Datenschutz-Auditbericht

erstellt am:	19.11.2024	Auditor:	Nenad Rogic

Einrichtung	Physiolounge GmbH		
Name Inhaber/in	Iris Düppen		
Name Verantwortlicher falls abweichend			
Straße	Zentralstraße 1		
PLZ; Stadt	04109 Leipzig		
Telefon	0341-9277200	Fax	
E-Mail	iris.dueppen@physiolounge-leipzig.de		
Homepage	www.physiolounge-leipzig.de		
Rechtsform/ Besonderheiten:	GmbH		
Tätigkeiten und Abweichungen zum „normalen“ Berufsbild (z.B. Therapie, Training, Verein etc.)			

Anzahl der Beschäftigten	Inhaber:		1	
	Angestellte in Therapie und Verwaltung:		19	
	Freiberufliche MA			
	Gesamtzahl aller tätigen Personen (*Anzahl der Personen mit Zugang zu Daten)		20	

DSB	Besteht eine Pflicht zur Benennung eines Datenschutzbeauftragten nach Artikel 37 DS-GVO und BDSG neu §38?	[x] ja	[ ] nein
	*Nach Artikel 37 DSGVO muss im Heilwesen Bereich ein DSB bestellt werden, wenn mindestens **10 Personen** ständig mit der Verarbeitung personenbezogener Daten zu tun oder Zugang haben.		
	Wurde ein DSB amtlich bestellt/gemeldet?	[ ] ja	[x] nein
DSB	Vollständige Kontaktdaten des offiziellen DSB:		
	*nur eintragen wenn DSB bereits offiziell bestellt bzw. bei der Behörde gemeldet ist oder ein Auftrag an die Consularis schriftl. erteilt wurde. Vollständige Adressdaten !		

Kostenloser Homepagecheck als inkl. Leistung zum DSB Auftrag?	[ ] ja	[x] nein
Separater Homepagecheck als Single Leistung gewünscht?	[x] ja	[ ] nein
BAFA Förderung beantragt?	[x] ja	[ ] nein
Wurde ein Sicherheitsbeauftragter (Arbeitsschutz) benannt?	[ ] ja	[x] nein

Sonstige, für die Auswertung wichtige Informationen zum geprüften Betrieb oder Besonderheiten o.ä.:

1. Organisatorisches			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
1	**VVT** Verzeichnis der Verarbeitungs-tätigkeiten	Gibt es ein Verzeichnis der Verarbeitungstätigkeiten (VVT)?		X		X
2		Ist das vorhandene VVT DSGVO konform (inkl. Übersichtsliste) ?		X		X
3	**TOM** Technische und Organisatorische Maßnahmen	Besteht eine Dokumentation der technischen und organisatorischen Maßnahmen (TOM)?		X		X
4		Ist die vorhandene Dokumentation der TOM DSGVO konform?		X		X
5	**AVV** Auftrags-verarbeitungsvertäge	Bestehen Auftragsverarbeitungs-Verträge (AVV) mit allen im Bereich der Datenverarbeitung involvierten Parteien ? *jede externe Partei, die in irgendeiner Form Daten im Auftrag der Praxis erhebt, speichert oder sonstig verarbeitet		X		X
6	**wichtige Informationen für Patienten**	Wird eine schriftliche Patienteninformation eingesetzt und wird diese abgezeichnet? (Einwilligung und Nachweis)	X			
7		Wird bei der Behandlung von Kindern die Einwilligung von den Erziehungsberechtigten eingeholt?		X		X
8		Ist die vorhandene Patienteninformation DSGVO konform?		X		X
9		Wird der Patient über sein Widerrufsrecht ausführlich aufgeklärt? *wichtig sonst Einwilligung ungültig		X		X

Folgende Patientendaten werden verarbeitet			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
Diese Angaben sind wichtig, da die Antworten in die Dokumentation des VVT und der TOM einfließen. Ja = diese Daten werden von dem Betrieb verarbeitet Nein = diese Daten werden nicht in die Dokumentation übernommen						
10	**Adressdaten**	Name, Nachname, Straße, Hausnummer, Land, Ort, PLZ	X			
11	**Kontaktdaten**	Telefon, Mobilnummer	X			
12		E-Mail Adresse	X			
13	**Versicherungs-daten**	Krankenkasse	X			
14	**Adressdaten nächste Angehörige bzw. Betreuer**	Name, Nachname, Straße, Hausnummer, Land, Ort, PLZ	X			

Folgende Patientendaten werden verarbeitet				Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
15	Kontaktdaten nächste Angehörige bzw. Betreuer	Telefon, Mobilnummer		X			
16		E-Mail Adresse		X			
17	Unterlagen zum Status	Vollmachten, Bestellungsurkunde in Kopie		X			
18	Biometrische Daten	Geburtsdaten		X			
19		Fingerabdruck			X		
20		Größe, Gewicht			X		
21		Umfänge (Lymphe), Körpermaße, Schuhgröße		X			
22	Finanz-daten	Rechnungen		X			
23		Zuzahlungen in bar		X			
24		Bankverbindung		X			
25		Abrechnungsdaten		X			
26		EC-Cash für Zuzahlungen oder Selbstzahler		X			
27	Gesundheits-daten	Krankheitsdaten		X			
28		Befunde		X			
29		Medikamentendaten		X			
30	Inhaltliche Daten	Termindaten		X			
31		Kommentare		X			
32		Texteingaben oder schriftliche Notizen auf Papier		X			
33		Fotodateien		X			
34		Videodateien			X		
35		Ton- /Sprachaufnahmen			X		
36		Die Einwilligung zur Verwendung von Ton oder Bildaufnahmen zu medizinischen/ therapeutischen Zwecken wurde eingeholt?			X		X
37	sonstige Daten				X		
38	Speicherort Patienten-daten	Die Speicherung/Verarbeit -ung der o.g. Daten erfolgt z.B. in einer:	analogen Patientenakte (z.B. Karteikarte o.ä.)	X			
39			digitalen Patientenakte	X			

Folgende Mitarbeiterdaten werden verarbeitet:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
!	**Keine Angestellten**	Es werden **keine** Mitarbeiterdaten verarbeitet, da es sich um eine Einzelpraxis handelt. Die Bezeichnung Mitarbeiter im FB bezieht immer den Inhaber / die Inhaberin mit ein. **Falls "ja" - weiter mit Frage 65**		X		

Diese Angaben sind wichtig, da die Antworten in die Dokumentation des VVT und der TOM einfließen.
Ja = diese Daten werden von dem Betrieb verarbeitet
Nein = diese Daten werden nicht in die Dokumentation übernommen

40	**Adressdaten**	Name, Nachname, Straße, Hausnummer, Land, Ort, PLZ	X			
41	**Kontaktdaten**	Telefon, Mobilnummer	X			
42		E-Mail Adresse	X			
43	**Bewerber o. Praktikantendaten**	Kontaktdaten, Bewerbungsunterlagen	X			
44	**Ver-sicherungs-/ und Finanzdaten**	Krankenkasse	X			
45		Lohn- und Gehaltsdaten	X			
46		Bankverbindung	X			
47		Betriebliche Altersvorsorge	X			
48		Sozialversicherung	X			
49	**Biometrische Daten**	Fingerabdruck / Face Scan		X		
50	**Gesundheits-daten**	Krankheitsdaten / Tage etc.	X			
51	**Inhaltliche Daten**	Lebenslauf	X			
52		Qualifikationsdaten und Fortbildung	X			
53		Leistungsdaten (z.B. Ertrags-Statistik)	X			
54		Zeiterfassungsdaten (analog)		X		
55		Digitale Zeiterfassung	X			
56		Reisekostenabrechnung	X			
57		Urlaubsdaten / Kalender / Planung	X			
58		Dokumentation Mitarbeitergespräche	X			
59		Fotodateien	X			
60		Videodateien	X			
61		Ton- / Sprachaufnahmen	X			
62		Notwendige Einwilligungen werden von den Mitarbeiter eingeholt? (z.Bsp. Foto, Geburtstagskalender, Urlaubsplan, etc.)		X		X
63	**sonstige Daten**			X		

				Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
64	**Speicherort Mitarbeiter-daten**	Die Speicherung/Ver-arbeitung der o.g. Daten erfolgt z.B. in einer:	analogen Mitarbeiterakte (z.B. Papierakte o.ä.)	X			
			digitalen Mitarbeiterakte	X			

2. Zutrittskontrolle

Die Angaben in diesem Bereich dienen der Dokumentation in den TOM und der Auswertung des Gefährdungspotenzials im Maßnahmenplan.
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

				Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
65	**unbemerkter Zutritt**	Ist es möglich die Praxis unbemerkt zu betreten?			X		
66		Sind unbeaufsichtigte Neben-/Hintereingänge immer verschlossen?			X	X	
67		Die Praxistüren und Fenster entsprechen mindestens der Sicherheitsstufe RC3.		X			
68	**Schließanlage & Schlüssel**	Gibt es eine Schließanlage?		X			
69		Ist die Praxis mit registrierten Schlüsseln ausgestattet?		X		X	
70		Wird eine Schlüsselliste geführt?		X		X	
71		Welches System wird zum Führen der Schlüsselliste verwendet?	analoge Schlüsselliste	X		X	
72			digitale Schlüsselliste (Verwaltungs-software)		X	X	
73		Erfolgt eine Ausgabe der Schlüssel nur gegen eine Quittung?			X		X
74	**Pin-Code Schließsystem**	Wird die Praxis mit einem PIN-Code abgeschlossen.			X	X	
75		Bei Kündigung / Ausscheidung eines Mitarbeiters wird der PIN-Code geändert.			X	X	
76	**Transponder- oder Fingerabdruck-Schließsystem**	Erfolgt der Zugang zur Praxis mit Hilfe eines Transponder/Fingerabdrucksystems?			X	X	
77		Werden bei Kündigung / Ausscheidung eines Mitarbeiters der Transponder eingezogen bzw. der registrierte Fingerabdruck umgehend gelöscht?			X	X	

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
78	**Fenster-sicherheit**	Die Fenster haben folgende einbruchhemmenden Merkmale:				
a)		Schließnocken	X			
b)		einbruchhemmende Verglasung	X			
c)		Getriebesperren (kleines Schloss am Handgriff)		X		
79	**Fenster-sicherheit**	Es gibt eine mündliche Vereinbarung mit allen Mitarbeitern, dass alle Fenster bei Dienstschluss kontrolliert werden	X		X	
80		Es gibt eine schriftliche Vereinbarung mit allen Mitarbeitern, dass alle Fenster bei Dienstschluss kontrolliert werden		X		X
81	**Privatbereich**	Private Türen sind mit "Zutritt nur für Personal", "Privat" o.ä. gekennzeichnet.	X		X	
82	**zusätzliche Sicherheits-systeme**	Gibt es eine funktionierende Alarmanlage? (optimal: Glasbruchsensoren, Bewegungsmelder, automatische Alarmmeldung über Mobilfunk, etc.)		X		
83		Besteht eine Videoüberwachung?		X		
84		Ist die Kamera aktiv?		X		
a)		Wird die Aufnahme gespeichert? *wenn nur eine Live Überwachung stattfindet, dann "nein" ankreuzen				
b)		Werden die Mitarbeiter über den Einsatz der Kamera/Kameras aufgeklärt und die Aufklärung schriftlich dokumentiert?				
c)		Existieren DSGVO konforme „Videoaufnahme“ Hinweisschilder?				
85	In welchem Bereich erfolgt die Videoüberwachung?					
86	Der Anmeldebereich ist Videoüberwacht und wird auf Bildschirme am Empfang und/oder in den Behandlungsräumen/-Kabinen übertragen. → *WICHTIG: Die Übertragung darf nur so lange aktiv sein, solange jemand den Bildschirm besetzt.*					

3. Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -Verfahren gehindert werden.
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
87	Software-schutz	Elektronische Geräte, die persönliche Daten speichern, werden per Benutzername, Passwort o.ä. Maßnahmen gesichert. (ideal: 8 Zeichen; Groß-/Kleinbuchstaben, Zahlen, ein Sonderzeichen)	X		X	
88		Auf den Geräten installierte Datenverarbeitungs-Software ist zusätzlich durch Benutzername und Passwort o.ä. gesichert (optimal: 8 Zeichen, Groß-/Kleinbuchstaben, Zahlen, etc.).	X		X	
89		Es besteht ein allgemeiner Zugangsaccount, der für alle Mitarbeiter gilt.		X	X	
90		Jeder Mitarbeiter erhält einen persönlichen Account und jeweilige Zugangsrechte.	X		X	
91		Alle Passwörter werden in regelmäßigen Abständen verändert (mindestens einmal im Jahr).		X		X
92		Jedes elektronische Gerät (PC, Laptop, Tablet, etc.) hat eine automatische Inaktivitätssperre, welche den Bildschirm nach spätestens 5 Minuten Inaktivität abschaltet.	X		X	
93		Lässt sich eine aktivierte Inaktivitätssperre / Bildschirmschoner nur durch erneute Eingabe der Zugangsdaten (Passwort und Benutzername) wieder aufheben?	X		X	
94	Firewall und Wartung	Alle Geräte und die Software werden regelmäßig gewartet/aktualisiert.	X		X	
95		Es wird eine Firewall und Anti Virus Software benutzt / eingesetzt, die regelmäßig auf den neuesten Stand gebracht wird.	X			
96		Hersteller/Lieferanten für Firewall und Software?	Microsoft Defender			
97	Zuständigkeit für Wartung und Aktualisierung	Die Aktualisierung erfolgt durch: *bitte ankreuzen				
a)		Praxismitarbeiter / Inhaber selbst	X		X	
b)		Automatisierte Softwareeinstellung in festen Intervallen.	X		X	
c)		Externer Systemadministrator / IT Dienstleister * bei externen Dienstleistern bitte im nächsten Feld die Kontaktdaten eintragen.	X		X	

