Schäf Systemtechnik

[redacted] **SST**

Zusammenfassung

Edition 2

Stand 18. Mai. 18

für:

Datenschutzvereinbarung

	Name	Datum	Unterschrift
Autor	Schäf	18. Mai. 18	
Review			

1 Inhalt

Seite

2 Historie

Edition	Datum	Autor	Änderung, Grund für Änderung
1	20. Apr. 18	Schaef	Erstversion
2	18. Mai. 18	Schaef	Personalisiert fertig zur Unterschrift

3 Anwendung

3.1 Anwendungsbereich für dieses Dokument

Dieses Dokument stellt eine Datenschutzvereinbarung zwischen

Praxis, Name, Adresse

Und der Schäf Systemtechnik Service U.G. dar.

Die Vereinbarung wird als Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG), insbesonderen des § 11 BDSG („Auftragsdatenverarbeitung“) geschlossen. Den Parteien ist bekannt, dass ab dem 25.05.2018 die Datenschutz-Grundverordnung (DSGVO – EU Verordnung 2016/679) gilt und sich die Vorgben der Auftragsdatenverarbeitung dann grundsätzlich nach Art. 28 DSGVO richten.

3.2 Anwendung

Im Rahmen der Wartung von Anlagen werden dem Wartungspersonal in diversen Weisen vertrauliche Patienteninformation angezeigt, dargestellt und teilweise übertragen.

Die hier dargestellten Vereinbarungen werden getroffen, um die Vertraulichkeit von Patientendaten sicher zu stellen.

4 Allgemeines

4.1 Ausgangssituation

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und / oder Pflegearbeiten an IT Systemen des Auftraggebers durch. In diesem Zusammenhang ist nicht ausgeschlossen, daß der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet umd die Wartung und Pflege von IT Systemen durchzuführen oder durchführen zu können.

4.2 Dauer und Beendigung des Wartungsvertrages

Zwischen dem Auftraggeber und dem Auftragnehmer besteht ein Wartungsvertrag im Hinblick auf die Wartung und Pflege des EDV Systemes des Auftraggebers.

Der Vertrag ist zeitlich nicht begrenzt und kann von jeder der beteilgten Parteien mit 3 Monaten zum Quartalsende gekündigt werden.

Die in dieser Vereinbarung getroffenen Maßnahmen bleiben auch nach Kündigung des Wartungsvertrages wirksam.

Das Personal des Auftragnehmers wird vergattert und zur Verschwiegenheit verpflichtet so daß eine Verschwiegenheitspflicht auch über das Beschäftigungsverhältnis hinaus besteht und die Daten des Auftraggebers bzw. dessen Patienten vertraulich behandelt werden.

5 Maßnahmen zur Datensicherheit

5.1 Verpflichtungserklärung

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen die zur Einhaltung der anzuwendnden Datenschutzvorschriften erforderlich sind.

5.2 Personal

Hinsichtlich Personal werden folgende Maßnahmen ergriffen:

5.2.1 Vergatterung

Das Personal der SST wird regelmäßig belehrt und zum Einhalten der Datenschutzregeln in der SST insbesondere dem vertraulichen Umgang und Geheimhaltung gegenüber Dritten vergattert.

Das Personal unterschreibt regelmäßig entsprechende Erklärungen.

5.2.2 Anstellungsvertrag

Im Anstellungsvertrag eines jeden Mitarbeiters wird die Einhaltung der Datenschutzregeln explizit erwähnt und gefordert. Die Mitarbeiter verpflichten sich auch nach Verlassen des Unternehmens ihrer Geheimhaltungspflicht nachzukommen.

5.3 Fernwartung

Für den Fall, daß der Auftragnehmer die Wartung und Pflege von IT- Systemen für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt, sind vom Auftragnehmer zwingend die von ihm getroffenen teschnischen und organisatorischen Maßnahmen im Sinne des §9 BDSG und der Anlage zu §9 satz 1 BDSG festzuhalten

Ab dem 25.05.2018 hat der Auftragnehmer eine Beschreibung der von im getroffenen teschnischen und organisatorischen Maßnahmen nach art. 32 DSGVO zur Verfügung zu stellen.

