Bericht des Datenschutzbeauftragten der Arztsysteme Rheinland GmbH (ASR)

Maßnahmen zum Datenschutz gemäß § 32 DSGGVO (Sicherheit der Verarbeitung)

Zur Einhaltung des Datenschutzes gemäß DSGVO und BDSGneu trifft die ASR folgende technische und organisatorische Maßnahmen:

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 autorisiertes Personal mit entsprechenden Schlüsseln zu betreten.
- Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern der ASR im Büro begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten.
- Wenn ein Mitarbeiter ausscheidet, gibt er seinen Büroschlüssel zurück.
- Die ASR 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 Servern ist durch eine separate 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 Servern.

2. Datenträgerkontrolle

(Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.)

- 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 möglichst zu schützen und nur möglichst wenige Daten aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server der ASR).
- Externer Zugriff von ASR-Mitarbeitern auf ASR-Server ist nur via VPN und Authentifizierung am ASR-LAN möglich.
- Anti-Viren-Software auf allen eingesetzten IT/DV-Anlagen.
- Personal- und Kundenakten unter Verschluss. Zugang nur für berechtigte Personen.
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an die ASR zurück.

3. Speicherkontrolle
(Die Speicherkontrolle umfasst Maßnahmen, mit denen die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.)

- Zugriffe auf die Server der ASR erfolgen durch Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen.
- Bei Daten von Auftraggebern wird die Zugriffsberechtigung in der Vereinbarung zum Datenschutz der medatixx oder ggf. mittels gesondertem AV-Vertrag_ASR gemäß Art. 28 DSGVO 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 ASR eingesetzte Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter der ASR 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.

4. Benutzerkontrolle
(Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.)

- Die Maßnahmen zur Umsetzung der Benutzerkontrolle sind in den Abschnitten Datenträgerkontrolle und Zugriffskontrolle umfassend beschrieben..

5. Zugriffskontrolle

(Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.)

- Vorhandensein eines Berechtigungskonzepts.
- Vorhandensein eins Datensicherungskonzeptes, Medienliste, Verschlüsselung.
- Zugriff zu den Festplatten mit Datensicherung nur für berechtigte Personen.
- Vorhandensein einer Verfahrensanweisung „Umgang IT“
- Zugriff auf Notebooks, PC und Server von medatixx nur mit Username und Passwort möglich.
- Passwörter unterliegen definierten Passwortrichtlinien (hohen Anforderungen).
- Administratoren sind für Vergabe und regelmäßige Änderung von Passwörtern verantwortlich. (automatisiertes Verfahren)
- Betrieb von Arbeitsplatz-PC und Servern nur nach Anmeldung mit Benutzername und Passwort.
- Sperrung nach mehrmaligen fehlerhaften Anmeldeversuchen.
- Zwischenlagerung defekter Datenträger bis zur datenschutzkonformen Vernichtung.

- Vernichtung ausgedruckter Daten im Aktenvernichter bzw. durch zugelassene Fachunternehmen.
- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDAs, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung schriftlich geregelt.

6. Übertragungskontrolle

(Die Übertragungskontrolle umfasst Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.)

- Regelungen zur Datenübertragung sind vorhanden.
- Übermittlung und Zur-Verfügung-Stellen von Daten wird protokolliert.
- ASR 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 ASR gelieferten Systeme bzw. von Systemen, für die ASR Serviceleistungen erbringt. Daten aus dem Bereich des Auftraggebers werden an einen Dritten (jeder durch den Auftraggeber nicht genehmigte Unterauftragsverarbeiter) nur weitergegeben, sofern der Auftraggeber das im Einzelfall schriftlich wünscht.
- Der Auftraggeber kann der ASR die Daten entweder verschlüsselt über eine gesicherte Fernwartungsverbindung auf einen Server von ASR übertragen oder als Datenbank auf einem Datenträger zur Verfügung stellen.

7. Eingabekontrolle

(Die Eingabekontrolle umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt worden sind.)

- Regelungen zur Dateneingabe sind vorhanden.
- Erstellung und Änderung von Daten wird protokolliert.
- Es ist nicht vorgesehen, dass ASR personenbezogene Daten aus dem Bereich des Auftraggebers in die Software eingibt.
- Werden personenbezogene Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche an ASR 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.
- Es ist nicht vorgesehen für Mitarbeiter der ASR, Daten in den operativen Systemen vom Auftraggebern einzugeben, zu ändern oder zu entfernen.

8. Transportkontrolle
(Die Transportkontrolle umfasst Maßnahmen, die 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.)

- Einsatz von Firewall mit aktueller Firmware
- Einsatz von VPN Technologie zur Verschlüsselung bei Übertragung

9. Wiederherstellbarkeit
(Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.)

- Die Maßnahmen zur Wiederherstellbarkeit sind im IT-Notfallkonzept sowie im Datensicherungskonzept umfassend beschrieben.

10. Zuverlässigkeit
(Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.)

- siehe Verfügbarkeitskontrolle.

11. Datenintegrität
(Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.)
- siehe Verfügbarkeitskontrolle.

12. Auftragskontrolle
(Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.)

- Alle ASR-Mitarbeiter sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Die Weitergabe personenbezogener Daten erfolgt nach schriftlicher Einwilligung vom Auftraggeber oder im Rahmen gesetzlicher Bestimmungen.
- Dienstleister der ASR unterliegen Überprüfungen (Lieferantenaudits).
- Die ASR 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 ASR oder die medatixx einen Fehler oder ein Problem meldet. Die Mitarbeiter von ASR sind angewiesen, solche Maßnahmen vorsorglich mit dem Auftraggeber abzustimmen.
- Alle Mitarbeiter der ASR, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind 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.

13. Verfügbarkeitskontrolle

(Die Verfügbarkeitskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- Tägliche Datensicherung inkl. Protokollfunktion
- Feuerlöscher im Gebäude.
- Vorgaben des Brandschutzes werden eingehalten
- Rauchverbot im Serverraum und in Büroräumen
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz.
- Datenschicherungskonzept für Server
- Alle Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.
- Von einem Auftraggeber übergebene Datenträger werden unter Verschluss verwahrt.
- Virenschutzprogramme auf allen Computersystemen.
- Firewall und aktuelle Virenscanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers. Die Virensignaturen des verwendeten Virenscanners werden täglich mehrmals aktualisiert.
- Arbeitsplatzrechner werden laufend 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 von medatixx zu überspielen.
- Notfallplan.

14. Trennbarkeit

(Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)

- Es ist nicht vorgesehen, dass 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.

DMS der ASR

Die internen Anweisungen der ASR im Hinblick auf Datenschutz und Datensicherheit sind im QM-System der ASR dargelegt. Eine Versionierung findet statt. Die Datenschutzbeauftragten von Auftraggebern sind berechtigt, relevante Dokumente bei der ASR einzusehen. Dazu wenden Sie sich bitte an unseren Datenschutzbeauftragten. Im Übrigen werden diese Dokumente aus Sicherheitsgründen geheim gehalten.

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

Stadthagen, 19.05.2018

Stefan Breitkopf, Datenschutzbeauftragter der ASR GmbH