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
98	**System-administrator**	Wenn die Einhaltung der Datenschutzrichtlinien / Aktualisierung der Software im IT Bereich durch einen vertraglich beauftragten externen Systemadministrator überwacht wird, bitte hier die Kontaktdaten eintragen - sonst streichen. *hierfür wird ein AVV benötigt (Vorlage im Konzept). Die Angabe wird benötigt für die AVV Liste, VVT und TOM Dokumentation.				
		Scheffelmeier Richter GbR, Bitterfelder Straße 4, 04129 Leipzig				
a)		AVV / AGB notwendig?	X			
b)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X
99	**interner Server**	Wird ein **interner Server** genutzt?	X			
a)		Ist der Server vor fremden Zugriff geschützt?	X		X	
100	**externe Server (Cloud)**	Werden **externe Server** (Cloudserver) genutzt?		X		
a)		Stehen die Rechenzentren innerhalb der EU oder sind durch entsprechende Verträge der DSGVO unterworfen?				
b)		Welcher Anbieter wird genutzt? *die Angabe wird benötigt für die AVV Liste und TOM Dokumentation				
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				
101	**Netzwerk-sicherheit**	Nutzt der Betrieb einen WLAN Anschluss? Wenn der Betrieb kein W-LAN nutzt **"Nein"** ankreuzen und **weiter mit Frage 102**	X			
a)		Welcher WLAN Anbieter wird genutzt? (Hardware / Router) *die Angabe wird benötigt für die AVV-Liste und TOM Dokumentation	FritzBox - AVM Computersysteme Vertriebs GmbH, Alt-Moabit 95, 10559 Berlin			
b)		AVV / AGB notwendig?	X			
c)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)	X		X	

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
d)	Netzwerk-sicherheit	Ist der Router vor fremden Zugriff geschützt?	X		X	
e)		Ist die Nutzeroberfläche des Internet-Routers mit einem extra Passwort geschützt?	X		X	
f)		Wurde das Passwort und die Zugangsdaten geändert? (wenn der Aufkleber mit den Zugangsdaten auf der Geräterückseite noch zu sehen ist, sollte das PW dringend geändert werden)	X		X	
g)		Ist der Zugriff mit einem 12 Stellen langen Passwort (WPA2 Schlüssel) gesichert mit Groß-, Kleinbuchstaben, Zeichen, Zahlen?	X		X	
h)		Sind WPS und Broadcasting ausgeschaltet?		X		X
i)		Wird ein Virtual Private Network genutzt (VPN)? [VPN steht für "Virtual Private Network" und beschreibt eine Technik, die es Ihnen erlaubt, von jedem Ort auf der Welt sicher auf Ressourcen in Ihrem privaten Netzwerk zuzugreifen. VPN verschlüsselt Ihre Internetverbindung beginnend von Ihrer Netzwerkkarte bis hin zu einem VPN-Server. Ihre Internetverbindung wird durch die Nutzung von VPN vollständig verschlüsselt.]		X		
j)		Der MAC-Filter (bei LAN oder WLAN) ist eingeschaltet und erlaubt lediglich Verbindungen von bereits bekannten / registrierten Geräten.		X	X	
k)		Erhalten Patienten / Besucher die Möglichkeit einen Gastzugang zu nutzen?		X		
102	mobile Datenträger	Werden Daten werden auf mobilen Datenträgern gespeichert? *Angaben werden benötigt für TOM Dokumentation. Wenn keine mobilen Datenträger verwendet werden "NEIN" und weiter mit der nächsten Frage.		X		
a)		USB Stick				
b)		Wird der USB Stick durch Passwort/Zugangsdaten verschlüsselt?				
c)		Wird der USB Stick nach Benutzung sicher verschlossen aufbewahrt?				
d)		externe Festplatte/CD/Bandlaufwerk				
e)		Wird der externe Datenträger durch Passwort/Zugangsdaten verschlüsselt?				
f)		Wird der externe Datenträger nach Benutzung sicher verschlossen aufbewahrt?				

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
103	**Diensthandys**	Werden Dienst- oder Praxishandys genutzt? (Mobilfunkvertrag)		X		
a)		Welcher **Hardware Hersteller** wird genutzt? (z.Bsp. Apple, Samsung)				
b)		Welcher **Netzanbieter** wird genutzt? *die Angabe wird benötigt für die AW Liste und TOM Dokumentation				
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				
104	**private Handys**	Werden private Handys zur Patientenkommunikation genutzt?		X		
105	**Messenger Dienste**	Werden Messenger Dienste zur Kommunikation mit Patienten oder Mitarbeitern genutzt?		X		
a)		WhatsApp				
b)		Threema				
c)		Signal				
d)		sonstiges bitte eintragen:				
e)		Liegt eine rechtskonforme, unterschriebene Einwilligungserklärung vor?				
106	Wir empfehlen einen Wechsel zu Signal oder Threema, wenn nicht ganz auf den Einsatz von Messengerdiensten verzichtet werden kann.					

4. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die, ihrer Zugriffsberechtigung unterliegenden, personenbezogenen Daten zugreifen können und dass die bei der Bearbeitung verwendeten personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
107	**analoge Daten, Patientenakten, Karteikarten**	Besteht eine Verschwiegenheitserklärung wie mit den personenbezogenen Daten (sowohl analog als auch digital) umgegangen wird? (Arbeitsvertrag reicht nicht)		X		X
108		Sind alle physischen Dokumente / Unterlagen grundsätzlich abschließbar und sicher gelagert.		X		X

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
109	**analoge Daten, Patientenakten, Karteikarten**	Alte Patientenakten sind abschließbar und getrennt von aktuellen Akten gelagert.	X		X	
110		Alle Gesundheitsdaten werden nur auf die Innenseite der Patientenunterlagen geschrieben oder in das Innere der Karteikarte gelegt.	X		X	
111		Liegen Patientenakten / -Unterlagen offen und für jeden einsehbar herum?	X			X
112		Werden Akten für die nächste Behandlung so zurechtgelegt, dass Unbefugte Einblick nehmen können?	X			X
113		Rezepte können vom Patienten so unterschrieben werden, dass niemand Unbefugtes Einblick in das Rezept erhält.	X		X	
114		Werden Unterlagen / Dokumente direkt nach dem Gebrauch wieder in den jeweiligen Aktenschrank eingeschlossen?	X		X	
115		Werden Patientenunterlagen in den Behandlungsräumen verwahrt?		X	X	
a)		Werden diese in verschließbaren Schränken gelagert?		X	X	
116		Werden vorrübergehend unverschlossen abgelegte Unterlagen/Dokumente/Akten so abgedeckt, dass Unbefugte keine Kenntnis vom Inhalt nehmen können?	X		X	
117		Werden alle analogen Unterlagen mit personenbezogenen Daten (z.B. Patientenakten, Karteikarten, Rezepte, Terminkalender, etc.) direkt eingeschlossen und verstaut, wenn der Raum oder die Anmeldung unbeaufsichtigt sind?	X		X	

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
118	**digitale Daten**	Elektronische Daten werden auf folgenden Geräten verarbeitet: *bitte ankreuzen	X			
a)		Laptop		X		
b)		Tablet	X			
c)		Fest installierter PC	X			
d)		Sind die Geräte ausreichend gegen Diebstahl geschützt? *wenn der Schutz nicht ausreichend ist, bitte alternative Schutzmal\nahmen vorschlagen - siehe nächster Punkt.	X		X	

119	Vor Diebstahl bereits geschützt durch:	Verschlossener Raum
120	Maßnahmenempfehlung zum Diebstahlschutz:	

Anmeldebereich, Tresen, Rezeption			**Ja**	**Nein**	**Maßnahme nicht erforderlich**	**Maßnahme erforderlich**
121	**Empfang**	Werden alle Besucher persönlich empfangen?	X			
122		Gibt es einen klassischen Empfangsbereich mit Tresen?	X			
123		Befindet sich die Anmeldung in einem abgeschlossenen Raum?		X		
124		Werden Patienten durch geeignete Maßnahmen (z.Bsp. ein Schild, Aufkleber, Fußmatte o.ä.) zur Wahrung der Diskretion angehalten?		X		X
125		Es existiert ein Aushang für Patienten im Empfangs-/Wartebereich zum Thema Datenschutz		X		X
a)		Ist der Aushang DSGVO konform?		X		X
126		Ist der Anmeldebereich so angelegt, dass diskrete (Telefon-) Gespräche hier möglich sind?		X		
127	**Gesprächs-führung**	Wurde schriftlich mit allen Mitarbeitern vereinbart, keine vertraulichen Patientengespräche in Hörweite anderer zu führen.		X		X
128		Wird ein Rückruf zu gegebener Zeit vereinbart, falls es nicht möglich ist ein privates und ungestörtes Telefongespräch zu führen?	X		X	
129		Werden die Fenster und Türen im jeweiligen Raum geschlossen, wenn vertrauliche Gespräche geführt werden müssen?	X		X	

Anmeldebereich, Tresen, Rezeption			**Ja**	**Nein**	**Maßnahme nicht erforderlich**	**Maßnahme erforderlich**
130	**Gesprächs-führung**	Ist der Anrufbeantworter auf „Stumm“ oder lautlos geschaltet, so dass man nicht mithören kann, was auf Band gesprochen wird?	X		X	

Anmeldebereich, Tresen, Rezeption			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
131	Sprachbox	Wird eine Online-Sprachbox genutzt?		X		
a)		Welcher Anbieter wird genutzt? *die Angabe wird benötigt für die AW Liste und TOM Dokumentation				
b)		AVV / AGB notwendig?				
c)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Terminkalender			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
132	Terminkalender/ Trainingsplan wird schriftlich geführt.	Der Terminkalender wird als Buch **schriftlich** (analog) geführt		X		
a)		Der Kalender / der Plan wird so bearbeitet, das Unbefugte ihn nicht einsehen können. → Auch beim Überbeugen.				
b)		Es besteht die schriftliche Anweisung den Kalender / den Plan, außer bei Benutzung, geschlossen zu halten.				
c)		Der Plan / Der Kalender wird, sobald dieser unbeaufsichtigt ist (der Arbeitsplatz verlassen wird), sicher eingeschlossen.				
133	Der Terminkalender/ Trainingsplan wird digital geführt.	Der Terminkalender wird digital geführt	X			
a)		Wird der Kalenderausdruck zusätzlich ausgehängt?	X			
b)		Alle Bildschirme / Monitore (PC, Laptop, Tablet, etc.) sind so aufgestellt, dass es für einen Unbefugten nicht möglich ist die Inhalte einzusehen.		X		
c)		Wird mit Hilfe einer Spiegelfolie / Sichtschutzfolie verhindert, dass die Monitore für Außenstehende einsehbar sind? *Damit kein seitliches Einsehen möglich ist, wenn die Monitore nicht anders aufgestellt werden können. Sollten die Monitore blickgeschützt aufgestellt sein, bitte "nein" angeben und "Maßnahme nicht erforderlich"		X		X
d)		Besteht die schriftliche Anweisung, dass man sich abmelden muss, sobald man den Arbeitsplatz verlässt? *Der Zugang muss gesperrt werden, bis zum nächsten Anmelden.	X		X	

In der Praxis gelagerte, patientenbezogene und mehrfach genutzte Utensilien (z.Bsp. Handtücher, persönliche Lagerungshilfen, Ersatzkleidung oder mehrfach nutzbare Therapiegerätaufsätze)			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
134	Kenn-zeichnung von Patienten-eigentum	Werden private Utensilien von Patienten in der Praxis gelagert?	X		X	
135		Werden die Utensilien mit Namen gekennzeichnet?	X		X	
a)		Zugriff durch Patienten möglich? Schutz der Namen der anderen Patienten		X	X	
b)		Die jeweilig benötigten Utensilien werden von Praxismitarbeitern vor Behandlung an den Patienten persönlich ausgegeben.	X		X	

Ausfüllen des Anamnese- /Anmeldebogens:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
136	Anamnese/ Anmeldung	Der Anmeldebogen wird dem Patienten mitgegeben, bzw. zur Verfügung gestellt, um ihn bei sich zuhause auszufüllen. Der Bogen wird ausgefüllt zum nächsten Termin wieder mitgebracht.		X	X	
137		Patienten erhalten eine Schreibmappe, um die Unterlagen im Wartebereich auszufüllen. **(Schutz)**	X		X	
138		Der Anamnesebogen wird gemeinsam im Gespräch zwischen Behandler und Patienten ausgefüllt.	X		X	
139		Erfolgt die Besprechung des Anamnesebogens in einem geschlossenen Raum, um die Privatsphäre zu sichern?	X		X	

