Stand des Dokuments: 22.06.2018

|  |
| --- |
| Dies ist die Vorlage zum Ausfüllen in LibreOffice oder MS Word |
| **Die Anleitung dazu finden Sie als PDF unter** [www.dataprivacydoctors.at/vorlagen/](http://www.dataprivacydoctors.at/vorlagen/) |

Datenschutz-Konzept-Psychotherapeut/in
gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

Logo/Schriftzug

*Titel / Vor-und Zuname
Verantwortliche gemäß DSGVO
Straße
PLZ-Ort
Email: …………...@…………………….
Tel.:*

Wenn fertig, bitte das Inhaltsverzeichnis neu erstellen

Inhaltsverzeichnis

[1 Allgemeine Angaben 4](#__RefHeading___Toc31831_1491107819)

[1.1 Datenschutz-Konzept 4](#__RefHeading___Toc31833_1491107819)

[1.2 Sachliche und räumliche Tätigkeit 4](#__RefHeading___Toc31835_1491107819)

[1.3 Datenschutzbeauftragter (DSB) 4](#__RefHeading___Toc31837_1491107819)

[1.4 Verantwortliche (Stammdaten) 4](#__RefHeading___Toc31839_1491107819)

[2 Verarbeitungs-Verzeichnisse 5](#__RefHeading___Toc31841_1491107819)

[2.1 Wurde eine Datenschutz-Folgenabschätzung durchgeführt? 5](#__RefHeading___Toc31843_1491107819)

[2.2 Rechnungswesen und Geschäftsabwicklung 6](#__RefHeading___Toc31845_1491107819)

 [9](#__RefHeading___Toc31847_1491107819)

[2.3 Klientenverwaltung und Dokumentation 9](#__RefHeading___Toc31849_1491107819)

[3 Daten-/Auftragsverarbeitungsverträge 16](#__RefHeading___Toc31851_1491107819)

[4 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs) 16](#__RefHeading___Toc31853_1491107819)

[4.1 Impressum und Datenschutzerklärung 16](#__RefHeading___Toc31855_1491107819)

[4.2 Grundsätzlich 16](#__RefHeading___Toc31857_1491107819)

[4.3 Kontaktaufnahme 16](#__RefHeading___Toc31859_1491107819)

[4.4 Erstgespräch 17](#__RefHeading___Toc31861_1491107819)

[4.5 Zutrittskontrolle 17](#__RefHeading___Toc31863_1491107819)

[4.6 Zugangskontrolle 18](#__RefHeading___Toc31865_1491107819)

[4.7 Zugriffskontrolle 18](#__RefHeading___Toc31867_1491107819)

[4.8 Weitergabekontrolle 19](#__RefHeading___Toc31869_1491107819)

[4.9 Eingabekontrolle 19](#__RefHeading___Toc31871_1491107819)

[4.10 Auftragskontrolle 20](#__RefHeading___Toc31873_1491107819)

[4.11 Verfügbarkeitskontrolle 20](#__RefHeading___Toc31875_1491107819)

[4.12 Trennungsgebot 21](#__RefHeading___Toc31877_1491107819)

[4.13 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 21](#__RefHeading___Toc31879_1491107819)

[5 Betroffenenrechte wahren 22](#__RefHeading___Toc31881_1491107819)

[5.1 Prozesse betreffs Betroffenenrechte 22](#__RefHeading___Toc31883_1491107819)

[5.2 Meldung von Datenschutzverletzungen 24](#__RefHeading___Toc31885_1491107819)

[6 Risikoanalyse 25](#__RefHeading___Toc31887_1491107819)

[6.1 Risikoanalyse ohne Maßnahmen 25](#__RefHeading___Toc31889_1491107819)

[6.2 Risiko-Matrix mit Maßnahmen 27](#__RefHeading___Toc31891_1491107819)

[7 Zusammenfassung 27](#__RefHeading___Toc31893_1491107819)

[8 Anhang 29](#__RefHeading___Toc31895_1491107819)

[8.1 Informationsblatt über sensible Daten (Art 9 + 13 DSGVO) 29](#__RefHeading___Toc31897_1491107819)

[8.2 Muster Datenschutzverletzung (WKO) an Behörde bzw Betroffene 33](#__RefHeading___Toc31899_1491107819)

[8.3 Mustervertrag Auftragsverarbeitung (WKO) 35](#__RefHeading___Toc31901_1491107819)

[8.4 Vorlage: Fernwartung und Pflege von IT-Systemen & Datenschutz 37](#__RefHeading___Toc31903_1491107819)

[8.5 Zusatz Verzeichnis: Kundenbetreuung und Kommunikation 38](#__RefHeading___Toc31905_1491107819)

[8.6 Muster: Einwilligungserklärung für Newsletter 43](#__RefHeading___Toc31907_1491107819)

[8.7 Muster: Auskunftserteilung 44](#__RefHeading___Toc31909_1491107819)

[8.8 Muster: Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO) 45](#__RefHeading___Toc31911_1491107819)

**DISCLAIMER**
Sämtliche zur Verfügung gestellten Inhalte wurden mit der größtmöglichen Sorgfalt erstellt. Die Autoren, Christopher Temt und Michael Werzowa, übernehmen jedoch keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der bereitgestellten Informationen (einschließlich des Verweises auf externe Quellen). Die korrekte Datenschutzdokumentation und die TOMs erfordert stets eine konkrete Prüfung im Einzelfall, und meist auch Änderungen in den eigenen Prozessen, weshalb die Beiziehung eines Datenschutzberaters (z.B. [https://www.dataprivacydoctors.at/](https://www.dataprivacydoctors.at/vorlagen/%22%20%5Cl%20%22Newsletter)) sowie eines Rechtsanwaltes, insbesondere bei der Erstellung oder Überprüfung von Verträgen, dringend empfohlen wird. Die zur Verfügung gestellten Inhalte stellen keine Beratungsleistung welcher Art auch immer dar und können eine Beratung auch nicht ersetzen.

Haftungsansprüche gegen den Christopher Temt, und/oder Michael Werzowa welche sich auf Schäden materieller oder ideeller Art, einschließlich entgangenen Gewinn oder sonstige direkte oder indirekte Folgeschäden, beziehen, die durch die Nutzung oder Nichtnutzung der zur Verfügung gestellten Informationen verursacht wurden, sind ausgeschlossen. Die Autoren behalten es sich ausdrücklich vor, Teile der zur Verfügung gestellten Information oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

In Gelb markiert, was Sie entsprechend der konkreten Situation
in Ihrer Einzelpraxis bearbeiten bzw. ändern sollten

# Allgemeine Angaben

## Datenschutz-Konzept

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSGVO geforderte Einhaltung der Verordnungskonformität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte ( Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1 ).

## Sachliche und räumliche Tätigkeit

Ich führe eine therapeutische Einzelpraxis und verarbeite daher als Einzelpersonen-unternehmen (EPU) personenbezogene Daten von natürlichen Personen auch unter 14 Lebensjahren (Kinder gemäß Art 8 DSGVO) ganz oder teilweise automatisiert und habe meine Niederlassung in der EU, in Adresse, Österreich.

