22. 05. 2018

D O K U M E N T A T I O N S P F L I C H T E N

D A T E N S C H U T Z - G R U N D V E R O R D N U N G

DSGVO

von

Dr. Helga HAHN

Soweit personenbezogene Bezeichnungen in diesem Schriftstück nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

Inhaltsverzeichnis:

1. Allgemeine Informationen

Name und Anschrift des Verantwortlichen:

Dr. Helga Hahn
Joanelligasse 12/28
1060 Wien
Austria

Datenschutzbeauftragter: nicht nötig

2. Verzeichnis von Verarbeitungstätigkeiten

Datenanwendungen, die der Verantwortliche betreibt:

- Verwaltung der Ordination/des Büros
- Patientenverwaltung

Sofern nichts Anderes angegeben ist, verweist das Verzeichnis von Verarbeitungstätigkeiten auf folgende Kategorien von Übermittlungsempfängern:

1 Banken
2 Rechtsvertreter
3 Wirtschaftstreuhänder, Wirtschaftsprüfer
4 Gerichte
5 Zuständige Verwaltungsbehörden
6 Inkassounternehmen
7 Fremdfinanzierer
8 Vertrags- und Geschäftspartner
9 (private) Versicherungen
10 Statistik Österreich
11 Inspektorate

12 betriebliche und außerbetriebliche Interessenvertretungen
13 Vorsorgekassen, Abfertigungskassen, Sozialversicherungen, Pensionskassen
14 Transportunternehmen
15 Lieferanten
16 Ärzte, Krankenhäuser, Ambulatorien, Labore, Physiotherapeuten, Pflegeheime
17 Apotheken, Gesundheitsdiensteanbieter, nicht-ärztliche Gesundheitsberufe

Verwaltung der Ordination/des Büros

Datenanwendung: Kommunikation mit der Kammer

Zweck der Verarbeitung: Abwicklung von organisatorischen Fragen mit der jeweiligen Ärztekammer zum Betrieb der Ordination einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegen- heit.

Beinhaltet auch: Beiträge und Umlagen, die Beantragung von Fortbildungsnachweisen.

Rechtsgrundlage der Verarbeitung: gesetzliche Grundlage

Beschreibung der **Kategorien betroffener Personen**: Mitglieder und Arbeitnehmer der Ärztekammer

Allgemeine Beschreibung organisatorischer Maßnahmen: Speicherdauer 30 Jahre

Datenanwendung: Finanzbuchhaltung, Rechnungswesen und Logistik

Zweck der Verarbeitung:
Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung (bzw. zur Abwicklung dieser) mit Patienten und Lieferanten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Risikomanagement, Kreditoren- und Debitorenverwaltung, Budgetierung und Kostenrechnung.

Rechtsgrundlage der Verarbeitung: Gesetzliche Verpflichtung

Beschreibung der **Kategorien betroffener Personen**: Patienten, vom Verantwortlichen betreute Unternehmen, Lieferanten, Steuerberater

Verarbeitung durch Auftragsverarbeiter: Steuerberatungskanzlei hhp

Allgemeine Beschreibung organisatorischer Maßnahmen: gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre

Datenanwendung: Personalverwaltung - Keine

Datenanwendung: Aktenverwaltung / Büroautomation

Zweck der Verarbeitung: Formale Behandlung der vom Verantwortlichen zu besorgenden Geschäftsfälle (einschließlich der Aufbewahrung der bei dieser Tätigkeit anfallenden Dokumente).

Beinhaltet auch: Inventarverwaltung und Verwaltung von Anlagevermögen

Rechtsgrundlage der Verarbeitung: Erfüllung eines Vertragsverhältnisses

Beschreibung der **Kategorien betroffener Personen**: Dr. Helga Hahn, Lieferanten

Patientenverwaltung

Datenanwendung: Patientenakte

Zweck der Verarbeitung: Erfüllung der Dokumentationspflicht gemäß § 51 Ärztegesetz sowie die Erfassung sämtlicher Leistun- gen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angele- genheiten.

Beinhaltet auch: Ausstellung von Bescheinigungen, Terminmanagement (Terminvereinbarung mit Patienten), die Wahrnehmung der Anzeige- und Meldepflicht gemäß § 54 Ärztegesetz, die Wahrnehmung der Anzeige- und Meldepflicht im Missbrauchsfall sowie Meldungen an div. Gesundheitsregister und im öffentlichen Meldewesen (Meldepflichten bei ansteckenden Krankheiten); die Mitwirkung bei Verfahren bei der Patientenanwaltschaft, der Schlichtungsstelle sowie dem Beschwerdemanagement bei der Standesvertretung und Versicherungen; die Erstellung medizinischer Gutachten. Verwaltung von Transportscheinen, Zuweisungen und Überweisungen.