Löschung und Vernichtung von sensiblen, personenbezogenen Daten:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
140	Lösch-verfahren und Löschfristen	Wird ein Aktenvernichter der Sicherheitsstufe 4 gemäß DIN 66399-2 (Kreuzschnitt; bzw. Partikelschnitt) eingesetzt?	X		X	
141		Wird ein Dienstleister (unter Beachtung der DIN 66399) eingesetzt, um Daten zu vernichten?		X		
a)		Welcher Anbieter wird genutzt? *die Angabe wird benötigt für die AW Liste und TOM Dokumentation				

Löschung und Vernichtung von sensiblen, personenbezogenen Daten:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
b)	Lösch-verfahren und Löschfristen	Mit Sonderstatus und Löschprotokoll?				
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				
142	Daten-vernichtung	Erfolgt die Datenvernichtung regelmäßig (gem. der gesetzl. Anforderungen)?	X		X	
a)		In welchen Zeitabständen?	Täglich und bei Bedarf			
b)		Alle Löschfristen entsprechen den gesetzlichen Anforderungen, sind schriftlich festgelegt und allen Verantwortlichen bekannt gegeben. (z.B. Patientendaten 10 Jahre laut §630 f. BGB, bis 30 Jahre §199 Abs.2 BGB)	X		X	

5. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern, nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
"Ja/ Nein -- Dokumentation in den TOM
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

Drucker und Faxgeräte			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
143	Faxgeräte und Drucker	Wird ein Drucker genutzt?	X			
144		Wird ein Faxgerät genutzt?	X			
a)		Leitet das Gerät die Faxe per E-Mail an die Empfänger weiter?	X		X	
b)		Werden eingehende Faxe erst ausgedruckt, sobald ein dazu befugter Mitarbeiter den Druck anfordert?		X	X	
145		Stehen die Geräte in einem separaten, abschließbaren Raum, welcher nur von einem Angestellten betreten werden kann?		X	X	
146		Sind die Geräte im Anmeldebereich so positioniert, dass Unbefugte keinen Blick auf eingehende oder ausgehende Dokumente werfen können?		X	X	

Kommunikation per E-Mail:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
147	gesamter E-Mail Verkehr	Nutzt die Praxis E-Mails zur Kommunikation mit anderen Parteien? (z.B. Ärzte, Therapeuten, Patienten, Lieferanten, etc.)	X			
148		Werden Patienten zu Werbezwecken per E-Mail kontaktiert und haben Sie sich hierfür die schriftliche Genehmigung eingeholt (auch Informationsmails, Newsletter, Werbezwecke)?		X	X	
149		Bei sensiblen personenbezogenen Daten werden die Dokumente zusätzlich mit einem Passwortschutz versehen.		X		X
150		Haben Sie Einwilligung zur Nutzung unverschlüsselter Kommunikationsmittel von Ihren Patienten eingeholt? *gilt auch für Versand von Patientendaten an andere an der Behandlung beteiligte Stellen		X		X
151		Welches E-Mail Programm wird verwendet? "Die Angabe wird benötigt für die VVT und die TOM Dokumentation	Microsoft Outlook			
152		TSL / SSL ist aktiviert. (Transport Layer Security / Secure Socets Layer → Protokoll, das eine Verschlüsselung von Datenübertragungen im Internet gewährleistet. (Ohne, wird die Mail im "Klartext" übertragen und kann leicht abgefangen und mitgelesen werden)	X		X	

Abrechnung und Verwaltungssoftware:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
*Die folgenden Angaben werden benötigt für die VVT und die TOM Dokumentation sowie ggf. für die AVV - Liste. Bitte genaue Angaben machen (z.Bsp. Noventi hat mehrere Untergruppen) . Nicht Zutreffendes bitte streichen.						
153	GKV	Wird mit der **GKV** abgerechnet?	X			
154	GKV Abrechnung mit Hilfe z. B. eines EDV Programms o.ä.	Wird die GKV Abrechnung mit Hilfe eines EDV Programms **selbst in der Praxis** gemacht?	X			
		Mit welchem **EDV- Programm oder Verwaltungstool** (z.B. Theorg, Microsoft Office o.ä.) wird die GKV - Abrechnung erstellt?	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg			
		AVV / AGB notwendig?	X			
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X

Abrechnung und Verwaltungssoftware:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
155	**GKV** **Abrechnung mit Abrechnungs-dienstleister**	Wurde zur Durchführung der GKV Abrechnung ein externer **Dienstleister** oder ein **Abrechnungszentrum von der Praxis beauftragt**?		X		
		Mit der GKV Abrechnung wurde folgender **Dienstleister/Abrechnungszentrum** (z.B. OptaData, RZH, Noventi o.ä.) beauftragt:				
		AVV / AGB notwendig?				
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				
156	**PKV**	Wird mit der **PKV** abgerechnet?	X			
157	**PKV** **Abrechnung mit Hilfe z. B. eines EDV Programms o.ä.**	Wird die **PKV** Abrechnung mit Hilfe eines EDV Programms **selbst in der Praxis** gemacht?	X			
		Mit welchem **EDV- Programm oder Verwaltungstool** (z.B. Theorg, Microsoft Office o.ä.) wird die **PKV** - Abrechnung erstellt?	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg			
		AVV / AGB notwendig?	X			
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X
158	**PKV** **Abrechnung mit Abrechnungs-dienstleister**	Wurde zur Durchführung der PKV Abrechnung ein externer **Dienstleister** oder ein **Abrechnungszentrum von der Praxis beauftragt**?		X		
		Mit der **PKV** Abrechnung wurde folgender **Dienstleister/Abrechnungszentrum** (z.B. OptaData, RZH, Noventi o.ä.) von der Praxis beauftragt:				
		AVV / AGB notwendig?				
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Abrechnung und Verwaltungssoftware:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
159	BG	Wird mit der **BG** abgerechnet?	X			
160	**BG** **Abrechnung mit Hilfe z. B. eines EDV Programms o.ä.**	Wird die **BG** Abrechnung mit Hilfe eines EDV Programms **selbst in der Praxis** gemacht?	X			
		Mit welchem **EDV- Programm oder Verwaltungstool** (z.B. Theorg, Microsoft Office o.ä.) wird die **BG** - Abrechnung erstellt?	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg			
		AVV / AGB notwendig?	X			
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X
161	**BG** **Abrechnung mit Abrechnungs-dienstleister**	Wurde zur Durchführung der **BG** Abrechnung ein externer **Dienstleister** oder ein **Abrechnungszentrum von der Praxis beauftragt**?		X		
		Mit der **BG** Abrechnung wurde folgender **Dienstleister/Abrechnungszentrum** (z.B. OptaData, RZH, Noventi o.ä.) von der Praxis beauftragt:				
		AVV / AGB notwendig?				
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Abrechnung und Verwaltungssoftware:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
162	**Bar und Zuzahlungen**	Werden Bar- und Zuzahlungen abgerechnet?	X			
163	**Bar und Zuzahlungen** **Abrechnung mit Hilfe z. B. eines EDV Programms o.ä.**	Wird die Abrechnung der **Bar und Zuzahlungen** mit Hilfe eines EDV Programms **selbst in der Praxis** gemacht?	X			
		Mit welchem **EDV- Programm oder Verwaltungstool** (z.B. Theorg, Microsoft Office o.ä.) wird die Abrechnung der **Bar und Zuzahlungen** erstellt?	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg			
		AVV / AGB notwendig?	X			
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X

Abrechnung und Verwaltungssoftware:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
164	**Bar und Zuzahlungen** **Abrechnung mit Abrechnungs-dienstleister**	Wurde zur Durchführung der Abrechnung der **Bar und Zuzahlungen** ein externer **Dienstleister** oder ein **Abrechnungszentrum von der Praxis beauftragt**?		X		
		Mit der Abrechnung der **Bar und Zuzahlungen** wurde folgender **Dienstleister / Abrechnungszentrum** (z.B. OptaData, RZH, Noventi o.ä.) von der Praxis beauftragt:				
		AVV / AGB notwendig?				
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				
165	**Selbstzahler**	Werden **Selbstzahler-Leistungen** abgerechnet?	X			
166	**Selbstzahler (Training, Wellness, Kurse, etc.) Abrechnung mit Hilfe z. B. eines EDV Programms o.ä.**	Wird die Abrechnung der **Selbstzahler-Leistungen** mit Hilfe eines EDV Programms **selbst in der Praxis** gemacht?	X			
		Mit welchem **EDV- Programm oder Verwaltungstool** (z.B. Theorg, Microsoft Office o.ä.) werden die **Bar und Zuzahlungen** - Abrechnung erstellt?	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg			
		AVV / AGB notwendig?	X			
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X
167	Erfolgt bei Zuzahlungen ein Eintrag ins das analoge Kassenbuch?			X	X	
168	**Hausbank der Praxis**	Wird elektronischer Zahlungsverkehr angeboten?	X			
		Die Abrechnung erfolgt über Überweisungen (Geldinstitut der Praxis eintragen) *für Überweisungs-verkehr ist kein AVV erforderlich	Hypo Vereinsbank			

Abrechnung und Verwaltungssoftware:				Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
169	Kartenzahlung	Besteht die Möglichkeit, Rechnungen per Kartenzahlung zu begleichen (Kartenlesegerät)?		X			
		Die Abrechnung erfolgt über Kartenzahlung / Kartenlesegerät (genutzten Anbieter eintragen)	Sparkasse Leipzig				
170	Bezahldienste	Besteht die Möglichkeit, Rechnungsbeträge mittels anderer Anbieter zu begleichen? (z.Bsp. PayPal, Vpay, Apple Pay, etc.)		X			
		Die Abrechnung erfolgt über folgenden Online Anbieter: (genutzten Anbieter eintragen)	PayPal (Europe) S.à.r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg (Gutscheine)				
		AVV / AGB notwendig?		X			
		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X			

Hausbesuche			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
171	Sicherer Daten-Transport	Werden Hausbesuche durchgeführt? *wenn "nein" - weiter mit Frage 172	X			
a)		Verfügt jeder Behandler über eine eigene, sicher verschließbare Mappe zum Transport von Patientenakten?	X		X	
b)		Die Umlaufmappe wird in sicheren Transporttaschen zum Patienten befördert. → Persönliche Handtaschen o.ä. sind nicht erlaubt!	X		X	
c)		Es gibt eine mündliche Vereinbarung bzgl. Regeln zu Hausbesuchen.	X			
d)		Es gibt eine schriftliche Vereinbarung bzgl. Regeln zu Hausbesuchen.		X		X
e)		Nach Hausbesuchen werden die Patientenunterlagen in die Praxis zurückgebracht.	X		X	
f)		Nach den Hausbesuchen werden die Patientenunterlagen mit nach Hause genommen und dann dort sicher verschlossen aufbewahrt.	X		X	

Home Office / Datenschutz zu Hause			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
172	Datenschutz zu Hause	Wird ein Home Office genutzt? *wenn nein - weiter mit Frage 173	X			
a)		Werden Akten / Unterlagen zu Hause dauerhaft aufbewahrt?	X			
b)		Werden die Akten sicher verschlossen aufbewahrt?	X		X	
c)		Erfolgt der Transport der Daten / analogen Akten in geeigneter, geschützter Weise?	X		X	
d)		Wird für Mitarbeiter im Home Office eine schriftliche Arbeitsanweisung zum Umgang mit Daten/Akten zu Hause erstellt?		X	X	
e)		Welche Hardware wird im Home Office verwendet? (Privater oder Firmen PC/Laptop?)	PC			
f)		Wie wird die Hardware vor fremden Zugriff geschützt? (Stichwort: Diebstahlschutz)	Verschlossener Raum			
g)		Welche Software/ welches Programm wird zur Bearbeitung verwendet?	Microsoft Windows			
h)		Wie sind die Daten auf dem Gerät vor unbefugtem Zugriff geschützt?	Passwort geschützt			

6. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
**Ja/ Nein = Dokumentation in den TOM*

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
173	Protokollierung	Wird jede Änderung in einem personenbezogenen Datensatz (z.B. Namensänderung, Änderung des Wohnorts oder der Kontaktdaten, etc.) protokolliert / festgehalten (z.Bsp. Per Datum und Namenszeichen)?	X		X	
174		Gibt es personalisierte Benutzerprofile, damit genau ermittelt werden kann, wer bestimmte Datensätze ändert, erhebt oder löscht? (elektrisch)	X		X	

7.Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

Daten-Sicherungen / Sicherungskopien				Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
175	Sicherungen	Existiert ein Datensicherungskonzept (hier zählen auch Kopien von analogen Akten)?		X		X	
176		Erfolgen alle Sicherungen der Daten zu festgelegten Intervallen?		X		X	
a)		Festgelegtes Intervall	Täglich				