Referenzen: Art 2 + 3 + 4 DSGVO, EuGH Entscheidung Weltimmo v. NAIH (C-230/34)

## Datenschutzbeauftragter (DSB)

Trifft einer der nachfolgenden Kriterien zu, ist ein externer oder interner DSB notwendig und zu bestellen:

|  |  |  |
| --- | --- | --- |
| **Kriterium** | **Ja** | **Nein** |
| Verarbeitung der Daten durch eine Behörde oder eine öffentliche Stelle, mit Ausnahme der Gerichte |  | **X** |
| Verarbeitung der personenbezogenen Daten stellt eine Kerntätigkeit der Organisation dar und/oder erfordert eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person |  | **X** |
| Verarbeitung besonders schutzwürdige Kategorien personenbezogenen Daten (Art 9 Z 1 DSGVO wie z.B. Gesundheitsdaten, ethische Herkunft, genetische bzw. biometrische Daten, Gewerkschaftszugehörigkeit, usw.) stellt eine Kerntätigkeit der Organisation dar |  | **X** |

 Referenzen: Art 37 DSGVO, Erwägungsgründe 97

Da für mein EPU keiner der obigen Kriterien zutrifft und die Verarbeitung von Art 9 Daten weder umfangreich noch eine Kerntätigkeit ist, wird kein DSB bestellt.

## Verantwortliche (Stammdaten)

*Titel / Vor-und Zuname
Straße
PLZ-Ort
Email: …………...@…………………….
Tel.:*

Referenzen: Art 4 Z 7 DSGVO

Schulung im Bereich Datenschutz und Datensicherheit

Ich habe an folgende Schulungen bzw. Seminaren betreffs der DSGVO teilgenommen:

|  |  |  |  |
| --- | --- | --- | --- |
| **Bezeichnung der Veranstaltung** | **Veranstalter** | **Datum** | **Nachweis/ZertifikatAnhang Nr.:** |
| Die EU-DSGVO für PsychotherapeutInnen - Einführung |  |  | Teilnahmebestätigung |

Referenzen: Art 4, 5-11 DSGVO

### Weiterbildung und Stand der Technik

Betreffs Weiterbildung und Stand der Technik setze ich folgende Aktivität:

|  |  |  |
| --- | --- | --- |
| **Aktivitäten** | **Veranstalter** | **sonstiges** |
| Info- u. Weiterbildungsveran­staltungen |  |  |
| Homepages bzw. Newsletter |  |  |
|  | [https://www.dataprivacydoctors.at/vorlagen#NewsletterAnmeldung](https://www.dataprivacydoctors.at/vorlagen/%22%20%5Cl%20%22NewsletterAnmeldung)  | Newsletter |
| Beratung Datenschutzexperte |  |  |
| WKO: <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html>  |

Referenzen: Art 4, 5-11 DSGVO

# Verarbeitungs-Verzeichnisse

Referenzen: Art 30, Art 31 DSGVO, Erwägungsgründe 13, 75, 76, 82, 89

## Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

**Ja  Nein X**

**Wenn Ja, wann?**

**Wenn Nein, aus welchem Grund nicht?**

Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, da sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht – siehe Risikobewertung und Maßnahmen, da keine automatisierte systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und da ebenso keine umfangreichen[[1]](#footnote-2) [Verarbeitung](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Grundsaetze-und-Rechtmaes.html) [sensibler Daten](https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung%3A-Wichtige-Begriffsbestimmu.html%22%20%5Cl%20%22sensibl) oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt.

Referenzen: Art 35 Z1-3 DSGVO + Erwägungen 91

Darüber hinaus hat die Datenschutzbehörde in Ihrer Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018 festgehalten, dass alle meine Verarbeitungen Standard- und Muster-Verarbeitungen sind und somit keine Folgeabschätzungen notwendig sind.

Referenzen: Art 35

## Rechnungswesen und Geschäftsabwicklung

### Verantwortliche

 Titel / Vor-und Zuname
 Straße
 PLZ-Ort
 Email: …………...@…………………….
 Tel.:

### Zweck

Verarbeitung und Übermittlung von **pB Daten der Betroffenen**, im Rahmen von Geschäfts­beziehungen mit Klienten/Kunden und Lieferanten, sowie an der Geschäftsabwicklung bzw. Beratung/Behandlung mitwirkende Dritte und Geschäftspartner sowie Honorar-Abrechnungs-Vereine; alle inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten, aber ausdrücklich keine Diagnosen (nach ICD-10) und sensible Informationen iSd Art. 8 + 9 + 10 DSGVO

### Kategorien der betroffenen Personen

|  |  |
| --- | --- |
| **Lfd.Nr.** | **Beschreibung der Kategorien betroffener Personen** |
| 1 | KlientInnen/PatientInnen bzw. deren Rechtsvertretern, Lieferanten sowie Auszubildende |
| 2 | Beratung/Behandlung mitwirkende Dritte inkl. deren jeweiligen Kontaktpersonen |

### Rechtsgrundlagen (in geltender Fassung)

* Art 6 Z 1 lit b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen) DSGVO
* § 132 BAO, §§ 190,2s12 UGB, sowie EStG und UStG
* Psychotherapiegesetz BGBl.Nr. 361/1990 ST0151
* (Berufskodex für Psychotherapeutinnen und Psychotherapeuten )
* Gesamtvertrag abgeschlossen zwischen der beruflichen Interessenvertretung des Auftraggebers und dem Hauptverband der österreichischen Sozialversicherungsträger gemäß § 349 Abs. 2 und Abs. 3 ASVG

### Verträge, Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen zu aufrechten Geschäfts-/Behandlungsabwicklungen, Rechnungen, erledigte Geschäftsfälle/Behandlungen, Unterlagen und Zustimmungserklärungen sowie Verträge mit Auftragsverarbeitern sind im Archiv abgelegt.

