Bericht des Datenschutzbeauftragten (DSB)
der medatixx GmbH & Co. KG

Maßnahmen der medatixx zum Datenschutz
gemäß § 11 Abs. 5 Bundesdatenschutzgesetz (BDSG)

Zur Einhaltung des Datenschutzes nach § 11 Abs. 5 BDSG trifft die medatixx folgende technische und organisatorische Maßnahmen gemäß den 8 Punkten der Anlage zu § 9 BDSG.

1. Zutrittskontrolle
(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)

Aufgrund der Lage der Geschäftsräume sind Einwirkversuche von außen über die Fenster ausreichend verhindert. Die Geschäftsräume sind nur durch Personal mit entsprechenden Transpondern oder Schlüsseln zu betreten.

Zusätzlich werden außerhalb der Bürozeiten einbruch- und feuerhemmende Sicherheitstüren verschlossen.

Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern der medatixx im Büro begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten.

Wenn ein Mitarbeiter ausscheidet, gibt er seinen Büroschlüssel zurück und sein Zugangscode zur Schließanlage wird gesperrt.

Die medatixx verpflichtet auch Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren.

Der Zutritt zu den Serverräumen ist durch eine separate digitale Schließanlage abgesichert. Die Zutrittserlaubnis ist auf das unbedingt notwendige Personal (Systemadministratoren) beschränkt. Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind, erhalten keinen Zutritt zu den Serverräumen.

2. Zugangskontrolle
(Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)

Der Zugang zu den IT-Systemen ist durch eine Zugangsberechtigung geregelt. Eine Firewall verhindert ungewollte Zugriffe von außen.
Werden Passwörter mehrfach fehlerhaft eingegeben, erfolgt eine Sperrung. Diese kann nur durch einen Administrator rückgängig gemacht werden.

Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten wie möglich aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server der medatixx).

Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an die medatixx zurück.

3. Zugriffskontrolle

(Maßnahmen, die geeignet sind zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.)

Zugriffe auf die Server der medatixx erfolgen durch Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen. Bei Daten von Auftraggebern wird die Zugriffsberechtigung in der Vereinbarung zum Datenschutz geregelt.

Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter nur auf die Datenbanken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen.

Bei Zugriff auf Daten beim Auftraggeber ist durch die von der medatixx eingesetzten Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter der medatixx ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass alle Zugriffe in der Kundendokumentation protokolliert werden.

Wenn ein Mitarbeiter ausscheidet, werden ihm die Zugriffsrechte entzogen.

Die Datenfernübertragungssysteme der medatixx sind mit Datenverschlüsselung versehen und werden auf dem jeweils aktuellen technischen Stand gehalten.

Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Auftraggeberbereich zu lesen, zu kopieren, zu ändern oder zu entfernen.

Wenn die medatixx die Daten aus dem Auftraggeberbereich nicht mehr benötigt, werden die Datenträger nach DIN 32757-1 und gemäß den Bestimmungen des Datenschutzes vernichtet. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht.

4. Weitergabekontrolle

(Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.)

Die medatixx bearbeitet die Daten nur im Rahmen der Weisungen des Auftraggebers.

Die Speicherung von Daten aus dem Auftraggeberbereich erfolgt nur während der Arbeiten zur Mängelbeseitigung oder zur Unterstützung des Einsatzes der von der medatixx gelieferten Systeme bzw. von Systemen, für die die medatixx Serviceleistungen erbringt. Daten aus dem Bereich des Auftraggebers werden an einen Dritten nur weitergegeben, sofern der Auftraggeber das im Einzelfall schriftlich wünscht.

Der Auftraggeber kann der medatixx die Daten entweder verschlüsselt über eine gesicherte Fernwartungsverbindung auf einen Server der medatixx übertragen oder als Datenbank auf einem Datenträger zur Verfügung stellen.

5. Eingabekontrolle

(Maßnahmen, die geeignet sind zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.)

Es ist nicht vorgesehen, dass die medatixx personenbezogene Daten aus dem Bereich des Auftraggebers in die Software eingibt.

Werden personenbezogene Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche an die medatixx übertragen, werden diese Daten nach Beendigung der Fehlersuche gelöscht. Eine Veränderung oder Entfernung im Sinne des Datenschutzrechts findet nicht statt; es sei denn, dass der Auftraggeber dies vorher ausdrücklich schriftlich beauftragt hat.

6. Auftragskontrolle

(Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)

Die medatixx führt Arbeiten, bei denen sie Kontakt zu personenbezogenen Daten aus dem Bereich des Auftraggebers bekommen kann oder bekommen soll, nur durch, wenn dieser diese im Einzelfall anfordert. Dies ist beispielsweise dann der Fall, wenn der Auftraggeber an die medatixx einen Fehler oder ein Problem meldet. Die Mitarbeiter der medatixx sind angewiesen, solche Maßnahmen vorsorglich mit dem Auftraggeber abzustimmen.

Alle Mitarbeiter der medatixx, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind gemäß § 5 BDSG schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.

7. Verfügbarkeitskontrolle

(Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

Vorgaben des Brandschutzes werden eingehalten und regelmäßig durch externe Prüfungen verifiziert.

Alle betroffenen Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren. Von einem Auftraggeber übergebene Datenträger werden in einem Tresor verwahrt.
Die medatixx setzt eine Firewall und aktuelle Virenscanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers ein. Die Virensignaturen des verwendeten Virenscanners werden täglich mehrmals aktualisiert.

Arbeitsplatzrechner werden laufend durch aktuelle Scannerprogramme auf schadhafte Software überprüft. E-Mail-Anhänge werden auf Infizierung überwacht.

Die Mitarbeiter sind angehalten, personenbezogene Daten, die sie auf ihren Notebooks gespeichert haben, möglichst bald auf ein zentrales System der medatixx zu überspielen.

8. Trennungsgebot

(Maßnahmen, die geeignet sind zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)

Es ist nicht vorgesehen, dass die medatixx personenbezogene Daten aus dem Bereich des Auftraggebers verarbeitet. Wenn Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche oder deren Wiederherstellung übertragen werden, werden diese gesondert von Daten anderer Auftraggeber gespeichert.

Dokumente der medatixx dazu

Die internen Anweisungen der medatixx im Hinblick auf Datenschutz und Datensicherheit sind im Führungshandbuch der medatixx dargelegt.

Die Datenschutzbeauftragten von Auftraggebern sind berechtigt, diese Dokumente bei der medatixx einzusehen. Im Übrigen werden diese Dokumente aus Sicherheitsgründen geheim gehalten.

Erklärung des Datenschutzbeauftragten der medatixx

Hiermit erkläre ich, dass ich die vorgenannten Maßnahmen im Hinblick auf die Art der betroffenen personenbezogenen Daten für ausreichend halte und dass die medatixx diese Maßnahmen nach meinen Erkundungen und Wissen implementiert hat.

Kerstin Kutzenberger
Datenschutzbeauftragte der medatixx