Verarbeitungsverzeichnis gemäß Art. 30 DSGVO

# VerantwortlicheR

*Im Praxissetting ist davon auszugehen, dass immer der / die einzelne PsychotherapeutIn VerantwortlicheR im Sinne der DSGVO ist.*

Nachname, Vorname:

Postanschrift:

Telefonnummer:

Emailadresse:

# Datenverarbeitungen

*Im folgenden sind alle digitalen und analogen Datenverarbeitungen, die durch den / die PsychotherapeutIn durchgeführt werden anzuführen. Die angeführten Inhalte sind daher beispielsweise zu verstehen und müssen immer an die eigenen Gegebenheiten angepasst werden. Im Sinne der Datenminimierung dürfen nur Daten erhoben werden, die unbedingt notwendig sind. Daten dürften nicht länger aufbewahrt werden, als unbedingt nötig – das Psychotherapiegesetz gibt hier aktuell einen Rahmen von mindestens (und damit im Sinne der DSGVO auch maximal) 10 Jahren vor. Die Datenverarbeitungen sind nach Verarbeitungszweck zu ordnen.*

**Anmerkungen: Rechtsgrundlage nach PhtG**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Verarbeitungszweck | Betroffene Personengruppe | Kategorie der personenbezogenen Daten | Besondere Datenkategorien iSd Art 9 DSGVO (sensible Daten) | Empfänger | Übermittlung in Drittland | Lösch- und Aufbewahrungsfrist |
| Dokumentation gemäß PthG, | KlientInnen | Stammdaten (Name, Adresse, Geburtsdatum, Telefonnummer), Gesundheits Daten (Diagnose, Krankheitsverlauf, behandelnde ÄrztInnen) | Ja | KlientInnen, gesetzliche VertreterInnen | Nein | 10 Jahre nach Beendigung der Psychotherapie |
| Abrechnung Netzwerk Psychotherapie Steiermark | KlientInnen | Stammdaten, Diagnose, SV-Nummer | Ja | Netzwerk Psychotherapie Steiermark | Nein | Keine Aufbewahrung |
| Kommunikation mittels Mobiltelefon (Telefon, SMS) | KlientInnen | Name, Telefonnummer | Nein | Entfällt | Nein | Periodisches Löschen der SMS alle 6 Monate |
| Abrechnung und Buchhaltung | KlientInnen | Name, Adresse | Nein | Entfällt | Nein | 7 Jahre |

# Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

*Um Vertraulichkeit, Integrität und Verfügbarkeit bzw. Belastbarkeit der Daten sicherzustellen sind entsprechende technische und organisatorische Maßnahmen zu treffen und unter diesem Punkt anzuführen. Die Folgenden Maßnahmen sind als Vorschläge zu verstehen und müssen an die eigenen Gegebenheiten angepasst werden. Die DSGVO verlangt ein geeignetes Schutzniveau, gibt jedoch keine genaueren Spezifikationen diesbezüglich vor. Voraussichtlich werden erst die Erfahrungen der nächsten Jahre zeigen, was unter einem geeigneten Schutzniveau zu verstehen ist.*

*Etwa auch:*

1. *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
2. *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
3. *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
4. *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

* Datenverschlüsselung auf Laptop mittels Software
* Zugangscode am Mobiltelefon, Mobiltelefon verschlüsselt
* Handschriftliche Akten unter Verschluss in der Praxis, ausschließlich durch mich als Verantwortlicher zugänglich
* Laufendes verschlüsseltes Backup aller relevanten Daten
* Hier eventuelle weitere technische und organisatorische Maßnahmen anführen