### Kategorien der verarbeiteten Daten

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kategorien der betroffenen Personengruppe** | **Lfd.Nr.** | **Datenkategorien** | **Besondere Daten iSd Art 9 10 DSGVO** | Empfängerkategorie |
| 1. KlientInnen/PatientInnen bzw. deren Rechtsvertretern, Lieferanten sowie Auszubildende | 1 | Ordnungs/Klientennummer | *Nein* | 2-5,6,8 |
| 2 | Name, Firma oder sonstige Geschäftsbezeichnung | *Nein* | 1-8 |
| 4 | Anschrift bzw. Lieferadresse | *Nein* | 1-8 |
| 5 | Kontaktdaten (Tel., Handy, Email, Fax, signal.org) | *Nein* | 1-8 |
| 6 | Termine | *Nein* | 2,4-5, 7, 8 |
| 7 | IP Adresse (Homepage) | *Nein* | 2,4 |
| 9 | Firmenbuchdaten | *Nein* | 2-8 |
| 10 | Bankverbindungen | *Nein* | 1-8 |
| 11 | Kreditkartennummern und unternehmen | *Nein* | 1-4 |
| 12 | Kenn-Nummern für Zwecke amtlicher Statistik wie UID-, Intrastat-Kenn-, SteuerNummer | *Nein* | 2-8 |
| 13 | Namen Kontaktpersonen/Erziehungsberechtigten | *Nein* | 2-8 |
| 14 | Kontaktdaten der Kontaktpersonen/Erziehungsberechtigten (Tel., Mail, Fax, Anschrift odgl.) | *Nein* | 2-8 |
| 15 | Funktion/Rolle der Kontaktperson bzw. Erziehungsberechtigten | *Nein* | 2, 4-7 |
| 16 | Art und Frequenz der Beratung/Behandlung | *Nein* | 2-5, 8 |
| 17 | Vertragstext und Geschäftskorrespondenzen | *Nein* | 2-5, 7, 8 |
| 18 | Sacn/Kopie zur Identitätsfeststellung | *Nein* | 2-5 |
| 19 | Auftragssperre= Recht auf Einschränkung geltend gemacht | *Nein* | 2-5 |
| 20 | Schlüssel für verschlüsselte Datenübertragung | Geheim | Alle |
| 2. An der Abwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten | 21 | Name, Firma oder sonstige Geschäftsbezeichnung | *Nein* | 1-8 |
| 22 | Anschrift, Lieferadresse | *Nein* | 2-8 |
| 23 | Homepage, Xing, ... | *Nein* | 3-5 |
| 24 | Kontaktdaten (Tel., Skyp, signal.org, Mail, Fax,) | *Nein* | 2-8 |
| 25 | Firmenbuchdaten | *Nein* | 2-8 |
| 26 | Bankverbindungen | *Nein* | 2-8 |
| 27 | Kreditkartennummern und unternehmen | *Nein* | 1-4 |
| 28 | Kenn-Nummern für Zwecke amtlicher Statistik wie UID-, Intrastat-Kennzahl,…., Steuer-Nummer | *Nein* | 2-8 |
| 29 | Namen Kontaktpersonen | *Nein* | 1-8 |
| 30 | Zuordnung zu einer bestimmten Kategorie (einschließlich regionale Zuordnung, usw.) | *Nein* |  |
| 31 | Art der Kooperation | *Nein* | 3-8 |
| 32 | Vertragstext und Geschäftskorrespondenzen | *Nein* | 2-5, 7, 8 |
| 33 | Auftragssperre= Recht auf Einschränkung geltend gemacht | *Nein* |  |

### Löschungs- und Aufbewahrungsfristen

|  |  |
| --- | --- |
| **Daten (Lfd. Nr.)** | **Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen** |
| 1 – 19; 21-33 | Aufgrund der gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre, darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen |
| 18 | Identitätskopie wird sogleich nach Zweckerfüllung gelöscht |
| 19, 33 | Bei Antrag auf Löschung werden nur die notwendigsten Buchhaltungsdaten beibehalten und für 7 Jahre eingeschränkt, d.h. sie können nicht mehr verarbeitet werden (= Auftragssperre in vielen Programmen) |
| 7 | IP-Adresse zu eigenen Sicherheitszwecken: Speicherfrist von maximal 7 Tagen (siehe auch Datenschutzerklärung Homepage) |

### Kategorien der Empfänger

Es erfolgt keine Übermittlung an Drittstaaten und internationale Organisationen. Übermittlungsort ist Wien bzw. Österreich

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Empfängerkategorien**  | **Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)** | **Internationale Organisation** |
| 1 | Banken | Nein | Nein |
| 2 | Rechtsvertreter im Anlassfall | Nein | Nein |
| 3 | Steuerberater, Bilanzbuchhalter | Nein | Nein |
| 4 | Gerichte im Anlassfall | Nein | Nein |
| 5 | Verwaltungsbehörden im Anlassfall | Nein | Nein |
| 6 | An der Abwicklung beteiligte Dritte | Nein | Nein |
| 7 | Vertrags- und Geschäftspartner(inklusiv. Honorarabr.--Vereine) | Nein | Nein |
| 8 | Privat-Versicherung | Nein | Nein |
| 9 | Homepage-Hoster /Software-Dienstleister  | ? | Nein |
| 10 | Alle weiteren (IT)-Dienstleister(auch mit Fernwartung) | ? | Nein |
|  | Datendienst verschlüsselt und sicher  | ? | Nein |

### TOMs

siehe dort. Nur an jene Empfängern, mit denen eine gesicherte und verschlüsselte Übertragung möglich ist, wird eine elektronische Übertragung sensibler Daten vorgenommen. Alle anderen erhalten die pB Daten der Klienten ausschließlich per eingeschriebener Post oder durch Ident.Brief auf Kosten des Empfängers.

Abrechnungen als Buchhaltungsunterlagen enthalten keine Diagnosen oder ähnliches bzw. sind von mir geschwärzt. Sollte das Finanzamt die Originalrechnungen der Sozialversicherungen etc. verlangen, so habe ich diese mit Diagnose archiviert (siehe Klientenverwaltung und Honorarabrechnung)

## Klientenverwaltung und Dokumentation

### Verantwortliche

Titel / Vor-und Zuname
 Straße
 PLZ-Ort
 Email: …………...@…………………….
 Tel.:

### Zweck der Datenverarbeitung

* Verarbeitung und Übermittlung von **sensiblen Informationen der Betroffenen**, insbesondere Datenkategorien iSd Art 9, möglicherweise Art 10 DSGVO und Art 8 somit auch von Kindern,sowie Führung und Pflege von PatientInnen/KlientInnenkarteien gemäß Psychotherapiegesetz 1990
* Erstellung und Übermittlung von medizinischen Gutachten/Befunde durch Therapeuten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten
* Honorarverrechnung psychotherapeutischer Behandlungen durch Personen, die gemäß § 11 des Psychotherapiegesetz , BGBl. Nr. 361/1990 zur selbständigen Ausübung der Psychotherapie berechtigt sind, (§ 135 Abs. 1 Z 3 ASVG) mit den Sozialversicherungsträgern einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.
* Archivierung x Jahr/ 6 Monate/ 3 Monate / gleich nach Beendigung der Beratung/Behandlung gemäß § 15 Verschwiegenheit und § 16b Dokumentationspflicht Psychotherapiegesetz

