persönlichen Daten zur Verfügung. Adressieren Sie Ihre Fragen gerne an datenschutz@medatixx.de.

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im oben genannten Vertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1. Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung

1.1 Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	Kreis der Betroffenen
Personenstammdaten	Ärzte, Praxispersonal, Patienten
Kommunikationsdaten (z.B. Telefon, E-Mail)	Ärzte, Praxispersonal, Patienten
Vertragsstammdaten	Praxisinhaber, Vertretungsberechtigter
Vertragsabrechnungs- und Zahlungsdaten	Praxisinhaber, Vertretungsberechtigter - sobald mindestens ein Zusatzmodul gebucht wurde und / oder keine DGS-Mitgliedschaft besteht
Praxisdaten	Ärzte, Praxispersonal
Behandlungsdaten	Patienten

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

2. Anwendungsbereich und Verantwortlichkeit

2.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»verantwortliche Stelle« im Sinne des § 3 Abs. 7 BDSG).

2.2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

3. Pflichten des Auftragnehmers

3.1. Der Auftragnehmer darf Daten von Betroffenen nur im Rahmen des Auftrages erheben, verarbeiten oder nutzen.

3.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) genügen. Diese Maßnahmen werden in Anlage 3 (Technische und organisatorische Maßnahmen) festgelegt.
Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.3. Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Informationen zur Verfügung, sofern er sie sich nicht selbst beschaffen kann.

3.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis entsprechend § 5 BDSG). Das Datengeheimnis besteht auch nach Beendigung des Auftrages fort.

3.5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten nach § 42a BDSG.

3.6. Der Auftragnehmer nennt dem Auftraggeber auf Verlangen den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

3.7. Der Auftragnehmer gewährleistet, seinen Pflichten nach §§ 4f, 4g BDSG nachzukommen (§ 11 Abs. 2 Nr. 5 i.V.m. § 11 Abs. 4 BDSG), wie z.B. seiner Pflicht, einen Datenschutzbeauftragen zu bestellen, soweit vom Gesetz vorgeschrieben.

3.8. Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.

3.9. Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die Anweisung erfolgt über ein Formblatt, welches Anlage zum Vertrag ist.

3.10. Alle Daten liegen auf verschlüsselten virtuellen Festplatten auf physikalischen Servern (siehe Anlage „Technische und organisatorische Maßnahmen"), auf die virtuelle Server zugreifen. Werden virtuelle Maschinen ersetzt (gelöscht), dann werden diese virtuellen Speicher unwiderruflich gelöscht. Physikalische Medien werden durch zertifizierte Akten- und Datenträgervernichter zerstört.

4. Pflichten des Auftraggebers

4.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2. Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.

5. Anfragen Betroffener

5.1. Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.

5.2. Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

6. Kontrollpflichten

6.1. Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen oder sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen.

6.2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

7. Subunternehmer

7.1. Eine Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer erfolgt nicht.

7.2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung.
Der Auftragnehmer wird mit Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

8. Informationspflichten, Schriftformklausel, Rechtswahl

8.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »verantwortlicher Stelle« im Sinne des Bundesdatenschutzgesetzes liegen.

8.2 Zur Gewährleistung eines Beschlagnahmeschutzes gem. § 97 Abs. 2 StPO gewährleistet O.Meany eine Speicherung der verschlüsselten medizinischen Daten getrennt von anderen Datenarten entsprechend den aktuellen Empfehlungen zu ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis (siehe DÄB 2014 (111); 21: A963-972).

8.3. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

8.4. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

8.5. Es gilt deutsches Recht.

Präambel

Diese Anlage konkretisiert die technischen und organisatorischen Maßnahmen, die O.Meany im Rahmen der Auftragsdatenverarbeitung zu oben genanntem Vertrag getroffen hat.

1. Zutrittskontrolle

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

1.1. Standort 1 (Rechenzentrum)

Technische Maßnahmen	Organisatorische Maßnahmen
Automatisches Zugangskontrollsystem	Personenkontrolle beim Pförtner / Empfang
Chipkarten-/Transponder-Schließsystem	Protokollierung der Besucher / Besucherbuch
Sicherheitsschlösser	Schlüsselregelung / Schlüsselbuch
	Sorgfältige Auswahl von Sicherheitspersonal
	Videoüberwachung der Zugänge

1.2. Standort 2 (Büro)

Technische Maßnahmen	Organisatorische Maßnahmen
Sicherheitsschlösser	Protokollierung der Besucher / Besucherbuch
Manuelles Schließsystem	Schlüsselregelung / Schlüsselbuch
	Videoüberwachung der Zugänge

2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können, wobei das Wort "nutzen" sich nicht auf die Legaldefinition des § 3 Abs. 5 BDSG beschränkt.

Technische Maßnahmen	Organisatorische Maßnahmen
Authentifikation mit Benutzer + Passwort	Benutzerberechtigungen verwalten
Einsatz von Anti-Viren-Software	Erstellen von Benutzerprofilen
Einsatz von Firewalls	Passwortregeln
Einsatz von VPN-Technologie	Protokollierung der Besucher / Besucherbuch
Gehäuseverriegelungen	Schlüsselregelung / Schlüsselbuch
Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)	Sorgfältige Auswahl von Reinigungspersonal
Verschlüsselung von Datenträgern	

3. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind und dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Aktenvernichtern	Anzahl der Administratoren auf das „Notwendigste" reduziert
Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (mit entsprechendem Zertifikat)
Physische Löschung von Datenträgern vor deren Wiederverwendung	Berechtigungskonzept
Protokollierung der Vernichtung von Daten	Passwortrichtlinie inkl. Länge und Wechsel
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	Sichere Aufbewahrung von Datenträgern
Verschlüsselung von Datenträgern	Verwaltung der Benutzerrechte durch Systemadministratoren

4. Weitergabekontrolle

Verhinderung, dass personenbezogene Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
Benutzen von VPN-Tunneln	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
Dateiübermittlung über https (TLS 1.2)	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
Sichere Transportbehälter/-verpackungen	

5. Eingabekontrolle

Sicherstellung, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Protokollierung der Eingabe, Änderung und Löschung von Daten	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle

Sicherstellung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
	Schriftliche Weisungen an den Auftragnehmer (durch Nutzen der vorgegebenen Vertragsanhänge) i.S.d. § 11 Abs. 2 BDSG
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)

7. Verfügbarkeitskontrolle

Sicherstellung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Feuerlöschgeräte in Serverräumen	Aufbewahrung der Datensicherung an einem sicheren, ausgelagerten Ort
Feuer- und Rauchmeldeanlagen	Backup- & Recoverykonzept
Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	Regelmäßiges Testen der Datenwiederherstellung
Klimaanlage in Serverräumen	Serverräume nicht unter sanitären Anlagen
Schutzsteckdosenleisten in Serverräumen	
Unterbrechungsfreie Stromversorgung (USV)	

8. Trennungsgebot

Sicherstellung, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	Berechtigungskonzept
Virtuell getrennte Speicherung auf gesonderten Systemen oder Datenträgern	Logische Mandantentrennung (softwareseitig)
Trennung von Produktiv- und Testsystem	