Rechtsgrundlage der Verarbeitung: gesetzliche Grundlage

Beschreibung der **Kategorien betroffener Personen**: Patienten, Arbeitnehmer arbeitsmedizinisch zu betreuender Firmen

Verarbeitung durch **Auftragsverarbeiter:** keine

Speicherdauer personenbezogener Daten und Behandlungsinformationen: 30 Jahre

Datenanwendung: Abrechnung (sowohl Krankenkasse / Privat)

Zweck der Verarbeitung: Abrechnung der erbrachten Leistungen gegenüber Versicherungen (Firmen, Versicherungen, Gerichten, Patienten) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Die Übermittlung an die Standesvertretung zur Prüfung und Evaluierung der Abrechnung.

Rechtsgrundlage der Verarbeitung: gesetzliche Grundlage, Erfüllung eines Vertragsverhältnisses

Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer verschiedener Firmen, Gerichtsparteien, Patienten

Verarbeitung durch **Auftragsverarbeiter:** keine

Allgemeine Beschreibung organisatorischer Maßnahmen: gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre

Datenanwendung: Befundanforderung / Befundübermittlung

Zweck der Verarbeitung: Anforderung von Befunden von Ärztinnen und Ärzten, Krankenanstalten, Labore, sowie anderen Gesundheitsberufen und den Betroffenen sowie die (Rück-)Übermittlung von Befunden einschließlich automationsunterstützt er- stellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Rückfragen

Rechtsgrundlage der Verarbeitung: gesetzliche Grundlage

Beschreibung der **Kategorien betroffener Personen**: Ärzte, Patienten, Firmen, Gerichte, Versicherungen

Verarbeitung durch **Auftragsverarbeiter:** keine

Allgemeine Beschreibung organisatorische Maßnahmen: gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)

Datenanwendung: Verwaltung von Rezepten

Zweck der Verarbeitung: Ausgabe, Verwaltung und Organisation von Rezepten

Rechtsgrundlage der Verarbeitung: gesetzliche Grundlage

Beschreibung der **Kategorien betroffener Personen**: Patienten

Verarbeitung durch Auftragsverarbeiter: keine

Allgemeine Beschreibung organisatorische Maßnahmen: gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)

3. Technische und organisatorische Maßnahmen

Technische Maßnahmen

Bildschirmsperre:

Der Verantwortliche stellt sicher, daß beim Verlassen des Arbeitsplatzes der Computer so gesperrt wird, daß er durch Dritte nicht genutzt werden kann (Stichwort: Bildschirmsperre). Dieser kann erst wieder nach Eingabe eines Kennworts verwendet werden.

Umgang mit Speichermedien:

Der Verantwortliche stellt sicher, daß der Computer so gesperrt wird, daß Speichermedien nur nach Eingabe eines Passworts verwendet werden können.

Sichere Nutzung des Internets:

Technische Maßnahmen zum Sichern des Computers:

Der Verantwortliche stellt sicher, daß der PC so gesichert ist, daß Rechnermikrofon und Kamera gegen unberechtigten Zugriff gesperrt sind, regelmäßige Sicherheitsupdates durchgeführt werden und regelmäßig auf Viren untersucht wird. Die Grundkonfiguration des Rechners sieht vor, daß der Rechner vor unberechtigtem Zugang geschützt ist (die Nutzung des Rechners ist nur nach Eingabe eines Passworts möglich).

Datensicherung:

Der Verantwortliche stellt sicher, dass sämtliche auf dem lokalen Rechner gespeicherten Daten regelmäßig gesichert werden.

Der Rechner wird wie folgt gesichert: externe Festplatte

Virenschutz: Firewall

Sicherung von öffentlich zugänglichen Bereichen:

Sofern der Verantwortliche öffentlich zugängliche Netzwerke („WLAN“) betreibt, wird er diese so sichern, dass ein Zugriff auf nicht öffentlich zugängliche Systeme des Verantwortlichen nicht möglich ist.

Unterbrechungsfreie Stromversorgung:

Der Computer und andere Komponenten sind mit einer unterbrechungsfreien Stromversorgung gesichert.

Software Sicherheitsmaßnahmen:

Der Verantwortliche stellt sicher, dass sämtliche Endgeräte regelmäßig mit Updates versorgt werden und Softwarepakete, welche Sicherheitslücken schließen, regelmäßig in die entsprechenden Systeme eingespielt werden.