### Rechtsgrundlage (in der geltenden Fassung)

* Art 6 Z 1 lit a (Einwilligung der Betroffenen betreffs Weiterleitung),
* Ansonsten Art 6 Z 1 lit b (zur Vertragserfüllung erforderlich) DSGVO sowie Art 6 Z 1 c gesetzliche Verpflichtungen DSGVO in Verbindung mit § 15 Verschwiegenheit und § 16b Dokumentationspflicht Psychotherapiegesetz . Bei sensiblen Daten kann kein berechtigtes Interesse geltend gemacht werden.
* § 349a Allgemeines Sozialversicherungsgesetz (ASVG), BGBl. Nr. 189/1955, (60. Novelle ASVG), § 193 Gewerbliches Sozialversicherungsgesetz (GSVG), BGBl. Nr. 560/1978, § 181 Bauern-Sozialversicherungsgesetz (BSVG), BGBl. Nr. 559/1978, § 3 des Bundesgesetzes über die Sozialversicherung freiberuflich selbständig Erwerbstätiger (FSVG), BGBl. Nr. 624/1978, § 128 Beamten- Kranken- und Unfallversicherungsgesetz (B-KUVG), BGBl. 200/1967,
* Gesamtvertrag abgeschlossen zwischen der beruflichen Interessenvertretung des Auftraggebers und dem Hauptverband der österreichischen Sozialversicherungsträger gemäß § 349 Abs. 2 und Abs. 3 ASVG
* Für den Träger der Krankenversicherung vom Hauptverband abgeschlossene Einzelverträge mit freiberuflichen Psychotherapeuten gemäß § 349 Abs. 2 ASVG.
* Psychotherapiegesetz BGBl.Nr. 361/1990 ST0151
* (Berufskodex für Psychotherapeutinnen und Psychotherapeuten)

**Sonstige Hinweise:**
Die Datensicherheitsmaßnahmen gemäß DSG 2018 bzw. DSGVO sind zu beachten. Insbesondere hat die Übermittlung der Datensätze an den Empfänger in sicherer, verschlüsselter Form zu erfolgen.

### Kategorien der verarbeiteten Daten

(siehe auch Psychotherapiegesetz)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Betroffene Personengruppen: | Nr.: | Datenkategorien | **Daten iSd Art 9 + 10 DSGVO** | **Daten f.Archivierung** | **Wissenschaftanonymisiert** | EmpfängerKategorien |
| Klienten des Verantwortlichen sowie Patienten/ Klienten von zuweisenden Gesundheitsdienste­anbietern oder ÄrztInnen. Klinische PsychologInnen, SozialarbeiterInnen und sonstigen Gesundheitsberufen | 01 | Patienten-/Klientennummer, Protokollnummer | Nein |  | Neue Zufallsnummer | Gesetzlich1 + 2 + 7Einwilligung3 + 4Auftragserfüllung5gesetz/Einw6 |
| 02 | Namen, frühere Namen (Namensteile) | Nein |  |  |
| 03 | Anschrift | Nein |  |  |
| 04 | Telefon- und Faxnummer, Email, | Nein |  |  |
| 05 | Geburtsdaten | Vertraulich |  |  |
| 06 | Staatsangehörigkeit | Nein |  |  |
| 07 | Geschlecht | Nein |  |  |
| 08 | Personenstand(Verpartnerung ist Info über sexuelle Orientierung) | Ja |  |  |
| 09 | Soziale Verhältnisse (z.B. erwerbstätig, Pensionist, Selbstversicherer, arbeitslos) sowie Zusatzfelder zB Beruf, .. | Vertraulich |  | Nur: erwerbstätig, Pensionist, Selbst-versicherer, arbeitslos |
| 10 | Sozialversicherungsnummer | Vertraulich |  |  |
| 11 | Sozialversicherungsträger | Vertraulich |  |  |
| 12 | Sonstige Daten zur Sozialversicherung (das Verwandtschaftsverhältnis zum Hauptversicherten bei mitversicherten Patienten und Daten des Antrages auf Kostenzuschuss für die Weiterführung der Behandlung/Therapie) | Vertraulich |  |  |
| 13 | Daten zu einem privaten Versicherungsverhältnis (Versicherer, Polizzennummer usw.) | Vertraulich |  |  |
| 14 | Daten sonstiger Kostenträger | Nein |  |  |
| 15 | Daten über die Erklärung der Kostenübernahme durch einen Kostenträger | Nein |  |  |
| 16 | Inanspruchnahme des Auftraggebers (Anlass, Datum, Art und Anzahl der Beratungen/Behandlungen/Therapieeinheiten) | Ja |  |  |
| 17 | Daten zur Verwaltung von Terminen und Wartelisten | Vertraulich |  |  |
| 18 | Zustand der Person bei Übernahme der Beratung oder Behandlung | Ja |  | anonymisiert |
| 19 | Anamnese (Familien- und Eigenanamnese, Berufsanamnese) | Ja |  | anonymisiert |
| 20 | Vorbehandlungen | Ja |  | anonymisiert |
| 21 | Diagnosen (nach ICD-10 und auch Fremddiagnosen) zu Behandlungsbeginn und bei Beendigung | Ja |  | anonymisiert |
| 22 | Besondere Risikofaktoren (zB tätigkeitsbedingte Einflüsse, familiäre Disposition, ausgeübte Tätigkeit) | Ja |  | anonymisiert |
| 23 | Gutachtliche Äußerungen des Auftraggebers (zB gegenüber Auftraggebern von Gutachten) | Ja |  | anonymisiert |
| 24 | Behandlungs-/Beratungsverlauf, besondere Vorkommnisse während der Behandlung | Ja |  | anonymisiert |
| 25 | Information an Patienten (insbesondere über Gesundheitsrisiken und Schutzfaktoren in verschiedenen Lebensabschnitten bzw.-situationen) sowie erfolgte Aufklärungsschritte und allfällige Empfehlungen zur ergänzenden Abklärung | Ja |  | anonymisiert |
| 26 | Angaben über Art, Umfang und Methoden (der beratenden, diagnostischen und therapeutischen Leistungen sowie der Pflege) | Ja |  | anonymisiert |
| 27 | Daten zur Anwendung von Arzneispezialitäten | Ja |  | anonymisiert |
| 28 | Daten zur Abrechnung von Honoraren, vereinbartes Honorar und sonstige weitere Vereinbarungen im Rahmen des Behandlungsvertrags | Ja, solange inklusive Diagnose |  |  |
| 29 | Daten zur Abrechnung der Gebühren oder Entgelte für Gutachtertätigkeit | Ja, solange inklusive Diagnose |  |  |
| 30 | Wert, Summe und Gesamtbetrag der Leistungen | Nein |  |  |
| 31 | Konsultationen von Berufskollegen sowie von Angehörigen anderer Gesundheitsberufe oder sonstiger relevanter Berufe | Ja |  | anonymisiert |
| 32 | personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten | Ja |  | anonymisiert |
| Arbeitgeber: | 33 | Name und Anschrift des Arbeitgebers des Hauptversicherten | Nein |  |  |
| Kontaktperson (nach Angabe des Patienten/Klienten) oder gesetzlicher Vertreter des Patienten/Klienten: | 34 | Name | Nein |  |  |
| 35 | Anschrift | Nein |  |  |
| 36 | Telefon- und Faxnummer und Email | Nein |  |  |
| 37 | Zustimmung des gesetzlichen Vertreters zur Behandlung/Beratung | Vertraulich |  |  |
| Für Alle | 38 | Sichere verschlüsselt Verbindung, (Schlüssel, Passwort, ...) | Geheim |  |  |
| **Für Alle**Psychotherapiegesetz  | 39 | Auskunft bzw Einsicht in Dokumentationerteilt bzw. verweigert | Geheim |  | **1 -7** |