Daten-Sicherungen / Sicherungskopien			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
177	digitale Sicherungen	Erfolgen Datensicherungen elektronisch?	X		X	
a)		Erfolgen die Sicherungen auf USB-Sticks?		X		
b)		Erfolgen die Sicherungen auf internen Festplatten?		X		
c)		Erfolgen die Sicherungen auf externen Festplatten / Bändern / CD ?		X		
d)		Erfolgen die Sicherungen auf einem netzwerkgebundenen sicheren Datenserver (NAS).	X			
178	Hardware Sicherung	Wird die zur Sicherung verwendete Hardware vor Datenverlust/Diebstahl gesichert?	X		X	
a)		Wird die Hardware nach der Benutzung in einem Tresor verwahrt?				
b)		Wird die Hardware nach der Benutzung in einem abschließbaren Schrank verwahrt?				
179	Cloud Speicherung	Erfolgen die Sicherungen in einer Cloud?		X		
a)		Welcher Cloudanbieter wurde beauftragt?				
b)		AVV / AGB notwendig?				
c)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Daten-Sicherungen / Sicherungskopien			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
180	Serverraum	Gibt es einen separaten abschließbaren Serverraum? *wenn nein - weiter mit Frage 181		X		
a)		Verfügt der Raum über eine unterbrechungsfreie Stromversorgung?				
b)		Ist der Raum mit einer Klimaüberwachung versehen? (Stichwort: Überhitzungsschutz)				
C)		Wird der Raum verschlossen gehalten?				
181	Serverschrank	Gibt es einen separaten abschließbaren Serverschrank? Wenn "Nein" - weiter mit der nächsten Frage		X		
a)		Verfügt der Serverschrank über eine unterbrechungsfreie Stromversorgung?				
b)		Ist der Serverschrank mit einer Klimaüberwachung versehen? (Stichwort: Überhitzungsschutz)				
c)		Wird der Serverschrank verschlossen gehalten?				
182	Brandschutz	Ist an jeder Schlüsselstelle der Praxis ein Feuerlöscher angebracht?	X		X	
183		Gibt es in jedem kritischen/relevanten Raum Feuer- und Rauchmelder?	X		X	
184	Diebstahlschutz	Existiert ein schriftlicher Notfallplan? → Wenn z.B. PC, Aktentasche oder Terminbuch gestohlen werden.		X		X

8. Trennungsgebot / Trennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan
Mehrfachnennung ist möglich.

Behandlungsbereiche			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
185	Datenschutz in "offenen" Bereichen der Praxis	Sind die Behandlungszimmer baulich voneinander getrennt? eigene, geschlossene Räume mit Türen	X		X	
186		Sind die Behandlungsbereiche lediglich mit einer hellhörigen Trennwand oder einem Vorhang getrennt? (Behandlungskabinen)		X	X	
187		Befindet sich das Wartezimmer in einem separaten, eigens dafür vorgesehenen Raum? Gespräche an der Rezeption oder aus den Räumen sind nicht hörbar.	X		X	

188	Datenschutz in "offenen" Bereichen der Praxis	Befindet sich der Wartebereich offen in der Nähe des Anmeldebereichs? (z.Bsp. auf dem Flur, so dass Gespräche mitgehört werden könnten)	X		X	
189		Werden Patienten in den offenen Bereichen darüber aufgeklärt, dass Diskretion nicht zu 100% hergestellt werden kann?		X		X

9. Datenschutz - Mitarbeiter

Maßnahmen, die die datenschutzrechtlichen Anforderungen für die Mitarbeiter umsetzen.
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
190	Mitarbeiter	Haben alle Mitarbeiter an einer Datenschutz-Basis-Schulung teilgenommen?		X		X
191		Haben alle Mitarbeiter schriftlich in die erweiterte Datenverarbeitung eingewilligt?		X		X
192		Werden Nachschulungen mindestens jährlich durchgeführt und dokumentiert? (→ Wahrung der Betroffenenrechte)		X		X
193		Wurden alle schriftlich auf das Datengeheimnis verpflichtet?		X		X
194		Wurden alle mündlich auf das Datengeheimnis verpflichtet?	X			

Weitere Bemerkungen und Hinweise zum Bereich Mitarbeiter - Datenschutz	

10. Auskunftsanspruch des Betroffenen

Nach §34 BDSG gilt der Auskunftsanspruch von Betroffenen gegenüber jeder Stelle, die personenbezogene Daten von ihm gespeichert hat - bei unrichtiger oder unvollständiger Auskunft drohen Bußgelder.
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

Auskunftsrecht nach § 15 DSGVO		Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
195	Gibt es ein System zur genauen Identifikation und Auffindung von Patientendaten (auch analoge Akten)? → z.B. wenn der Patient Auskunft ersucht (Auskunftsrecht nach Artikel 15 DSGVO)	X		X	
196	Wurde schriftlich festgelegt, wer berechtigt ist, die Auskünfte zu erteilen?	X			
197	Wer darf Auskünfte im Namen der Einrichtung erteilen?	Inhaberin			

11. Verhalten bei Datenschutzverstößen

Nach Art.33 – EU-DSGVO meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (nachdem ihm die Verletzung bekannt wurde).
**Ja/ Nein = Dokumentation in den TOM*
Maßnahme erforderlich = Eintrag einer Handlungsempfehlung im Maßnahmenplan

Datenverlust			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
198	Notfall-absicherung	Besteht ein Notfallplan für die Meldung von Verstößen?		X	X	
199		Besteht eine Absicherung in der Berufshaftpflicht gegen Schadenersatzansprüche von Betroffenen?		X	X	
200		Besteht eine Absicherung für Gerichtskosten in der Rechtsschutzpolice bei DSGVO Verstößen mit Verfahren?		X	X	
201		Ist der Status der Absicherung zum Zeitpunkt des Audits bekannt? bei "nein" - auch "Maßnahme erforderlich" ankreuzen, um hier eine Maßnahmenempfehlung auszusprechen		X	X	

12. Zusätzlicher Fragenteil für AVV & VVT

				Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
202	Arbeitsschutz	Werden Arbeitsschutzmaßnahmen durchgeführt und dokumentiert?		X		X	
203	Ärzte	Werden die Daten zu behandelnden/überweisenden Ärzten gespeichert?		X		X	
a)		Welches System wird dazu verwendet?	Patienten-Karteikarte	X		X	
b)			Verwaltungssoft-ware (eGK)	X		X	
204	Fuhrpark	Werden Daten zu Dienstfahrzeugen gespeichert (Fahrtenbuch)?			X		
a)		Welches System wird dazu verwendet?	analoges Fahrtenbuch				
b)			digitales Fahrtenbuch (Navigationsgerät o.ä.)				

			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
205	Lieferanten	Werden Kontaktdaten von Herstellern / Lieferanten oder werden Kataloge o.ä. gespeichert/aufbewahrt?	X		X	

Videobehandlung, Telemedizin (therapeutisch/medizinische Online- Behandlung oder Beratung)			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
206	**Online - Behandlung**	Wird die Behandlung / Beratung per Video / Telemedizin angeboten? *wenn nein - weiter mit Frage 207		X		
a)		Werden die schriftlichen Einwilligungserklärungen vorab eingeholt?				
b)		Welcher Anbieter wird verwendet?				
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Kurse, Rehasport			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
207		Wird Rehasport angeboten?		X		
208		Werden Kurse angeboten?		X		
a)		Werden die Kurse von externen Anbietern angeboten (z.Bsp. Rehasportverein, Ernährungsberatung, o.ä.)?		X		
b)		Werden z.Bsp. Kontaktdaten von Teilnehmern/Mitgliedern über die Praxis weiterverarbeitet? *Diese Angabe wird benötigt für die VVT Liste sowie die TOM Dokumentation				
c)		Welcher externe Anbieter führt die Kurse durch?				
d)		AVV / AGB notwendig?				
e)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Videokurse (Sportangebote o.ä.)			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
209		Werden Videokurse angeboten ? *wenn nein - weiter mit Frage 210		X		
a)		Werden die notwendigen schriftlichen Einwilligungen eingeholt?				
b)		Welcher Anbieter wird verwendet?				
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Geräte mit Speicherfunktion			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
210	Geräte mit Speicher-funktion	Werden Geräte mit Speicherfunktion für Therapie, Training oder Behandlung genutzt (z.Bsp. Milon Zirkel o.ä.) *wenn nein - weiter mit Frage 211		X		
a)		Werden die notwendigen schriftlichen Einwilligungen zur Datenverarbeitung durch den externen Anbieter eingeholt bzw. erfolgt eine schriftliche Aufklärung über Umfang und Weise der Speicherung?				
b)		Welcher Anbieter wird verwendet?				
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Sonstige Software Tools			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
211	Software, Tools o.ä.	Nutzen Sie weitere Software Tools, z.Bsp. für Diagnostik, Führung, Coaching, Beratung o.ä.? *wenn nein - weiter mit Frage 212		X		
a)		Werden die notwendigen schriftlichen Einwilligungen zur Datenverarbeitung durch den externen Anbieter eingeholt bzw. erfolgt eine schriftliche Aufklärung über Umfang und Weise der Speicherung?				

Sonstige Software Tools			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
b)		Welcher Anbieter wird verwendet? **Anbieter Nr. 1**				
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				
e)		Welcher Anbieter wird verwendet? **Ggf. Anbieter Nr. 2**				
f)		AVV / AGB notwendig?				
g)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Die **Steuerbuchhaltung** wird durchgeführt von:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
212		Praxis selbst?		X		
a)		Welcher Dienstleister wurde mit der Steuerbuchhaltung beauftragt? *Diese Angaben werden benötigt für das Konzept und die VVT.				
b)		Braune & Tauche Steuerberater-Partnerschaft mbB Inselstraße 31, 04103 Leipzig				
c)		AVV / AGB notwendig?		X		
d)		AVV / AGB liegen vor **(ja ankreuzen)** oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X	X	

Die **Finanzbuchhaltung** wird durchgeführt von:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
213		Praxis selbst?		X		
a)		Welcher Dienstleister wurde mit der Finanzbuchhaltung beauftragt? *Diese Angaben werden benötigt für das Konzept und die VVT.				
b)		Braune & Tauche Steuerberater-Partnerschaft mbB Inselstraße 31, 04103 Leipzig				
c)		AVV / AGB notwendig?		X		
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X	X	

Die **Lohnbuchhaltung** wird durchgeführt von:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
214		Praxis selbst?		X		
a)		Welcher Dienstleister wurde mit der Lohnbuchhaltung beauftragt? *Diese Angaben werden benötigt für das Konzept und die VVT.				
b)		Braune & Tauche Steuerberater-Partnerschaft mbB Inselstraße 31, 04103 Leipzig				
c)		AVV / AGB notwendig?		X		
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X	X	

Die **Kassenführung** für Barausgaben wird durchgeführt von:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
215		Praxis selbst?		X		
a)		Welches System / Welcher Dienstleister wird zur Kassenführung eingesetzt? *Diese Angaben werden benötigt für die VVT und ggf. die AVV-Liste.				
b)		Braune & Tauche Steuerberater-Partnerschaft mbB Inselstraße 31, 04103 Leipzig				
c)		AVV / AGB notwendig?		X		
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X	X	

Die **Auslagenabrechnung** wird durchgeführt von:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
216		Praxis selbst?		X		
a)		Welches System / Welcher Dienstleister wird zur Auslagenabrechnung eingesetzt? *Diese Angaben werden benötigt für die VVT und ggf. die AVV-Liste.				
b)		Braune & Tauche Steuerberater-Partnerschaft mbB Inselstraße 31, 04103 Leipzig				
c)		AVV / AGB notwendig?		X		
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X	X	

Für **Mahnwesen** ist zuständig:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
217		Praxis selbst?	X			
a)		Welches System / Welcher Dienstleister wird für das Mahnwesen eingesetzt? *Diese Angaben werden benötigt für das Konzept und die VVT.				
b)		THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg				
c)		AVV / AGB notwendig?	X			
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X

Für **Inkassoleistungen** ist zuständig:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
218		Praxis selbst?			X	
a)		Welches System / Welcher Dienstleister wird für Inkasso eingesetzt? *Diese Angaben werden benötigt für das Konzept und die VVT.				
b)						
c)		AVV / AGB notwendig?				
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Empfangsquittungen werden ausgestellt von:			Ja	Nein	Maßnahme nicht erforderlich	Maßnahme erforderlich
219		Praxis selbst?	X			
a)		Welches System / Welcher Dienstleister wird für Empfangsquittungen eingesetzt? *Diese Angaben werden benötigt für die VVT und ggf. die AVV-Liste.				
b)		THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg				
c)		AVV / AGB notwendig?	X			
d)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X

Genutzte Bürosoftware:			**Ja**	**Nein**	**Maßnahme nicht erforderlich**	**Maßnahme erforderlich**
220		Wird Bürosoftware eingesetzt?	X			

221	Büro-Software 1	Welches Verwaltungs- / Bürosoftware wird eingesetzt? *Diese Angaben werden benötigt für das Konzept und die VVT.				
a)		THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg				
b)		AVV / AGB notwendig?	X			
c)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)		X		X
222	Büro-Software 2	Welches Verwaltungs- / Bürosoftware wird eingesetzt? *Diese Angaben werden benötigt für das Konzept und die VVT.				
a)		Microsoft Office Microsoft Deutschland GmbH Walter-Gropius-Straße 5, 80807 München				
b)		AVV / AGB notwendig?	X			
c)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)	X		X	

Freiberufliche Mitarbeiter:			**Ja**	**Nein**	**Maßnahme nicht erforderlich**	**Maßnahme erforderlich**
223		Werden Freiberufliche Mitarbeiter beschäftigt?		X		
a)		AVV / AGB notwendig?		X	X	
b)		AVV / AGB liegen vor (ja ankreuzen) oder müssen noch angefordert werden (Nein & Maßnahme erforderlich ankreuzen)				

Zusammenfassung Auditbericht und Maßnahmenliste

Audit vom:	19.11.2024	
Betrieb:	Physiolounge GmbH	
Auditor:	Nenad Rogic	

Die Risikobewertung zur Erstellung eines Datenschutz-Konzeptes hat ergeben, dass folgende Punkte in unserer Praxis einer Handlung bzw. Neuorganisation bedürfen, um die Datensicherheit gemäß der DSGVO in unserer Praxis für unsere Mitarbeiter und Patienten weiter zu verstärken.