In §9 seht Zitat:

< Zitat>
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. 2Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
</ Zitat>

In Anlage 1 steht:
< Zitat>

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. 2Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

</ Zitat>

5.3.1 Automatisierte Verarbeitung

Seitens der SST Service wird eine automatisierte Verarbeitung von Daten nicht angeboten und auch nicht durchgeführt. Die dargestellten Anforderungen beziehen sich also im Wesentlichen Auf den Auftraggeber.

In diesem Zusammenhang wird die SST Service U.G. Als Auftragnehmer als eine der am Rande beteiligten Parteien gesehen und muß sich entsprechend verhalten.

5.3.2 Zutrittskontrolle

Der physikalische Zugang zu Anlagen wird kundenseitig organisiert und entsprechend abgesichtert. Die Mitarbeiter der SST haben keine Schlüssel zu Räumen in denen sich Kundenanlagen befinden.

5.3.3 Zugangskontrolle

Sämtliche Zugangsmechanismen zu Kundenanlagen per Fernwartung sind passwortgeschützt und nicht allgemein zugänglich.

5.3.4 Einschränkung des Zugriffes

Im Umfeld der Aktivitäten der SST Service U.G. ergeben sich zwei Aktivitätsbereiche:

5.3.4.1 Arbeiten an Bildverarbeitungsgeräten

Arbeiten an Bildverarbeitungsgeräten beschränken sich auf Geräte wie DICOM Archive, DR-Anlagen und Befundungsworkstations.

Die Mitarbeiter haben hier vollen Zugriff auf alle Daten. Die Inhalte der Daten sind hinsichtlich Datenschutzrechtlicher Relevanz als wenig sensibel einzustufen (Bilder mit Namen, Geburtsdatum, Gechlecht und Untersuchungsdatum).

Die Arbeiten können vom Auftraggeber unbeaufsichtigt erfolgen, das Personal ist entsprechend eingewiesen, geschult und vergattert.

5.3.4.2 Arbeiten an allgemeinen EDV Geräten des Auftraggebers

In einigen Fällen ist es erforderlich auf allgemeine EDV Systeme des Auftraggebers zuzugreifen um dort z.B. Bildverteilungssysteme zu konfigurieren oder zu warten.

Diese Arbeiten werden nur unter Aufsicht des Auftraggebers (bzw. dessen Personales) sowie nach expliziter Freigabe durch den Auftraggeber (Übermitteln der Zugangsdaten) durchgeführt.

Der Auftraggeber trägt hier die Verantwortung dafür, daß dem Wartungspersonal keine Daten dargestellt werden, die es nicht sehen soll. Der Auftraggeber sorgt dafür, daß Daten hier nicht

unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Auftraggeber dokumentiert ggf. wer Daten eingegeben, verändert gespeichert oder gelöscht hat.

Veränderungen an Daten die nicht unmittelbar mit der Bildverarbeitung zu tun haben werden hier seitens SST Service U.G. nicht vorkommen.

Den Weisungen des Auftraggebers wird hier in jedem Falle Folge geleistet.

In § 9 wird gefordert, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Der Schutz dieser Daten liegt im Verantwortungsbereich des Auftraggebers und kann vom Auftragnehmer nicht beeinflusst werden.

5.3.5 Getrennte Verarbeitung

Im Bundesdatenschutzgesetz § 9 wird ausdrücklich gefordert, daß zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Das bedeutet, daß die Bildverarbeitung (PACS) in einer medizinischen Einrichtung grundsätzliche auf eigenständigen Systemen (Software und Hardware) realisiert und nur mittels EDV Schnittstelle miteinander verbunden werden.

Die Funktionalität der entsprechenden Schnittstellen beschränkt sich auf die im medizinischen Arbeitsablauf sinnvollen Vorgänge.

6 Generelle Regeln in der SST

Die in 5. Dargestellen Forderungen werden durch weitere flankierende Regeln in der SST Gruppe unterstützt:

6.1 So wenig wie möglich

Es werden so wenig wie möglich datenschutzrelevante Daten dargestellt angezeigt, gespeichert bzw. übertragen.

In den Bildern, die von SST Software und Hardware bearbeitet bzw. gespeichert werden sind nur minimal kritische Informationen enthalten (Name Geb. Datum, Geschlecht). Weitergehende daten werden hier nicht gespeichert.