### Kategorien der Empfänger

Es erfolgt keine Übermittlung an Drittstaaten oder Internationale Organisationen, Übermittlungsort ist Wien bzw. Österreich

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Rechtsgrundlage** | **Empfängerkategorien** |
| 1 | gesetzlich | Sozialversicherungsträger (einschließlich Betriebskrankenkassen), MA11 und sonstige Kostenträger im Rahmen ihrer rechtlichen Befugnisse auf Grund von Gesetzen oder Sozialversicherungsabkommen; |
| 2 | gesetzlich | Auftraggeber von Gutachten, soweit die rechtlichen Voraussetzungen für die Erstellung des Gutachtens vorliegen; |
| 3 | mit ausdrücklicher Einwilligung der KlientInnen | Privatversicherungen zum Zweck der Abwicklung des Versicherungsanspruches |
| 4 | mit ausdrücklicher Einwilligung der KlientInnen | Ärzte, Vertreter von sonstigen Gesundheitsberufen und medizinische oder soziale Einrichtungen, sowie nicht-ärztliche Gesundheitsberufe in deren Behandlung der Patient steht oder überwiesen wird. |
| 5 | mit ausdrücklicher Einwilligung der KlientInnen | Ihren Honorar-Abrechnungs-Verein eintragen |
| 6 | Nur im Anlassfall (gesetzl. Regelung bzw. Einwilligung der KlientInnen) | Mit der Rechtsdurchsetzung, Streitschlichtung und Klärung von Beschwerden der Patienten/Klienten und Abrechnungsansprüchen (des Auftraggebers) betraute Stellen, insbesondere Rechtsanwälte, Gerichte, Schlichtungsstellen und Patientenanwälte, |
| 7 | Im Falle meiner Karenz,Pensionierung, Arbeitsunfähigkeit oder Todes | ist der Erbe oder sonstige Rechtsnachfolger unter Wahrung des Datenschutzes verpflichtet, die Dokumentation für die der Aufbewahrungspflicht entsprechende Dauer gegen Kostenersatz 1. einem genannten Berufsangehörigen, der in diese Benennung und Pflichtenübernahme schriftlich eingewilligt hat, andernfalls2. vom Bundesministerium für Gesundheit zu bestimmenden Dritten zu übermitteln. |

### Speicherdauer und Löschfristen

Die sensiblen Informationen der PatientInnen/KlientInnen sind gemäß §16a (3) Dokumentationspflicht Psychotherapiegesetz 1990 zehn Jahre aufzubewahren. Weiters ist es zulässig, alle Daten bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden, aufzubewahren.

Vor allem bei Kindern und Jugendlichen, die Opfer von kriminellen Handlungen und Übergriffen geworden sind und bei denen die Dokumentation später als Beweise benötigt werden könnte, kann die Löschungsfrist auf 30 Jahre und länger im Einzelfall verlängert werden.

### TOMs

siehe dort. Insbesondere nur an jene Empfängern, mit denen eine gesicherte und verschlüsselte Übertragung möglich ist, wird eine elektronische Übertragung vorgenommen. Alle anderen erhalten die pB Daten der Klienten/Patienten ausschließlich per eingeschriebener Post bzw. Ident.Brief auf Kosten des Empfängers.

x Jahr/ 6 Monate/ 3 Monate / gleichnach **Beendigung der Beratung/Behandlung** bzw. umgehend bei **Antrag auf Löschung** der pb Daten seitens des Betroffenen,

1. werden alle pb Daten aus dem „Rechnungswesen und Geschäftsabwicklung“ und da ich einen Newsletter versenden, auch alle Daten „Kundenbetreuung und Kommunikation“ gelöscht, ausgenommen sind Daten, die für die Buchhaltung aufgrund der gesetzlichen Aufbewahrungsfrist 7 Jahre aufbewahrt werden müssen
2. werden alle für Archivierung angekreuzten sensiblen Daten aus diesem „Klientenverwaltung und Honorarabrechnung“ -verzeichnis wie folgt behandelt:

|  |  |
| --- | --- |
| Bitte ankreuzen | Methode |
|  | Analog(ausgedruckt in Ordnern an einem sicheren Ort) |
|  | Digital-Intern( verschlüsselt auf mind. 2 verschiedenen Datenträger an einem sicheren Ort) |
|  | Digital-Extern(verschlüsselt bei einem Anbieter + Vereinbarung Art 28 DSGVO) |
|  | Mikroverfilmung(Verfilmt + Vereinbarung Art 28 DSGVO, an einem sicheren Ort) |

# Daten-/Auftragsverarbeitungsverträge

Bitte hier alle Verträge bzw Links zu AGBs usw für alle ihre Auftrags/Datenverarbeiter eintragen:

|  |  |  |  |
| --- | --- | --- | --- |
| **Zweck** | **Firma** | **Vertrag archiviert** | **Bemerkungen** |
| Homepage-Hoster |  |  |  |
| Newsletter |  |  |  |
| IT mit Fernwartung |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

## Impressum und Datenschutzerklärung

Hier Link zu AGBs , Impressum und Datenschutzerklärung in der eigenen Homepage eintragen

## Grundsätzlich

Die im „Berufskodex für Psychotherapeutinnen und Psychotherapeuten“ formulierten Grundsätze und Maßnahmen sind für mich binden und Grundlage meiner Beratung.

## Kontaktaufnahme

Wenn ein potentieller Klienten von seiner Seite mit mir per Email oder telefonisch Kontakt aufnimmt, so darf ich dessen Namen, Kontaktdaten, Interesse (Einzel- oder Gruppentherapie, …) zur Durchführung vorvertraglicher Maßnahmen verarbeiten (Art 6 (1) b DSGVO ... auf Anfrage der betroffenen Person ...). Sollte es zu keinem Behandlungsvertrag kommen, so werde ich diese Daten nach 2 Jahren löschen.

In allen meinen Emails steht unter P.S.: „Zur werten Kenntnisnahme meine Datenschutzerklärung!“ mit Link zur Homepage/Datenschutzerklärung

## Erstgespräch

Im Erstgespräch informiere in meine Klienten

* und lege den **Aushang** „ Datenschutzerklärung“ zur Kenntnisnahme vor und dokumentiere dies
* vor allem mit Hilfe des „**Informationsblatt über sensible Daten (Art 9 + 13 DSGVO)**“ (siehe Anhang) über seine Rechte gemäß DSGVO und wie ich welche sensible Daten verarbeite
* ,dass die gesamte Kommunikation sicher und vertraulich bzw. verschlüsselt erfolgen wird, und zeige auch mit Hilfe meines eigenen sicheren Kommunikations-App, wie dies dann in der Praxis erfolgen könnte. Sollte der Klient kein sicheres App verwenden wollen oder können, so erkläre ich, dass ich z.B. Gutachten ihm/ihr nur per eingeschriebenen Brief zusenden werde und nicht unverschlüsselt per Email.
* abschließend bitte ich meinen Klienten die „Einwilligungserklärungen betreffs Weiterleitung“ anzukreuzen.
* Auch Bestandsklienten werde ich entsprechend informieren und ihnen diese **Informationsblatt über sensible Daten (Art 9 + 13 DSGVO)** zur Kenntnisnahme vorlegen.

## Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*

|  |  |  |  |
| --- | --- | --- | --- |
| ? | Alarmanlage |  | Absicherung von Gebäudeschächten |
| **X** | Rücksicht beim Aufrufen der Klienten usw.(siehe Kodex) |  | Chipkarten-/Transponder-Schließsystem |
|  | Schließsystem mit Codesperre | **X** | Manuelles Schließsystem |
|  | Automatisches Zugangskontrollsystem |  | Videoüberwachung der Zugänge |
|  | Lichtschranken / Bewegungsmelder | **X** | Sicherheitsschlösser – auch bei Aktenkästen |
| **X** | Schlüsselregelung (Schlüsselausgabe etc.) |  | Personenkontrolle beim Pförtner / Empfang |
| **X** | Protokollierung der Besucher | **X** | Sorgfältige Auswahl von Reinigungspersonal |
| **X** | Bildschirmsperre nach 10 Minuten |  | Tragepflicht von Berechtigungsausweisen |
| **X** | Verschlossene Türen bei Abwesenheit | **X** | Fenstersicherung (Erdgeschoss) |

## Zugangskontrolle

*Maßnahmen, die geeignet sind* *zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

|  |  |  |  |
| --- | --- | --- | --- |
| **X** | Zuordnung von Benutzerrechten**Einzelpraxis, daher Verantwortliche** | **X** | Erstellen von Benutzerprofilen**Einzelpraxis, daher Verantwortliche** |
| **X** | Passwortvergabe**Einzelpraxis, daher Verantwortliche** |  | Authentifikation mit biometrischen Verfahren |
| **X** | Authentifikation mit Benutzername / Passwort | **X** | Zuordnung von Benutzerprofilen zu IT-Systemen**Einzelpraxis, daher Verantwortliche** |
| **X** | Gehäuseverriegelungen |  | Einsatz von VPN-Technologie |
| **X** | Sperren von externen Schnittstellen (USB etc.) | **X** | Sicherheitsschlösser |
| **X** | Schlüsselregelung (Schlüsselausgabe etc.) |  | Personenkontrolle beim Pförtner / Empfang |
| **X** | Protokollierung der Besucher | **X** | Sorgfältige Auswahl von Reinigungspersonal |
| ? | Eigenes Handy für Beruf |  | Tragepflicht von Berechtigungsausweisen |
| **X** | Einsatz von Intrusion-Detection-Systemen | **X** | Verschlüsselung von mobilen Datenträgern |
| **X** | Verschlüsselung von Smartphone-Inhalten | **X** | Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |
| **X** | Einsatz von Anti-Viren-Software | **X** | Verschlüsselung von Datenträgern in Laptops / Notebooks / USB |
| **X** | Einsatz einer Hardware-Firewall | **X** | Einsatz einer Software-Firewall |

## Zugriffskontrolle

*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung, hier nur der Verantwortliche. unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

|  |  |  |  |
| --- | --- | --- | --- |
| **X** | Erstellen eines Berechtigungskonzepts**Einzelpraxis, daher Verantwortliche** | **X** | Verwaltung der Rechte durch Systemadministrator**Einzelpraxis, daher Verantwortliche** |
| **X** | Anzahl der Administratoren auf das „Notwendigste“ reduziert**Einzelpraxis, daher Verantwortliche** | **X** | Passwortlänge, Passwortwechsel |
| **X** | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten**Einzelpraxis, daher Verantwortliche** | **X** | Sichere Aufbewahrung von Datenträgern(Data-Safe) |
| **X** | physische Löschung von Datenträgern vor Wiederverwendung(extern nur mit Datenverarbeitungsvereinbarung) | **X** | ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| **X** | Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | **X** | Protokollierung der Vernichtung |
| **X** | Verschlüsselung von Datenträgern |  |  |

## Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

|  |  |  |  |
| --- | --- | --- | --- |
|  | Einrichtungen von Standleitungen bzw. VPN-Tunneln | **X** | Weitergabe von Daten in anonymisierter oder pseudonymisierter Form**=> siehe Verarbeitungsverzeichnis** |
| **X** | E-Mail-Verschlüsselung | **X** | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen**=> siehe Verarbeitungsverzeichnis** |
| **X** | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen **=> siehe Verarbeitungsverzeichnis** | **X** | Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| **X** | Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen | **X** | Verschlüsselung der übertragenen Daten |

## 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.*

|  |  |  |  |
| --- | --- | --- | --- |
| **X** | Protokollierung der Eingabe, Änderung und Löschung von Daten**Einzelpraxis, daher nur Verantwortliche** | **X** | Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.**=> siehe Verarbeitungsverzeichnis** |
| **X** | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)**Einzelpraxis, daher nur Verantwortliche** | **X** | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| **X** | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts**Einzelpraxis, daher nur Verantwortliche** |  |  |

## Auftragskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Hier kommt die* ***Datenverarbeitungs-Vereinbarung nach Art 28 DSGVO*** *zum Tragen, somit alles ankreuzen, siehe Anhang*

|  |  |  |  |
| --- | --- | --- | --- |
| **X** | Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)Sollte eine Dokumentation gemäß DSGVO gemacht haben! | **X** | vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| **X** | schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) siehe Anhang | **X** | Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis |
|  | Auftragnehmer hat Datenschutzbeauftragten bestellt | **X** | Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| **X** | Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | **X** | laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |
| ? | Vertragsstrafen bei Verstößen |  |  |

## Verfügbarkeitskontrolle

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | Unterbrechungsfreie Stromversorgung (USV) |  | Klimaanlage in Serverräumen |
|  | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen |  | Schutzsteckdosenleisten in Serverräumen |
| **X** | Feuer- und Rauchmeldeanlagen | **X** | Feuerlöschgeräte (in Serverräumen) |
|  | Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | **X** | Erstellen eines Backup- & Recoverykonzepts |
| **X** | Testen von Datenwiederherstellung |  | Erstellen eines Notfallplans |
| **X** | Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort |  | Serverräume nicht unter sanitären Anlagen |
|  | In Hochwassergebieten: Serverräume über der Wassergrenze |  |  |