Die Umsetzung erfolgt umgehend, sofern organisatorische Maßnahmen notwendig sind (z.Bsp. Arbeitsanweisungen für Mitarbeiter, Anbringen von Hinweisschildern, o.ä.) und mindestens zeitnah, wenn zusätzliche Mittel zur Umsetzung beschafft werden müssen (z. Bsp. Aufbewahrungsmöbel, sichere Software, Diensthandys, etc.).

Nach Auswertung des Auditbogens haben wir hier eine Zusammenfassung der erfassten Mängel in einer To-do Liste für Sie zusammengestellt.
Wenn Sie alle Mängel in den verschiedenen Bereichen beseitigt (abgehakt) haben, senden Sie uns bitte die Liste unterschrieben zurück. Vielen Dank

1. Organisatorisches		erledigt
1	Es besteht die gesetzliche Pflicht zur Erstellung eines Verzeichnisses von Verarbeitungstätigkleiten > VVT. Überprüfen Sie die Angaben in diesem Ordner und passen Sie sie den Umständen Ihrer Praxis ggf. an.	
2	Sie sollten die vorhandene Version Ihres VVT regelmässig dahingehend überprüfen, ob sie DSGVO konform aufgebaut ist und ggf. aktualisieren, damit sie immer dem neuesten Stand in Ihres Betriebes entspricht.	
3	Die Dokumentation der technischen und organisatorischen Maßnahmen ist gesetzl. verpflichtend für jeden Betrieb, der Daten verarbeitet. Überprüfen Sie die Angaben in diesem Ordner und passen Sie sie ggf. an die Umstände in Ihrem Betrieb an.	
4	Überprüfen und aktualisieren Sie die Dokumentation der TOM regelmässig, ob sie DSGVO konform ist und immer dem neuesten Stand in Ihrer Praxis entspricht.	
5	Mit jedem Dritten, der in Ihrem Auftrag Daten verarbeitet oder weiterverarbeitet, muss ein Auftragsverarbeitungsvertrag AVV geschlossen werden. Überprüfen Sie ob Ihnen alle notwendigen AVV vorliegen und schließen Sie ggf. noch fehlende AVV ab.	
7	Für Minderjährige (bis 16 Jahre) müssen Sie die Einwilligung in ddie Datenverarbeitung von den Erziehungsberechtigten /gesetzl. Vertretern einholen.	
8	Achten Sie darauf, ob Ihre vorhandene Patienteninformation DSGVO konform aufgebaut ist und alle verpflichtenden Punkte ausreichend erläutert werden.	
9	Sie müssen Ihre Patienten ausführlich zu dem Widerrufsrecht aufklären, sonst ist die Einwilligung ungültig.	
36	Denken Sie daran die notwendigen Einwilligungen Ihrer Patienten für die Verwendung von Fotos, Ton- und Videoaufnahmen zu therapeutischen/medizinischen Zwecken einzuholen.	
62	Denken Sie daran die notwendigen Einwilligungen Ihrer Mitarbeiter für die Verwendung von Fotos, Videos, Qualifikationen und Einträge von Geburtstagen/Urlaub in Listen einzuholen.	

2. Zutrittskontrolle		erledigt
73	Die Ausgabe von Praxisschlüsseln sollte nur gegen Quittung erfolgen, damit Sie die Kontrolle darüber haben, wer Zugang zu Ihrer Praxis hat.	
80	Wir empfehlen Ihnen eine schriftliche Vereinbarung mit den Mitarbeitern abzuschließen, dass alle Fenster nach Dienstschluß verschlossen und kontrolliert werden.	

3. Zugangskontrolle		erledigt
91	Idealerweise erinnert Sie ein Programm automatisch daran, wenn ein Passwort geändert werden muss. Wählen Sie hierzu bei der Einrichtung einen Zeitraum der nicht länger ist als 6 Monate.	
98b	Holen Sie von Ihrem vertraglich bestimmten Systemadministrator einen AVV ein.	
101h	Sie sollten WPS und Broadcastingfunktionen ausschalten.	

4. Zugriffskontrolle		erledigt
107	Die Vereinbarung mit den Mitarbeitern zur vertraulichen Handhabung aller Gespräche am Empfangsbereich sollte schriftlich fixiert werden.	
108	Alle physischen Dokumente / Unterlagen sind grundsätzlich abschliessbar und sicher zu lagern.	
111	Lassen Sie niemals Patientenakten unbeaufsichtigt und offen und somit für Unbefugte einsehbar herumliegen.	
112	Legen Sie niemals Akten für die nächste Behandlung so bereit, dass Unbefugte Einblick nehmen können. Abgelgete Akten werden nur abgedeckt und nie unbeaufsichtigt bereit gelegt.	

Anmeldebereich, Tresen, Rezeption		erledigt
124	Nutzen Sie geeignete Maßnahmen, um Ihre Patienten und Besucher auf die Einhaltung eines Diskretionsabstands hinzuweisen z.B. Schilder, Fussmatten, Aufkleber o.ä.	
125	Hängen Sie im Eingangs- oder Wartebereich eine Patienteninformation zum Datenschutz gut sichtbar aus.	
125a	Achten Sie darauf den Aushang zur Datenschutzinformation regelmässig auf DSGVO Konformität zu prüfen und ggf. zu aktualisieren.	
127	Wir empfehlen eine schriftliche Vereinbarung mit den Mitarbeitern abzuschließen, in der darüber aufgeklärt wird, dass zukünftig keine vertraulichen Patientengespräche in Hörweite anderer geführt werden.	

Terminkalender		erledigt
133b	Monitore sind so positioniert oder mit Spiegelfolie versehen, dass ein seitlicher Einblick nicht mehr möglich ist.	

In der Praxis gelagerte, patientenbezogene und mehrfach genutzte Utensilien (z.Bsp. Handtücher, persönliche Lagerungshilfen, Ersatzkleidung oder mehrfach nutzbare Therapiegerätaufsätze)	erledigt

Ausfüllen des Anamnese- /Anmeldebogens:		**erledigt**
Löschung und Vernichtung von sensiblen, personenbezogenen Daten		**erledigt**
5. Weitergabekontrolle		**erledigt**
Drucker und Faxgeräte		**erledigt**
Kommunikation per E-Mail		**erledigt**
149	Schützen Sie bei sensiblen, personenbezogenen Daten die Dokumente für den Versand mit einem Passwort oder holen Sie sich vorab die Einwilligung Ihrer Patienten zum unverschlüsselten Versand. Eine Vorlage hierfür finden Sie in Ihrem DSGVO Konzept	
150	Holen Sie sich vorab die Einwilligung Ihrer Patienten zum unverschlüsselten Daten-Versand per E-Mail auch dann, wenn Sie die Daten ncht nur an Ihre Patietnen senden, sondern auch an andere Stellen senden, die an der Behandlung mitbeteiligt sind.	
Abrechnung und Verwaltungssoftware:		**erledigt**
154	Benötigte AVV /AGB für das genutzte Verwaltungsprogramm für die Abrechnung und Verwaltung von GKV Versicherten sollten vorliegen bzw. eingeholt werden.	
157	Benötigte AVV /AGB für das genutzte Verwaltungsprogramm für die Abrechnung und Verwaltung von PKV Versicherten sollten vorliegen bzw. eingeholt werden.	
160	Benötigte AVV /AGB für das genutzte Verwaltungsprogramm für die Abrechnung und Verwaltung von BG Fällen sollten vorliegen bzw. eingeholt werden.	
163	Benötigte AVV /AGB für das genutzte Verwaltungsprogramm zur Abrechnung und Verwaltung von Bar- und Zuzahlungen sollten vorliegen bzw. eingeholt werden.	
166	Benötigte AVV /AGB für das genutzte Verwaltungsprogramm zur Abrechnung und Verwaltung von selbstzahlenden Kunden sollten vorliegen bzw. eingeholt werden.	
Hausbesuche		**erledigt**
171d	Legen Sie schriftlich verbindliche Regeln fest, wie in Ihrer Praxis mit Daten / Unterlagen während Hausbesuchen und Aussenterminen umzugehen ist.	
Home Office / Datenschutz zu Hause		**erledigt**
6. Eingabekontrolle		**erledigt**
7. Verfügbarkeitskontrolle		**erledigt**
184	Erstellen Sie einen Notfallplan, um festzulegen wie im Falle eines Datenverlusts oder Diebstahls vorgegangen werden soll.	

8. Trennungsgebot / Trennungskontrolle		erledigt
189	Weisen Sie Mitarbeiter und Patienten darauf hin, dass in den offenen Kabinen keine vertraulichen Themen besprochen werden, da durch die baulichen Gegebenheiten keine hundertprozentige Diskretion hergestellt werden kann.	

9. Datenschutz - Mitarbeiter		erledigt
190	Schulen und sensibilisieren Sie Ihre Mitarbeiter im Bereich Datenschutz und dokumentieren Sie die Teilnahme an Datenschutzschulungen.	
191	Sie sollten eine schriftliche Einwilligung zur erweiterten Datenverarbeitung von Ihren Mitarbeitern einholen.	
192	Denken Sie daran, dass jährlich Nachschulungen stattzufinden haben, damit alle Mitarbeiter immer auf dem neuesten Stand sind.	
193	Wir empfehlen Ihnen, alle Mitarbeiter schriftlich auf das Datengeheimnis zu verpflichten.	

10. Auskunftsanspruch des Betroffenen	erledigt

11. Verhalten bei Datenschutzverstößen	erledigt

12. Zusätzlicher Fragenteil für AVV & VVT		erledigt
217d	Wenn Sie z.Bsp. ein Verwaltungsprogramm oder einen externen Anbieter für die Organisation / Durchführung von Mahnfällen heranziehen, sollte ein AVV / die AGB vorliegen oder eingeholt werden.	
219d	Wenn Sie z.Bsp. ein Verwaltungsprogramm oder einen externen Anbieter für Ihre Empfangsquittungen nutzen, sollte ein AVV / die AGB vorliegen oder eingeholt werden.	
221c	Für die Büro- und Verwaltungsprogramme, die Sie nutzen sollten die AVV / die AGB vorliegen oder eingeholt werden.	

Bemerkungen und Ergänzungen

Ort / Datum **Unterschrift Inhaber/in**

Technische und organisatorische Maßnahmen (TOM)

Einrichtung	Physiolounge GmbH		
Name Inhaber/in	Iris Düppen		
Name Verantwortlicher (falls abweichend):			
Adresse:	Zentralstraße 1		
	04109 Leipzig		
Telefon	0341-9277200	Fax	
E-Mail	iris.dueppen@physiolounge-leipzig.de		
Homepage	www.physiolounge-leipzig.de		
Stand	19.11.2024	DSB wurde bestellt und gemeldet	nein

Die folgende Aufstellung stellt die Bemühungen zur Einhaltung der Verordnungen und Gesetze zum Datenschutz der o.g. Praxis dar. Nach dem o.g. Datum durchgeführte Änderungen und Verbesserungen wurden noch nicht berücksichtigt.

1. Datenfeststellung - folgende Daten werden verarbeitet

Patientendaten:

Adressdaten wie: Name, Nachname, Straße, Hausnummer, Land, Ort, PLZ
Kontaktdaten wie: Telefon, Mobilnummer
E-Mail Adresse
Versicherungsdaten wie Krankenkasse

Daten zu betreuenden Personen (pflegende Angehörige, Bevollmächtigte, Betreuer etc.)

Name, Nachname, Straße, Hausnummer, Land, Ort, PLZ
Telefon Nr. Mobilnummer
E-Mail Adresse
Vollmachten, Bestellungsurkunde, etc.

