**Musterverzeichnis von Verarbeitungstätigkeiten**

**15**

Rechtliche Grundlage: Artikel 30 Absatz 1 Datenschutz -Grundverordnung (DSGVO)

Bitte berücksichtigen Sie, dass für jede identifizierte Verarbeitungstätigkeit je ein Verzeichnis zu

führen ist! Das Muster beinhaltet mögliche Tätigkeiten, die individuell einzufügen sind.

**Angaben zum Verantwortlichen**

Name:

Anschrift:

Telefon:

E-Mail:

Internet -Adresse:

**Angaben zur Person des Datenschutzbeauftragten (sofern gem. Art. 37 DSGVO benannt)**

Vorname und Name:

Anschrift:

Telefon:

E-Mail:

**Verarbeitungstätigkeit**

Datum der Anlegung:

Datum der letzten Änderung:

Bezeichnung der Verarbeitungstätigkeit: **Allgemeine Bezeichnung der dokumentierten Verarbeitungstätigkeit, z. B.:**

\* "Dokumentation der Behandlung"

\* "E -Mail -Verarbeitung"

\* "Lohn- und Gehaltsabrechnung"

Zweckbestimmung: **z.B.:**

\* Verarbeitungstätigkeit: "Dokumentation der Behandlung" -> Zweckbestimmung: sachgerechte therapeutische Behandlung und Weiterbehandlung; Erfüllung gesetzlicher Pflichten

\* Verarbeitungstätigkeit: "E-Mailverarbeitung" -> Zweckbestimmung: Durchführung der elektronischen Kommunikation

\* Verarbeitungstätigkeit: "Lohn- und Gehaltsabrechnung" -> Zweckbestimmung: Erstellung der Lohnabrechnung; Erfüllung

gesetzlicher Pflichten

Es können auch mehrere Zweckbestimmungen für eine Verarbeitung

angegeben werden.

Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO **z.B.:**

\* Verarbeitung besonderer Kategorien personenbezogener Daten, Gesundheitsdaten auf der Grundlage eines Behandlungsvertrages (Art. 9

Abs. 2 lit. h DSGVO)

\* Einwilligung (Art. 6 Abs. 1 lit. A, Art. 7 DSGVO)

\* Wahrung berechtigter Interessen des Verantwortlichen oder des Dritten (Art. 6 Abs. 1 lit. f DSGVO)

**Erhebung der Daten**

Betroffene Personengruppen **z.B.:** Patienten, Mitarbeiter, Bewerber

Beschreibung der Datenkategorien /

Art der gespeicherten Daten **z.B.:**

\* Name / Vorname / Anrede / Titel, Geburtsdatum, Adressdaten

\* Gesundheitsdaten (besondere Kategorien personenbezogener Daten)

\* Lohn- und Gehaltsdaten

\* Zeiterfassungsdaten

\* Sozialversicherungsdaten

\* Vertragsdaten

**Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können**

Interne Empfänger **z.B.:**

(innerhalb der Einrichtung des

Verantwortlichen) Praxispersonal, Personalabteilung, Buchhaltung, Auftragsverarbeiter

Externe Empfänger und Dritte,

soweit nicht Auftragsverarbeiter **z.B.:** externe andere Arzte / Psychotherapeuten,Kassenärztliche Vereinigungen, Krankenkassen, derMedizinische Dienst der Krankenversicherung,Ärztekammern, privatärztliche Verrechnungsstellen

**Datenübermittlung in Drittstaaten / internationale Organisationen (z. B. Cloud-Dienste)**

Datenübermittlung in Drittstaaten Sofern eine Datenübermittlung in Drittstaaten erfolgt, ist vorab zu klären, ob Datenüermittlungen in ein Drittland oder an eine internationale Organisation stattfinden. Die Übermittlung von personenbezogenen Daten in Drittländer ist ausschließlich zulässig, wenn neben der Rechtmäßigkeit der Datenverarbeitung weiterführend das durch die DSGVO gewährleistete

Schutzniveau in dem jeweiligen Drittland nicht untergraben wird. (ggf. Auskunft von der Aufsichtsbehörde einholen)

**Fristen für die Löschung der verschiedenen Datenkategorien**

Daten sind zu löschen, wenn sie nicht

mehr benötigt werden; dabei sind ggf.

Aufbewahrungsfristen zu beachten **z. B.:** §630 lit. f Abs. 3 BGB(Behandlungsdokumentation)§ 28 Abs. 3 RöV

**Beurteilung der Angemessenheit technischer und organisatorischer Maßnahmen (TOM)**

Allgemeine Maßnahmen müssen unter anderem Folgendes einschließen:

Beschreibung der technischen \* die Pseudonymisierung und Verschlüsselung personenbezogener

und organisatorischen Daten;

Maßnahmen (Art. 32 Abs. 1 DSGVO) \* die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und

Und des etwaigen verbleibenden Belastbarkeit der Systeme und Dienste im Zusammenhang

Risikos unter Berücksichtigung mit der Verarbeitung auf Dauer sicherstellen;

der eingesetzten technisch \* die Fähigkeit, die Verfügbarkeit der personenbezogenen

organisatorischen Maßnahmen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

\* ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

der Wirksamkeit der technischen und organisatorischen Maßnahmen zur

Gewährleistung der Sicherheit der Verarbeitung.

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zweck der Datenverarbeitungen sowie der

unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche geeignete TOM, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO).

**Prüfung durch den Verantwortlichen**

Prüfung erfolgt / nicht erfolgt

Datum, Unterschrift (Verantwortlicher)