6.2 Speichern

Datenschutzrelevante Daten werden von der SST nur im absolut erforderlichen Umfang gespeichert und sofort nach Beendigung der jeweiligen Aktion gelöscht.

6.3 Personaldaten

Alle Personaldaten werden in Papier geführt und sind verschlossen aufbewahrt.

6.4 Hardware

Hardwarekomponenten, insbesondere Speichermedien werden nicht weggeworfen sondern gesammelt und dann zuverlässig vernichtet. Dadurch wird verhindert, dass aus weggeworfenen Medien wieder Daten rekonstruiert werden könnten.

6.5 Zugangsschutz

Die Räume, in welchen Zugriff auf entsprechende EDV Systeme bestünden, sind verschlossen.

6.6 Der Zugang wird protokolliert

Der Zugang in die Firma wird dokumentiert.

6.7 Allgemeine Sicherheitsmaßnahmen

Allegemeine Sicherheitsmaßnahmen wie Passwortschutz, regelmäßige Updates, etc. werden durchgeführt und gepflegt

6.8 WEB Site

Die Datenschutzerklärung ist von jeder Seite der WEB Page aus aufrufbar.

Die Datenschutzerklärung ist eine eigene Seite.

6.9 CIP

Im Rahmen unseres kontinuierlichen Verbesserungsprozesses werden die entsprechenden Regeln regelmäßig überprüft (internes Audit) und ggf. verbessert.

7 Empfohlene Maßnahmen beim Kunden

Es werden folgende Maßnahmen empfohlen:

7.1 Zugangsschutz

PACS Workstations und Server sollten nur in abgeschlossenen Räumen bzw. nur in Räumen aufbewahrt werden, in welchen unbeaufsichtigter Zugriff durch Dritte ausgeschlossen ist.

Server sollte hierbei in einem abgeschlossenen Raum aufbewahrt werden.

7.2 Passwortschutz

Alle betroffenen Workstations sollten mit Passwortschutz ausgerüstet sein.

7.3 Backup Daten

Backup Daten (DVDs) sollten in verschlossenen Räumen aufbewahrt werden.
Backups sind nach BDSG §9 Anlage zwingend vorgeschrieben.

7.4 Datenträger

Datenträger die Patientendaten enthalten sollten entweder sofort ausgehändigt oder sofort zerstört werden (wenn verschrieben, falscher Patient, etc.)

Bitte nicht alte beschriebene CDs offen rumliegen lassen.

Mitgebrachte Datenträger sollten entweder nach Betrachtung dem Patienten wieder ausgehändigt werden oder elektronisch importiert werden, nicht jedoch offen zugänglich sein.

Gleiches gilt für Papierdokumente die gescannt werden können oder sollen.

7.5 Personal

Das Praxispersonal sollte in jedem Falle hinsichtlich Datenschutz belehrt und vergattert werden.

Gleiches gilt für Reinigungspersonal und Wartungspersonal das regelmäßig in der Praxis arbeitet.

Eine Schlüsselliste ist zu führen und alles Personal mit einem Schlüssel zu belehren und zu vergattern.

7.6 Patienten

Es sollte darauf geachtet werden, dass Patienten keinen Einblick in Akten anderer Patienten erhalten.

Es sollte sichergestellt sein, dass Patienten nicht z.B. beim Warten auf den Arzt unkontrolliert Zugriff auf geöffnete Patientenakten (auch elektronisch) haben.

Der unbeaufsichtigte Patient im Arztzimmer muß hier als Risikofaktor angesehen werden.

7.7 Patientenerklärung

Es ist zwar nicht vorgeschrieben aber grundsätzlich eine gute Idee, jeden Patienten eine Einverständniserklärung unterschreiben zu lassen, dass seine Daten elektronisch gespeichert und im Rahmen der üblichen Arbeitsabläufe in einer Praxis ausgewertet werden.

§9 BDSG sagt hierzu nichts aus.

7.8 Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist zu benennen.

7.9 Allgemeine Regeln

Die allgemeinen Regeln der neuen Datenschutzverordnung sind einzuhalten.

8 Unterschriften

Datum: _____

_____ _____

H.-M. Schaef (Geschäftsführer) Micha Schuh (Datenschutzbeauftragter)

Auftraggeber (Praxis)