Biometrische Daten wie:

Geburtsdatum
Umfänge (Lymphe), Körpermaße, Schuhgröße

Finanzdaten wie:
Rechnungen
Zuzahlungen in bar
Bankverbindung
Abrechnungsdaten
EC Cash für Zuzahlungen oder Selbstzahler
Gesundheitsdaten wie:
Krankheitsdaten
Befunde
Medikamentendaten
Inhaltliche Daten wie:
Termindaten
Kommentare
Texteingaben oder schriftliche Notizen auf Papier
Fotodateien
sonstiges:
Primärer Speicherort Patientendaten:
analogen Patientenakte (z.B. Karteikarte o.ä.)
digitalen Patientenakte
Mitarbeiterdaten:
Adressdaten wie: Name, Nachname, Straße, Hausnummer, Land, Ort, PLZ
Kontaktdaten wie: Telefon, Mobilnummer
Kontaktdaten wie: E-Mail-Adresse
Kontaktdaten von Bewerbern/Praktikanten und die jeweiligen Bewerbungsunterlagen
Versicherungs- und Finanzdaten:
Krankenkasse
Lohn- und Gehaltsdaten
Bankverbindung
Betriebliche Altersvorsorge
Sozialversicherung

Gesundheitsdaten wie:
Krakheitsdaten / Tage etc.
Inhaltliche Daten wie:
Lebenslauf
Qualifikationsdaten und Fortbildungen
Leistungsdaten z.Bsp. Ertragsstatistik
Digitale Zeiterfassung
Reisekostenabrechnung
Urlaubsdaten / Kalender / Planung
Dokumentation Mitarbeitergespräche
Fotodateien
Videodateien
Ton-/Sprachaufnahmen im Rahmen der medizinischen/therapeutischen Tätigkeit.
sonstiges:
Primärer Speicherort Mitarbeiterdaten:
analoge Mitarbeiterakte
digitale Mitarbeiterakte

2. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Hier ist größtenteils der räumliche Zugang zu den Anlagen gemeint.

Es ist nicht möglich die Praxis unbemerkt zu betreten.
Die Praxistüren und Fenster entsprechen mindestens der Sicherheitsstufe RC3. Die Praxis ist mit einer Schließanlage und registrierten Schlüsseln ausgestattet. Eine Schlüsselliste wird geführt. Die Schlüsselliste wird analog geführt.
Die Praxisfenster haben folgende einbruchhemmenden Merkmale: Schließnocken einbruchhemmende Verglasung Es gibt eine mündliche Vereinbarung mit allen Mitarbeitern, dass alle Fenster bei Dienstschluss kontrolliert werden. Private Türen sind mit -Zutritt nur für Personal-, -Privat- o.ä. gekennzeichnet.

3. Zugangskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -Verfahren gehindert werden.

Alle elektronischen Geräte, die persönliche Daten speichern, haben Benutzername, Passwort o.ä. (ideal: 8 Zeichen; Groß-/Kleinbuchstaben, Zahlen, ein Sonderzeichen)

Auf Geräten installierte Datenverarbeitungs-Software ist zusätzlich durch Benutzername und Passwort o.ä. gesichert.

Die Mitarbeiter haben jeweils einen persönlichen Account mit eigenem Passwort (Log-In).

Jedes elektronische Gerät (PC, Laptop, Tablet, etc.) hat eine automatische Inaktivitätssperre, welche den Bildschirm nach 5 Minuten Inaktivität abschaltet.

Bei jeder Aktivierung der Inaktivitätssperre/Bildschirmschoner muss sich der Nutzer erneut mit den Zugangsdaten (Passwort/Benutzerkennung) identifizieren/anmelden.

Alle Geräte und die genutzte Software werden regelmäßig gewartet/aktualisiert.

Es wird eine Firewall und Anti Virus Software benutzt / eingesetzt, die regelmässig auf den neuesten Stand gebracht wird.

Hersteller/Lieferanten für Firewall und Software: Microsoft Defender

Die Aktualisierung erfolgt durch:

Praxismitarbeiter / Inhaber selbst

Erfolgt automatisiert

Beauftragten Systemadministrator / IT Dienstleister

Systemadministrator:

Scheffelmeier Richter GbR, Bitterfelder Straße 4, 04129 Leipzig

Es existiert ein interner Server.

Der Server befindet sich in einem eigenen, abgeschlossenen Raum.

Es existiert ein WLAN-Zugriff.

Folgender Anbieter wird genutzt: FritzBox - AVM Computersysteme Vertriebs GmbH, Alt-Moabit 95, 10559 Berlin

Der Router (Hardware) ist vor fremden Zugriff geschützt.

Die Nutzeroberfläche des Internet-Routers ist mit einem extra Passwort geschützt.

Der Zugriff ist mit einem 12 Stellen langen Passwort (WPA2 Schlüssel) gesichert mit Groß-, Kleinbuchstaben, Zeichen, Zahlen.

Es werden keine privaten Handys zur Patientenkommunikation eingesetzt.

Es werden keine Messenger-Dienste zur Kommunikation mit Patienten/Mitarbeitern genutzt.

4. Zugriffkontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass die bei der Bearbeitung verwendeten personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Alte Patientenakten sind sicher, abschließbar und getrennt von aktuellen Akten gelagert (nach Löschfrist).

Alle Gesundheitsdaten werden auf die Innenseite der Patientenunterlagen geschrieben oder in das Innere der Karteikarte gelegt.

Rezepte können so von Patienten unterschrieben werden, dass Unbeteiligte keinen Einblick erhalten.

Nach Gebrauch von Akten / Unterlagen / Dokumenten werden diese direkt wieder in den jeweiligen Aktenschrank verstaut und eingeschlossen.

Falls Patientenunterlagen abgelegt werden, werden diese sofort mit einem anderen Blatt, einem Klemmbrett, etc. abgedeckt, um diese vor unbefugten Blicken zu schützen.

Wenn die Anmeldung oder der Behandlungsraum nicht besetzt sind, werden alle Unterlagen mit personenbezogenen Daten (z.B. Patientenakten, Karteikarten, Rezepte, Terminkalender, etc.) direkt eingeschlossen und verstaut.

Elektronische Daten werden auf folgenden Geräten verarbeitet und gespeichert:

Tablet

fest installierter PC

Das Gerät ist / Die Geräte sind ausreichend gegen Diebstahl geschützt.

Das Gerät ist / Die Geräte sind wie folgt gesichert:	Verschlossener Raum

Anmeldebereich, Tresen, Rezeption

Alle Besucher werden persönlich empfangen.

Es gibt einen klassischen Anmeldebereich mit Tresen.

Wenn es nicht möglich ist, ein vertrauliches Telefongespräch zu führen, wird ein Rückruf vereinbart.

Wenn vertrauliche Gespräche geführt werden müssen, werden die Fenster im jeweiligen Raum geschlossen.

Der Anrufbeantworter ist auf stumm oder lautlos geschaltet, so dass man nicht mithören kann, was auf das Band gesprochen wird.

Terminkalender

Der Terminkalender wird digital / elektronisch geführt.

Es besteht die schriftliche Anweisung, dass beim Verlassen des Computers/Tablets eine Abmeldung des Nutzers erfolgen muss.

In der Praxis gelagerte, patientenbezogene mehrfach genutzte Untensilien. (z.Bsp. Patientenhandtücher, Laken, persönliche Lagerungshilfen, Ersatzkleidung oder mehrfach nutzbare Therapiegerätaufsätze)

Ein Zugriff durch andere Patienten ist nicht möglich.

Die jeweilig benötigten Utensilien werden vom Personal ausgegeben oder bereit gelegt.

Ausfüllen des Anamnesebogens

Die Besprechung des Anamnesebogens erfolgt in einem geschlossenen Raum, um die Privatsphäre zu sichern.

Patienten erhalten eine Schreibmappe (Schutz), um die Unterlagen im Wartebereich auszufüllen.

Der Anamnesebogen wird gemeinsam von Therapeut und Patient im Gespräch ausgefüllt.

Löschung und Vernichtung von sensiblen, personenbezogenen Daten

Es wird ein Aktenvernichter der Sicherheitsstufe 4 gemäß DIN 66399-2 (Kreuzschnitt; bzw. Partikelschnitt) eingesetzt.

Die Datenvernichtung erfolgt regelmäßig.

Zeitabstände zur Datenvernichtung: Täglich und bei Bedarf

Alle Löschfristen entsprechen den gesetzlichen Anforderungen, sind schriftlich festgelegt und allen Verantwortlichen bekannt gegeben. (z.B. Patientendaten 10 Jahre laut §630 f. BGB bis 30 Jahre §199 Abs.2 BGB).

5. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern, nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Drucker und Faxgeräte

Es wird ein Drucker genutzt.

Es wird ein Faxgerät genutzt.

Faxe werden als E-Mail an den Empfänger weitergeleitet.

Kommunikation per E-Mail

Es wird folgendes E-Mail Programm genutzt:	Microsoft Outlook

Eine E-Mail Kommunikation zu Werbezwecken findet nicht statt.

Abrechnung und Verwaltungssoftware

Wir nehmen die Abrechnung der GK Versicherten selbst vor.

Folgendes Verwaltungsprogramm wird bei der Selbstbearbeitung der GKV Abrechnung eingesetzt: THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg

Wir nehmen die Abrechnung der PK Versicherten selbst vor.

Folgendes Verwaltungsprogramm wird bei der Selbstbearbeitung der PKV Abrechnung eingesetzt: THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg

Wir nehmen die Abrechnung mit der BG selbst vor.	
Folgendes Verwaltungsprogramm wird bei der Selbstbearbeitung der BG Abrechnung eingesetzt:	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg
Wir nehmen die Abrechnung der Bar- und Zuzahlungen selbst vor.	
Folgendes Verwaltungsprogramm wird bei der Selbstbearbeitung der Bar- und Zuzahlungen eingesetzt:	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg
Wir nehmen die Abrechnung der Mitgliedsbeiträge und Selbstzahlerleistungen selbst vor.	
Folgendes Verwaltungsprogramm wird bei der Abrechnung der Selbstzahlerleistungen eingesetzt:	THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg
Wir bieten elektronischen Zahlungsverkehr an.	
Die Praxis rechnet über folgendes Geldinstitut ab:	Hypo Vereinsbank
Wir bieten die Möglichkeit der Kartenzahlung an.	
Die Praxis nutzt dazu folgenden Anbieter:	Sparkasse Leipzig
Wir bieten die Möglichkeit der Nutzung folgender Bezahldienste an:	
Die Praxis nutzt dazu folgenden Bezahldienst:	PayPal (Europe) S.à.r.l. et Cie, S.C.A., 22-24 Boulevard Royal, L-2449 Luxembourg (Gutscheine)

Hausbesuche

Jeder Behandler hat eine eigene, sicher verschließbare Mappe zum Transport von Akten.

Die Umlaufmappe wird in sicheren Transporttaschen zum Zielort befördert. → Persönliche Handtaschen o.ä. sind nicht erlaubt.

Es gibt eine mündliche Vereinbarung bzgl. Regeln zu Hausbesuchen.

Nach Hausbesuchen werden die Unterlagen in die Praxis zurückgebracht.

Nach den Hausbesuchen werden die Unterlagen mit nach Hause genommen und dann dort sicher verschlossen aufbewahrt.

Home Office / Datenschutz zu Hause

Es werden Akten / Unterlagen im Home Office aufbewahrt.	
Die Aufbewahrung der Daten erfolgt sicher verschlossen.	
Der Transport der Daten / analoger Akten erfolgt geschützt und in geeigneter Weise.	
Folgende Hardware wird verwendet:	PC
Die Hardware wird geschützt durch:	Verschlossener Raum

Folgende Software wird verwendet:	Microsoft Windows
Die Software wird geschützt durch:	Passwort geschützt

6. Eingabekontrolle

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

Jede Änderung in einem analogen personenbezogenen Datensatz (z.B. Namensänderung, Änderung des Wohnorts oder der Kontaktdaten, etc.) wird protokolliert / festgehalten, z.Bsp. durch Datum und Namenszeichen.

Aufgrund von personalisierten Benutzerprofilen kann genau ermittelt werden, wer bestimmte Datensätze ändert, erhebt oder löscht. (digital)

7. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Es existiert ein Datensicherungskonzept auch für analoge Akten.

Alle Sicherungen der Daten erfolgen zu festgelegten Intervallen.

Festgelegter Intervall:	Täglich

Die Sicherungen erfolgen elektronisch.

Die Sicherungen erfolgen auf einem netzwerkgebundenen sicheren Datenserver (NAS).

Die zur Sicherung verwendete Hardware wird ausreichend vor Diebstahl geschützt.

An jeder Schlüsselstelle der Praxis ist ein Feuerlöscher angebracht.

In jedem Raum gibt es Feuer- und Rauchmelder.

8. Trennungsgebot / Trennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Die Behandlungszimmer sind voneinander getrennt. → Eigene, geschlossene Räume.

Das Wartezimmer befindet sich in einem separaten, eigens dafür vorgesehenen Raum.

Das Wartezimmer befindet sich in einem offenen Bereich (z.Bsp. Flur). Die Mitarbeiter wurden dazu sensibilisiert.

Die Patienten werden darauf hingewiesen, dass durch die baulichen Umstände keine hundertprozentige Diskretion gewährleistet werden kann.

9. Datenschutz - Mitarbeiter

Maßnahmen, die die datenschutzrechtlichen Anforderungen für die Mitarbeiter umsetzen.