## Trennungsgebot

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

|  |  |  |  |
| --- | --- | --- | --- |
| **X** | physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern |  | Logische Mandantentrennung (softwareseitig) |
| **X** | Erstellung eines Berechtigungskonzepts**Einzelpraxis, daher Verantwortliche** | **X** | Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
| **X** | Versehen der Datensätze mit Zweckattributen/Datenfeldern**=> siehe Verarbeitungsverzeichnis** | **X** | Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System**=> siehe Verarbeitungsverzeichnis** |
| **X** | Festlegung von Datenbankrechten**Einzelpraxis, daher Verantwortliche** |  | Trennung von Produktiv- und Testsystem |

Quelle unter anderem: <https://www.datenschutz-guru.de/files/Ausfuellhilfe_TOM_9_BDSG_V2.docx>

## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Risikoanalyse

Datenschutzfreundliche Voreinstellungen

Weiterbildung siehe Schulung

### Auftragskontrolle:

Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, sichere und verschlüsselte Speicherung und Übertragung, ( zB. Ob Datenschutzbeauftragter und/oder Dokumentation nach DSGVO vorhanden, Vorabüberzeugungspflicht, Nachkontrollen) siehe Punkt 3. oben

### Ein Kontroll- und Verbesserungsprozess wir mindestens 1x jährlich durchgeführt:

|  |  |
| --- | --- |
| **Jahr** | Ergebnisse der Überprüfung, Bewertung und Evaluierung |
| 2019 |  |
| 2020 |  |

Referenzen: Art 32 Z 1 DSGVO

# Betroffenenrechte wahren

Gemäß der DSGVO hat jeder Betroffene folgende Rechte, soweit diese das Vertrauensverhältnis zwischen Klienten und mir als nicht gefährden (§ 16a. (2) Psychotherapiegesetz 1990):

* Recht auf Auskunft (Art 15 DSGVO) nur in Verbindung mit
Recht auf Einsicht in die Dokumentation (§16a. (1) Psychotherapiegesetz 1990)
* Recht auf Berichtigung (Art 16 DSGVO)
* Recht auf Löschung (Art 17 DSGVO )
* Recht auf Einschränkung (Art 18 DSGVO)
* Recht auf Übertragbarkeit (Art 20 DSGVO)
* Recht auf Widerspruch (Art 21 DSGVO)
* Recht auf Beschwerde bei der [Datenschutzbehörde](https://www.dsb.gv.at/rechte-der-betroffenen%22%20%5Cl%20%22Zustaendigkeit_der_Datenschutzbehoerde)

## Prozesse betreffs Betroffenenrechte

**Definition Stammdatenblatt**: Dies sind alle pb Daten des Betroffenen aus dem Verarbeitungsverzeichnis „Rechnungswesen und Geschäftsabwicklung“ und „Kundenbetreuung und Kommunikation“ - ohne sensible Informationen.

1. Ich erhalte Kenntnis dass ein Betroffener seine Rechte geltend machen will, sei es z.B. mündlich, schriftlich. per Email (insbesondere hier ihr Email ), …
2. **Feststellung der Identität:**
Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:

Bitte hier gemäß Ihrer Risiko-Analyse Ihren gewählten Prozess betreffs Identität eintragen

1. Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits sind notwendig.
2. Identität zweifelsfrei festgestellt und die Anfrage ist rechtens
=> Der Betroffene bekommt gemäß Art 19 DSGVO innerhalb von maximal 4 Wochen abhängig von seiner Anfrage in klarer und verständlicher Sprache folgende Antworten:
* Recht auf Auskunft (Art 15 DSGVO)
Der Betroffene erhält den
	+ Anhang Auskunftsersuchen ausgefüllt für alle Stammdaten betreffs „„Rechnungswesen und Geschäftsabwicklung“ und „Kundenbetreuung und Kommunikation“
	+ und kostenlos **Einsicht** in die Dokumentation über die zu seiner Person gespeicherten sensiblen Daten oder einmalig ohne Kosten die Herstellung von Abschriften, beides soweit diese das Vertrauensverhältnis zwischen mir und meinen Klienten nicht gefährden. (§ 16a. (2) Psychotherapiegesetz 1990)
* Recht auf Berichtigung (Art 16 DSGVO)
Der Betroffene bekommt als PDF
	+ sein Stammdatenblatt mit den berichtigten Daten (Screenshot)
* Recht auf Löschung (Art 17 DSGVO )
Der Betroffene bekommt als PDF
	+ sein gelöschtes Stammdatenblatt (ausgenommen Name) als Screenshot als Nachweis, dass die Löschung erfolgt ist mit den Hinweis, dass
		- die Daten **anonymisiert** für die interne Statistik oder wissenschaftlicher Auswertung verwendet werden
		- und das alle Daten inklusive Namen anschließend unwiderruflich gelöscht wurde. **oder**
	+ Bei einem bestehenden oder abgeschlossenem Beratung/Behandlungsvertrag mit dem Betroffenen kommt der Prozess betreffs der sensiblen Daten, wie beim Verarbeitungsverzeichnis „Klientenverwaltung und Honorarabrechnung“ dort bei den TOMs als **Archivierung** , zum Tragen (§16a (3) Dokumentationspflicht Psycho­therapie­gesetz 1990). Das Ende des Prozesses ist die vollständige Löschung aller Daten des Betroffenen im System, ausgenommen sind Buchhaltungsunterlagen aufgrund gesetzlicher Aufbewahrungsfristen, diese werden dann „einge­schränkt“ (siehe unten Art 18) und nach 7 Jahren gelöscht, darüber hinaus­gehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen.

	Die Löschungsfrist für die archivierte Dokumentation ist 10 Jahre, darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen.

	Vollständig anonymisiert gibt es keine Löschungsfristen

.

* Recht auf Einschränkung (Art 18 DSGVO)
Der Betroffene bekommt als PDF
	+ sein Stammdatenblatt, dem er entnehmen kann, dass bei „Recht auf Einschränkung geltend gemacht“ ein Hackerl gesetzt ist und somit keine Verarbeitung seiner pb Daten erfolgt.
	(= Auftragssperre bei den meisten CRM-Systemen)
* Recht auf Übertragbarkeit (Art 20 DSGVO)
Gemäß Art 20 Z2 DSGVO übermittle ich alle Daten des Betroffenen inklusive Doku­mentation als CC. an einen anderen verantwortlichen Berufsangehörigen, sobald ich dessen Benennung und Pflichtenübernahme schriftlich erhalten habe (ähnlich Todesfall des Therapeuten), aber nur wenn eine sichere und verschlüsselte Übertragung möglich ist. Ansonsten nur per eingeschriebener Post.
* Recht auf Beschwerde bei der [Datenschutzbehörde](https://www.dsb.gv.at/rechte-der-betroffenen%22%20%5Cl%20%22Zustaendigkeit_der_Datenschutzbehoerde)

### Profiling

Ich mache kein Profiling .