Der Verantwortliche stellt sicher, dass der Zugriff auf Systeme nur nach Eingabe eines Passworts möglich ist.

Der Verantwortliche stellt sicher, daß regelmäßig Backups der Datenbestände erstellt werden:

Der Verantwortliche stellt sicher, dass sämtliche Systeme durch eine Firewall geschützt werden, um einen unberechtigten externen Zugriff zu verhindern. Der Verantwortliche stellt sicher, dass ein aktueller Viren- und Spamfilter installiert ist und gewartet wird.

Sicherung von Telekommunikationseinrichtungen:

Der Verantwortliche stellt sicher, dass sämtliche Telekommunikationseinrichtungen (etwa Telefonanlage, Fax, VPN, W-LAN, E-Mailserver, Firewalls) vor unberechtigtem Zugriff geschützt sind.

Bauseitig organisatorische Maßnahmen:

Regelungen über den Zutritt zu Räumlichkeiten: Ausschließlich der Verantwortliche

Maßnahmen zum Schutz der Infrastruktur: Der Verantwortliche stellt sicher, dass die Infrastruktur vor unberechtigtem Zutritt geschützt ist. Ferner hat der Verantwortliche Maßnahmen ergriffen, die Infrastruktur vor Zerstörung (etwa durch Feuer) zu schützen.

Archiv: Der Verantwortliche hat Maßnahmen dahingehend ergriffen, dass der Zutritt zum Archiv nur berechtigten Personen möglich ist.

Nutzung von Kommunikationsmitteln:

Der Verantwortliche klassifiziert Dokumente wie folgt:

1. Vertraulich
2. Nicht vertraulich
3. Öffentlich bekannt

Der Verantwortliche nutzt folgende Kommunikationsmedien:

1. Persönliche Übergabe
2. Versand per verschlüsselter elektronischer Kommunikation
3. Versand per eingeschriebenem Brief
4. Versand per Post
5. Versand per Fax
6. Versand per E-Mail
7. Telefonische Mitteilung
8. Versand per SMS

Zur Einhaltung eines angemessenen Sicherheitsniveaus verpflichtet sich der Verantwortliche, Informationen ausschließlich wie folgt zu übermitteln bzw. zu übersenden:

Klassifizierung	Kommunikationsmedium
Vertraulich	Persönliche Übergabe Versand per verschlüsselter elektronischer Kommunikation Versand per Post
Nicht vertraulich	Jedes Medium
Öffentlich bekannt	Jedes Medium

Der Verantwortliche klassifiziert Informationen wie folgt:

Information	Klassifizierung
Informationen, die die Sozialversicherungsnummer enthalten	Vertraulich
Gesundheitsdaten	Vertraulich
Adreßinformationen	Vertraulich
Kontaktinformationen	Vertraulich
Informationen über Patienten	Vertraulich
Befunde	Vertraulich

Weitergabe von Zugangsdaten und Passwörtern: keine

Zulässige Kommunikationsmedien:

Der Arzt als datenschutzrechtlicher Verantwortlicher wird vertrauliche Informationen (etwa Gesundheitsdaten und Befunde) an Patienten/Arbeitnehmer mittels unverschlüsselter E-Mail nur senden, wenn der jeweilige Patient vorab in die unverschlüsselte Zusendung eingewilligt hat. Sollte keine schriftliche Einwilligung des Patienten vorliegen, hat der Arzt als datenschutzrechtlicher Verantwortliche die mündliche Einwilligung des Patienten/Arbeitnehmers in der Patientenakte zu dokumentieren.

Der Verantwortliche verpflichtet sich, vertrauliche Informationen (etwa Gesundheitsdaten) an zulässige Übermittlungsempfänger (etwa: Apotheken, Ärzte, Krankenhäuser, Pflegeheime, Krankenversicherungen) ausschließlich mittels verschlüsselter elektronischer Kommunikation, Versand per Post oder mittels Fax zu senden.

Regeln zum Verlassen der Räumlichkeiten:

Der Verantwortliche stellt sicher, daß sämtliche Fenster und Türen bei Verlassen der Räumlichkeiten geschlossen bzw. abgeschlossen werden, sowie die Alarmanlage aktiviert ist, sodaß unbefugte Dritte keinen Zugang zu den Räumlichkeiten des Verantwortlichen bzw. zu personenbezogenen Daten hat.

Sicherung von physischen Dokumenten:

Der Verantwortliche stellt sicher, daß Dokumente der Kategorie „vertraulich“ in einem verschlossenen Aktenordner oder Aktenschrank verwahrt und unmittelbar nach dem Gebrauch wieder eingeschlossen werden.