Alle wurden mündlich auf das Datengeheimnis verpflichtet.

10. Auskunftsanspruch des Betroffenen

Nach §34 BDSG gilt der Auskunftsanspruch von Betroffenen gegenüber jeder Stelle, die personenbezogene Daten von ihm gespeichert hat - bei unrichtiger oder unvollständiger Auskunft drohen Bußgelder.

Es gibt ein System zur genauen Identifikation und Auffindung von Patientendaten → z.B. wenn der Patient Auskunft ersucht (Auskunftsrecht nach Artikel 15 DSGVO).

Es wurde schriftlich festgelegt, wer im Fall eines Auskunftersuchens berechtigt ist, Auskünfte zu erteilen.

Auskünfte werden erteilt von: Inhaberin

11. Verhalten bei Datenschutzverstößen

Nach Art.33 – EU-DSGVO meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (nachdem ihm die Verletzung bekannt wurde).

12. Zusätzlicher Fragenteil für AVV & VVT

Es werden Daten betreffend Arbeitsschutzmaßnahmen dokumentiert und gespeichert.

Es werden Daten zu (mit-)behandelnden Ärzten, Therapeuten etc. gespeichert.

Die Angaben werden in der Patientenkartei vermerkt.

Die Angaben werden per Verwaltungssoftware verarbeitet (eGK).

Zum Zeitpunkt des Audits wurden keine Freiberuflichen Mitarbeiter beschäftigt.

AVV Liste

Externe Datenverarbeiter im Auftrag unserer Einrichtung.

Die folgende Liste stellt eine Übersicht unserer externen Datenverarbeiter dar, d.h. die Firmen, Personen oder Gesellschaften, die in unserem Auftrag die Daten unserer Kunden verarbeiten.

Im Rahmen dieser Tätigkeiten haben wir mit allen Firmen oder Personen dieser Liste bereits einen AVV (Auftragsverarbeitungsvertrag) geschlossen oder sind im Begriff einen AVV zu schließen, um die Datensicherheit unserer Patienten und Kunden zu gewährleisten oder der Auftrag zur Datenverarbeitung ist in den jeweiligen Anbieter AGB geregelt.

	AVV / AGB nötig	AVV / AGB liegt vor	AVV / AGB liegt nicht vor
Hypo Vereinsbank	nicht notwendig		
Sparkasse Leipzig	nicht notwendig		
Braune & Tauche Steuerberater-Partnerschaft mbB Inselstraße 31, 04103 Leipzig	nicht notwendig		
THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH, Franckstraße 5, 71636 Ludwigsburg	X		X
Microsoft Office Microsoft Deutschland GmbH Walter-Gropius-Straße 5, 80807 München	X	X	
Scheffelmeier Richter GbR, Bitterfelder Straße 4, 04129 Leipzig	X		X
FritzBox - AVM Computersysteme Vertriebs GmbH, Alt-Moabit 95, 10559 Berlin	X	X	

Verarbeitungstätigkeiten in der Praxis (VVT)	
Betrieb:	Physiolounge GmbH
Inhaber (verantwortliche Person):	Iris Düppen
Stand:	19.11.2024

Die folgende Übersicht stellt die gesammelten Verarbeitung Tätigkeiten der o.g. Praxis gem. Art.30 DSGVO dar. Aus Gründen der besseren Übersicht haben wir die geforderten Angaben in mehrere Listen gesplittet.

Die Auflistung der technischen und organisatorischen Maßnahmen entnehmen Sie bitte der Aufstellung TOM, die dem Dokument beigefügt ist.

Als Löschfristen gelten die gesetzlichen Löschfristen der einzelnen Datensätze, eine Übersicht befindet sich am Ende der allgemeinen Erklärung zu den VVT.

Eine Weitergabe in Drittstaaten findet nicht statt.

Übersichtsliste VVT

Folgende Verarbeitungstätigkeiten werden ausgeführt:	ja	nein
Aufnahme und Verwaltung der Stammdaten der mitbehandelnden, überweisenden Ärzte	X	
Aufnahme und Verwaltung der Stammdaten freiberuflicher Mitarbeiter		X
Aufnahme und Verwaltung der Stammdaten der Mitarbeiter	X	
Lohnabrechnung	X	
Arbeitszeiterfassung	X	
Weiterbildungserfassung	X	
Schlüsselausgabe und Verwaltung der Zugangsmöglichkeiten zu den Einrichtungsräumen	X	
Urlaubsplanung und -verwaltung	X	
Abwesenheits- und Fehlzeiten (Krankmeldungen)	X	
Betriebliche Altersvorsorge	X	
Dienst- und Fuhrparkverwaltung (inkl. Fahrtenbücher)		X
Dokumentation der Mitarbeitergespräche	X	
Verwaltung der Stammdaten von Patienten	X	
Verwaltung der Stammdaten von Betreuern / nächsten Angehörigen	X	
Terminverwaltung	X	
Medizinische Dokumentation (Texteingaben)	X	
Abrechnung mit der Gesetzlichen Krankenversicherung	X	
Abrechnung mit der Privaten Krankenversicherung	X	
Abrechnung mit Patienten der Unfallversicherung (BG)	X	
Abrechnung der Bar- oder Zuzahlung	X	
Abrechnung der selbstzahlenden Kunden	X	
Elektronischer Zahlungsverkehr mit Patienten	X	
Verwaltung der Stammdaten von Bewerbern und /oder Praktikanten	X	
Verwaltung der Stammdaten von Lieferanten und Herstellern von in der Praxis genutzten Produkten und Geräten	X	
Finanzbuchhaltung	X	
Reisekostenabrechnung	X	
Kassenführung Barausgaben bzw. Bareinzahlungen	X	
Auslagenabrechnung	X	
Mahnwesen	X	
Inkassoleistungen		X
Empfangsquittungen	X	
Nutzung von Bürosoftware, (Microsoft Office, Open Office usw.)	X	

E-Mail Kommunikation	**X**	
E-Mail Marketing		**X**
Chat und Messenger Dienste		**X**
Gäste WLAN / Gast-Netzwerkzugang		**X**
Externe Systemadministration	**X**	
Mitgliederverwaltung im Reha Verein		**X**
Trainingsgeräte mit Chipfunktion (z.Bsp. Milon)		**X**
Weitere eingesetzte Software oder Tools		**X**
Führen von Kurslisten		**X**
Datenverarbeitung mit stationären Bürogeräten (z.B. Multifunktionsgeräten, Fax, o.ä.)	**X**	
Versicherungen und sonstige Schadensregulierung im Interesse des Verantwortlichen		**X**
Arbeitsschutzmaßnahmen	**X**	

Datenverarbeitung beteiligte Ärzte

Bezeichnung der Verarbeitungstätigkeit:

Aufnahme und Verwaltung der Stammdaten der mitbehandelnden, überweisenden Ärzte

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufnahme und Verwaltung der Stammdaten von Ärzten

Verwaltungssystem

Zweck der Verarbeitung

Organisation Rückmeldungen an den Arzt; Kommunikation Arztbrief und Änderung Rezeptdaten

Kategorie betroffener Daten

Rezeptdaten, Gesundheitsdaten, Behandlungsdaten

Erlaubnistatbestand

Zusammenarbeit aufgrund Rahmenvertrag, Art. 6 Abs. 1c DSGVO

Kategorie betroffener Personen

Ärzte, die an der Behandlung unserer Patienten beteiligt sind.

Empfänger

Krankenkasse, Abrechnungszentrum, andere Ärzte oder Therapeuten

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Aufnahme und Verwaltung der Stammdaten der Mitarbeiter

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufnahme und Verwaltung der Stammdaten der Mitarbeiter

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte

Zweck der Verarbeitung

Organisation des Beschäftigungsverhältnisses, Erfüllung steuerlicher und sozialversicherungsrechtlicher Pflichten

Kategorie betroffener Daten

Name, Geb. Datum, Adressdaten, Kommunikationsdaten, Kostenträger-Info, Qualifikation, Krankmeldungen, Krankheitstage, Konfession

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Kategorie betroffener Personen

Mitarbeiter

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Lohnabrechnung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufzeichnung der Arbeitszeit, Fehltage etc. zur Lohnabrechnung

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte

Zweck der Verarbeitung

Organisation des Beschäftigungsverhältnisses, Erfüllung steuerlicher und sozialversicherungsrechtlicher Pflichten

Kategorie betroffener Daten

Bankdaten, Sozialversicherungsdaten

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Kategorie betroffener Personen

Mitarbeiter

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Arbeitszeiterfassung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufzeichnung der Arbeitszeit, Fehltage etc. zur Lohnabrechnung

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte
Digitale Zeiterfassung (Stechuhr)

Zweck der Verarbeitung

Organisation des Beschäftigungsverhältnisses, Lohnabrechnung

Kategorie betroffener Daten

Zeiterfassung, Arbeitszeiterfassung

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Weiterbildungserfassung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Erfassung der Teilnahme an Fort- und Weiterbildungen, Aufzeichnung der Arbeitszeit, Fehltage etc. zur Lohnabrechnung

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte

Zweck der Verarbeitung

Organisation des Beschäftigungsverhältnisses, Erfüllung arbeitsrechtlicher Verpflichtungen zur Schulung etc. ,evtl. Lohnanpassung

Kategorie betroffener Daten

Arbeitszeit, Kursbezeichnungen etc., Qualifikation nach Teilnahme

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Schlüsselausgabe und Verwaltung der Zugangsmöglichkeiten zu den Einrichtungsräumen

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Eintrag in einer Schlüsselliste zur Organisation und Sicherung der Praxis.

Verwaltungssystem

analoge Mitarbeiterakte
digitale Mitarbeiterakte
analoge Schlüsselliste

Zweck der Verarbeitung

Organisation der Geschäftsabläufe und Sicherung der Praxisräume.

Kategorie betroffener Daten

Name des Beschäftigten, Schlüsselbezeichnung, Belehrung zum Umgang mit Praxisschlüsseln

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Empfänger

keine

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Urlaubsplanung und -verwaltung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Erfassung von geplanten oder bereits erhaltenen Urlaubstagen

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte
Urlaubskalender

Zweck der Verarbeitung

Organisation des Beschäftigungsverhältnisses

Kategorie betroffener Daten

Name des Beschäftigten, Zeiterfassung

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO, schriftliche Einwilligung des Mitarbeiters bei öffentlich zugänglichem Kalender

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Abwesenheits- und Fehlzeiten (Krankmeldungen)

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufzeichnung der Arbeitszeit, Fehltage etc. zur Lohnabrechnung

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte

Zweck der Verarbeitung

Organisation des Beschäftigungsverhältnisses

Kategorie betroffener Daten

Name des Beschäftigten, Zeiterfassung

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Empfänger

ggf. Krankenkasse im Falle von Lohnfortzahlung

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Betriebliche Altersvorsorge

Gültigkeit

Angelegt am:	19.11.2024
Zuletzt geändert am:	

Beschreibung der Verarbeitung

Aufzeichnung der Arbeitszeit, Dauer der Betriebszugehörigkeit, Buchhaltungsdaten

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte

Zweck der Verarbeitung

Organisation des Beschäftigungsverhältnisses

Kategorie betroffener Daten

Buchhaltungsdaten

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Mitarbeiterdaten

Bezeichnung der Verarbeitungstätigkeit:

Dokumentation der Mitarbeitergespräche

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Dokumentation der Führung von Mitarbeitergesprächen inkl. Planung von Fortbildungen, Weiterbildungen und Zielsetzungen, Lohnerhöhungen

Verwaltungssystem

Analoge Mitarbeiterakte
Digitale Mitarbeiterakte

Zweck der Verarbeitung

Organisation des Geschäftsbetriebes, Organisation des Beschäftigungsverhältnisses

Kategorie betroffener Daten

Name des Mitarbeiters, Leistungsdaten, Planung von Fort- und Weiterbildungen, Zielsetzungen innerhalb der Betriebsstruktur

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Arbeitsvertrag, Art. 6 Abs. 1b DSGVO

Empfänger

keine

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Verwaltung der Stammdaten von Patienten

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufnahme der Stammdaten durch manuelle Eingabe oder Einlesen der eGK

Verwaltungssystem

Analoge Patientenakte/Karteikarte
Digitale Patientenakte

Zweck der Verarbeitung

Organisation der Behandlung oder Dienstleistung, Kommunikation

Kategorie betroffener Daten

Patientendaten

Kategorie betroffener Personen

Patienten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

keine

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Verwaltung der Stammdaten von Betreuern und nächsten Angehörigen bzw. gesetzl. Vertretern

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufnahme der Stammdaten durch manuelle Eingabe und Einwilligungserklärung

Verwaltungssystem

Analoge Patientenakte/Karteikarte
Digitale Patientenakte/Karteikarte

Zweck der Verarbeitung

Organisation der Behandlung oder Dienstleistung, Kommunikation bezüglich der Behandlung des Patienten

Kategorie betroffener Daten

Patientendaten ,Vollmachten, Stammdaten der betreuenden Person (Name, Adresse, E-Mail, Telefonnummer)

Kategorie betroffener Personen

Patienten und deren Betreuer bzw. nächste Angehörige, welche als betreuende Personen angegeben sind.

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO und unterschriebene Einwilligungserklärung

Empfänger

keine

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Terminverwaltung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Eintragung von Name, geplanter Leistung, geplanter Behandler in Kalender

Verwaltungssystem

Digitaler Terminkalender

Zweck der Verarbeitung

Organisation der Behandlung bzw. Therapie, Terminverwaltung

Kategorie betroffener Daten

Name des Patienten, Zeiterfassung der geplanten Leistungsabgabe, Art der geplanten Leistung, geplanter Therapeut

Kategorie betroffener Personen

Patientendaten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

keine

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Medizinische Dokumentation

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Dokumentation auf Karteikarten Dokumentation in der elektronischen Patientenakte

Verwaltungssystem

Analoge Patientenakte/Karteikarte
Digitale Patientenakte

Zweck der Verarbeitung

Organisation der Behandlung - Dokumentation erbrachter Leistungen und deren Ergebnis

Kategorie betroffener Daten

Anamnese, Therapieformen und Reaktion, Dokumente des Patienten, Befund, Behandlungsverlauf

Kategorie betroffener Personen

Patientendaten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

u.U. Rückmeldung an überweisenden Arzt, Therapeuten, gesetzliche Krankenversicherung

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Abrechnung mit der GKV

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Sammelabrechnung: Versand der Daten nach §302 SGB V an Kostenträger

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Zweck der Verarbeitung

Abrechnung erbrachter Leistungen

Kategorie betroffener Daten

Daten des Rezeptes, Buchhaltungsdaten

Kategorie betroffener Personen

Patientendaten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

Kostenträger GKV

Abrechnungszentrum:

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Abrechnung mit der PKV

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Sammelabrechnung: Versand der Daten nach §302 SGB V an Kostenträger

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Zweck der Verarbeitung

Abrechnung erbrachter Leistungen

Kategorie betroffener Daten

Daten des Rezeptes, Buchhaltungsdaten

Kategorie betroffener Personen

Patientendaten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

Kostenträger PKV

Abrechnungszentrum:

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Abrechnung mit Patienten der Unfallversicherung (BG)

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Sammelabrechnung: Versand der Daten nach §302 SGB V an Kostenträger

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Zweck der Verarbeitung

Abrechnung erbrachter Leistungen

Kategorie betroffener Daten

Anamnese, Therapieformen und Reaktion, Dokumente des Patienten, Befund, Behandlungsverlauf

Kategorie betroffener Personen

Patientendaten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

u.U. Rückmeldung an überweisenden Arzt, Therapeuten, gesetzliche Krankenversicherung, BG

Abrechnungszentrum:

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Abrechnung der Bar- oder Zuzahlung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Bareinnahme Kassenbucheintrag

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Zweck der Verarbeitung

Abrechnung erbrachter Leistungen

Kategorie betroffener Daten

ggf. Daten des Rezeptes, Buchhaltungsdaten, Rechnungsdaten

Kategorie betroffener Personen

Patientendaten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

Barzahler, Buchhaltung

Abrechnungszentrum:

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Abrechnung der Leistungen für selbstzahlende Kunden

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Abrechnung von erbrachten Leistung für selbstzahlende Kunden außerhalb von Verordnungen oder Rezept (gemeint sind hier z. Bsp. Wellnessmassagen, Geschenkgutscheine, Kursteilnahmen o.ä. Angebote)

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Zweck der Verarbeitung

Abrechnung erbrachter Leistungen

Kategorie betroffener Daten

ggf. Daten zur erbrachten Leistung, Rechnungsdaten

Kategorie betroffener Personen

ggf. Kundendaten

Erlaubnistatbestand

Vertrag Art. 6 Abs 1b DSGVO

Empfänger

Selbstzahler, Buchhaltung

Datenverarbeitung Patientendaten

Bezeichnung der Verarbeitungstätigkeit:

Elektronischer Zahlungsverkehr mit Patienten

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Rechnungsstellung, Eintrag Offene Posten Liste

Verwaltungssystem

Hypo Vereinsbank

Sparkasse Leipzig

PayPal (Europe) S.à.r.l. et Cie, S.C.A.,
22-24 Boulevard Royal, L-2449 Luxembourg (Gutscheine)

Zweck der Verarbeitung

Abrechnung erbrachter Leistungen

Kategorie betroffener Daten

Rechnungsdaten, Kostenstelle

Kategorie betroffener Personen

Selbstzahler, Privatpatienten

Erlaubnistatbestand

Behandlungsvertrag Art. 6 Abs 1b DSGVO

Empfänger

beteiligtes Geldinstitut, Selbstzahler

Datenverarbeitung Bewerberdaten

Bezeichnung der Verarbeitungstätigkeit:

Verwaltung der Stammdaten von Bewerbern und /oder Praktikanten

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufnahme der Stammdaten von Bewerbern und Praktikanten

Verwaltungssystem

Analoge Personalakte

Zweck der Verarbeitung

Aufnahme der Stammdaten von Bewerbern und Praktikanten zur Durchführung eines Auswahlverfahrens mit dem Ziel der Gewinnung neuer Mitarbeiter

Kategorie betroffener Daten

Name, Adressdaten Kommunikationsdaten, Lebenslauf mit Bild, Bewerbungsschreiben, ggf. Zeugnisse und Qualifikationen

Kategorie betroffener Personen

Bewerber um freie Stelle oder Praktikumsplatz

Erlaubnistatbestand

Vorvertragliches Vertragsverhältnis, Art. 6 Abs. 1 b DSGVO

Empfänger

keine

Datenverarbeitung Lieferanten-/Herstellerdaten

Bezeichnung der Verarbeitungstätigkeit:

Verwaltung der Stammdaten von Lieferanten und Herstellern von in der Praxis genutzten Produkten und Geräten

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Aufnahme der Stammdaten von Lieferanten und Herstellern von in der Praxis genutzten Produkten und Geräten

Verwaltungssystem

Kataloge und analoge Lieferantenakte, Visitenkarten

Zweck der Verarbeitung

Praxisorganisation, Beschaffung, Dienstleistungs- oder Kaufvertrag oder deren Anbahnung

Kategorie betroffener Daten

Name, Adressdaten Kommunikationsdaten

Kategorie betroffener Personen

Lieferant, Hersteller oder Vertrieb

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

keine

Datenverarbeitung Buchhaltungsdaten

Bezeichnung der Verarbeitungstätigkeit:

Finanzbuchhaltung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Einnahmen- Kostenaufstellung

Verwaltungssystem

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Zweck der Verarbeitung

Praxisorganisation, Buchhaltung und Finanzverwaltung

Kategorie betroffener Daten

Geschäftsführung, Einnahmen und Ausgaben der Praxis

Kategorie betroffener Personen

/

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Buchhaltungsdaten

Bezeichnung der Verarbeitungstätigkeit:

Reisekostenabrechnung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Einnahmen- Kostenaufstellung

Verwaltungssystem

Kassenbuch

Zweck der Verarbeitung

Praxisorganisation, Buchhaltung und Finanzverwaltung

Kategorie betroffener Daten

Geschäftsführung, Einnahmen und Ausgaben der Praxis

Kategorie betroffener Personen

/

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Buchhaltungsdaten

Bezeichnung der Verarbeitungstätigkeit:

Kassenführung Barausgaben bzw. Bareinzahlungen

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Einnahmen- Kostenaufstellung

Verwaltungssystem

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Zweck der Verarbeitung

Praxisorganisation, Buchhaltung und Finanzverwaltung

Kategorie betroffener Daten

Geschäftsführung, Einnahmen und Ausgaben der Praxis

Kategorie betroffener Personen

/

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Buchhaltungsdaten

Bezeichnung der Verarbeitungstätigkeit:

Auslagenabrechnung

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Einnahmen- Kostenaufstellung

Verwaltungssystem

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Zweck der Verarbeitung

Praxisorganisation, Buchhaltung und Finanzverwaltung

Kategorie betroffener Daten

Geschäftsführung, Einnahmen und Ausgaben der Praxis

Kategorie betroffener Personen

/

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

Braune & Tauche Steuerberater-Partnerschaft mbB
Inselstraße 31, 04103 Leipzig

Datenverarbeitung Buchhaltungsdaten

Bezeichnung der Verarbeitungstätigkeit:

Mahnwesen

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Zahlungsversäumnisse verfolgen

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Zweck der Verarbeitung

Praxisorganisation, Buchhaltung und Finanzverwaltung

Kategorie betroffener Daten

Geschäftsführung, Einnahmen und Ausgaben der Praxis

Kategorie betroffener Personen

/

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Datenverarbeitung Buchhaltungsdaten

Bezeichnung der Verarbeitungstätigkeit:

Empfangsquittungen

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Einnahmen- Kostenaufstellung

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Zweck der Verarbeitung

Praxisorganisation, Buchhaltung und Finanzverwaltung

Kategorie betroffener Daten

Geschäftsführung, Einnahmen und Ausgaben der Praxis

Kategorie betroffener Personen

/

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

Zahler

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Datenverarbeitung in IT-Bereich

Bezeichnung der Verarbeitungstätigkeit:

Nutzung von Bürosoftware, (Microsoft Office, Open Office usw.)

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Daten Erfassung, Speicherung und Sicherung

Verwaltungssystem

THEORG – SOVDWAER Gesellschaft für EDV-Lösungen mbH,
Franckstraße 5, 71636 Ludwigsburg

Microsoft Office
Microsoft Deutschland GmbH
Walter-Gropius-Straße 5, 80807 München

Zweck der Verarbeitung

Praxisorganisation und Verwaltung

Kategorie betroffener Daten

Geschäftsführungs- und Organisationsdaten (Mitarbeiterführung, Praxiskommunikation, etc.)

Kategorie betroffener Personen

Geschäftsführung, Patienten, Mitarbeiter, Lieferanten, Bewerber

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

keine

Datenverarbeitung in IT-Bereich

Bezeichnung der Verarbeitungstätigkeit:

E-Mail Kommunikation

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Anschreiben, Erinnerungsservice, Behandlungsberichte, Praxisorganisation

E-Mail Programm

Microsoft Outlook

Zweck der Verarbeitung

Kontakterhalt und Praxisorganisation

Kategorie betroffener Daten

Name, Adressdaten, Kommunikationsdaten, Gesundheitsdaten

Kategorie betroffener Personen

Patienten, Lieferanten, andere an der Behandlung beteiligte Behandler

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

E-Mail Empfänger

Datenverarbeitung in IT-Bereich

Bezeichnung der Verarbeitungstätigkeit:

Systemadministration

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Überwachung und Kontrolle der verwendeten Systeme

Zweck der Verarbeitung

Überprüfung der Einhaltung von Datenschutzvorgaben

Kategorie betroffener Daten

Alle Daten der Praxis

Kategorie betroffener Personen

Mitarbeiter, Patienten, Lieferanten, Bewerber

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO, Einwilligungserklärung

Empfänger

Systemadministrator / Inhaber

Scheffelmeier Richter GbR,
Bitterfelder Straße 4,
04129 Leipzig

Datenverarbeitung im Sekretariat/Büro

Bezeichnung der Verarbeitungstätigkeit:

Datenverarbeitung mit stationären Bürogeräten (z.B. Multifunktionsgeräten)

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Praxisführung und Organisation

Verwaltungssystem

analoge Listen und Datenblätter bzw. digitale Listen

verwendete Geräte

Drucker

Zweck der Verarbeitung

Praxisorganisation und -führung

Kategorie betroffener Daten

Name, Teilnahmebestätigung, Kontodaten

Kategorie betroffener Personen

Patienten, Lieferanten, Bewerber, Vereinsmitglieder, Mitarbeiter

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

keine

Datenverarbeitung im Sekretariat/Büro

Bezeichnung der Verarbeitungstätigkeit:

Arbeitsschutz

Gültigkeit

Angelegt am: 19.11.2024

Zuletzt geändert am:

Beschreibung der Verarbeitung

Dokumentation der getroffenen Maßnahmen

Verwaltungssystem

Analoge Listen und Datenblätter bzw. digitale Listen

Zweck der Verarbeitung

Praxisorganisation und -führung

Kategorie betroffener Daten

Name, ausgehändigte Ausrüstungsgegenstände, Arbeitsanweisungen

Kategorie betroffener Personen

Mitarbeiter

Erlaubnistatbestand

Wahrung berechtigter Interessen der Praxis, Art. 6 Abs. 1 f DSGVO

Empfänger

keine

Durchgeführte Maßnahmen im Bereich des Datenschutzes

Praxis:	Physiolounge GmbH

Hier werden die durchgeführten Änderungen, die wir nach dem Audit vornehmen oder bereits vorgenommen haben von uns dokumentiert, um den Maßnahmenverlauf und die stetige Weiterentwicklung in unserem Unternehmen lückenlos darzustellen.

Gegenstand der Dokumentation sind die durchgeführte Änderung / Maßnahme und der Zeitraum der Umsetzung.

Nr.	Beschreibung der Änderung / Maßnahme	Datum