Referenzen: Art 4, Art 8, Art 9 DSGVO; Erwägungsgründe: 26ff, 51ff; § 4 Abs 4 DSG 2018;

### E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO)

Ich versende keine Newsletter wenn doch, siehe siehe Anhang

## Meldung von Datenschutzverletzungen

Die DSGVO definiert in Art 33 eine „Verletzung des Schutzes personenbezogener Daten“ (data breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

ch erlange Kenntnis von einer Datenschutzverletzung und führe eine neuerliche Risikoanalyse aus der Sicht der Betroffenen durch

1. **Innerhalb von 72 Stunden** mache ich eine Meldung mit Hilfe des „Muster Datenschutzverletzung“ (siehe Anhang) an die gemäß Art 55 DSGVO zuständige **Aufsichtsbehörde, wenn** die Verletzung des Schutzes pb Daten voraussichtlich zu einem **Risiko** für die Rechte und Freiheiten natürlicher Personen führt.
2. mache ich eine Meldung mit Hilfe des „Muster Datenschutzverletzung“ (siehe Anhang) auch **an alle Betroffene, wenn** die Verletzung des Schutzes pb Daten voraussichtlich zu einem **hohem Risiko** für die Rechte und Freiheiten natürlicher Personen führt.
3. Die Datenschutzbehörde ist wohlbegründet der Meinung, dass hier ein hohes Risiko vorliegt und fordert mich auf auch alle/gewisse Betroffenen zu informieren, siehe Art 34 Z4 DSGVO.
	1. Ich informiere Betroffenen umgehend mit einer entsprechenden Variation des „Muster Datenschutzverletzung“ (siehe Anhang)
4. Ich werde alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht, siehe Art 33 Z5 DSGVO.

# Risikoanalyse

Referenzen: Art 24 + 25 DSGVO, Erwägungsgründe: 74-78, 81

## Risikoanalyse ohne Maßnahmen

Schutzziele für meine Risikobewertung nach Art 4 Z 12 sind: Vertraulichkeit, Integrität und Verfügbarkeit. Die Risiko-Bewertung erfolgt nach „Schwere“ und „Eintrittswahrscheinlichkeit (EWK)“ (siehe Anleitung)

Folgende Daten wurden vorab analysiert und dann hier in die entsprechenden Kategorien eingetragen:

### Risikokategorien

|  |  |
| --- | --- |
| **Kategorie** | **pb Daten** |
| **1** | **Besondere Datenkategorien iSd Art 9 DSGVO**Kinder unter 14 Jahren gem. Art 8, bzw. DSG 2018, möglicherweise strafrechtliche Daten gem. Art 10; sowie Mitschriften u. Fotos, Personenstand, DokumentationBitte ausfüllen**=> geheim/vertraulich** |
| **2** | Schlüssel, Passwörter, … , Vertragstext und Geschäftskorrespondenzen, sonstige Vereinbarungen, Geburtsdatum , Bankverbindungen, Kreditkartennummern und -unternehmenBitte ausfüllen**=> geheim** |
| **3** | Pb Daten mit vernachlässigbaren bis begrenzten Schutzbedarf, siehe Vorabanalyse in der AnleitungBitte ausfüllen**=> intern/vertraulich** |

### Risiko-Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Schwere** |  |  |  |  |  |
| Existenzgefährdend |  |  |  | **1** |  |
| Wesentlich |  |  |  | **2** |  |
| Begrenzt |  |  |  | **3** |  |
| Vernachlässigbar |  |  |  |  |  |
|  | Vernachlässigbar | Möglich | Sehr wahrscheinlich | Garantiert | **EWK** |

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

**Folgen ohne Maßnahmen:**

|  |
| --- |
| **Data Breach** |
| **Kein Risiko** | **Risiko** | **Hohes Risiko** |
|  | * Datenschutzbehörde **UND** Betroffene informieren
* Folgeabschätzung notwendig
 |

### Maßnahmen

Siehe TOMs, insbesondere **Verschlüsselung am Datenträger (encryption of data in rest), bei der Übertragung (data in motion) und Backup!**

### Vertraulichkeit

1. **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mit Schlüssel
2. **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung mit Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Data in Rest und Motion und somit keine Weiterleitung ohne sichere und verschlüsselter Übertragung bzw. RSB - Einzelpraxis
3. **Zugriffskontrolle**: Zugriff nur durch Verantwortlichen - Einzelpraxis

### Integrität

1. **Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt, Dokumentenmanagement - Einzelpraxis

### Verfügbarkeit

1. **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, Sicherungskonzept mit verschlüsselter Lagerung der Sicherungen
2. Rasche **Wiederherstellbarkeit**: Backup mindestens wöchentlich, am besten täglich

## Risiko-Matrix mit Maßnahmen

Bitte hier die Kategorien 1, 2, 3 gemäß Ihrer Maßnahmen überprüfen **sollten im grünen Bereich sein**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Schwere** |  |  |  |  |  |
| Existenzgefährdend |  |  |  |  |  |
| Wesentlich |  |  |  |  |  |
| Begrenzt |  | **1** |  |  |  |
| Vernachlässigbar | **3** | **2** |  |  |  |
|  | Vernachlässigbar | Möglich | Sehr wahrscheinlich | Garantiert | **EWK** |

### Folgen der Maßnahmen betreffs Risiko

|  |
| --- |
| **Data Breach** |
| **Kein Risiko** | **Risiko** | **Hohes Risiko** |
|  | * Datenschutzbehörde informieren
 |  |
| **Betroffene sind nicht zu informieren**Keine Folgenabschätzung notwendig |

Aufgrund der gesetzten TOMs muss bei einem Data Breach der betroffene Klient nicht informiert werden, nichts desto trotz muss die Behörde bei Data Breach mit Risiko für pb Daten der Kategorie 1 informiert.
Referenzen: Art 22 + 35 DSGVO, Erwägungsgründe: 76, 84 und 89 – 93, Working Paper 240 der Art 29 Gruppe

# Zusammenfassung

Ich sehe das hier dokumentierte Datenschutzniveau vor allem mit der Trennung der Verarbeitungskreisen und mit den gesetzten TOMs für mich als Therapeut und EPU (siehe Allgemeiner Teil) auch aufgrund meiner finanziellen, technischen und organisatorischen Beschränkungen als **angemessen und ausreichend** an.

Ich kann so gegenüber meinen Klienten mit gutem Gewissen sagen:

*Liebe Klienten und Klientinnen!*

*Vertrauen zwischen mir als Verantwortliche und Ihnen ist die Grundlage und Voraussetzung für meine Beratung, daher sind auch alle Ihre persönlichen und beruflichen Daten bei mir in guten Händen.

Ich sichere Ihnen zu, dass ich sorgsam und streng vertraulich damit umgehe und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen bin.*

*Darauf können Sie vertrauen.*

*Ort am……...*

*……………………………………………..
Unterschrift*

# Anhang

## **Informationsblatt über sensible Daten (Art 9 + 13 DSGVO)**

Sehr geehrte Klientin!
Sehr geehrter Klient!

Gemäß Artikel 13 DSGVO möchte ich Name Psychotherapeut/in Sie vorab informieren, dass ich als Verantwortliche/r folgende sensible Daten von Ihnen aufgrund unseres Beratungsvertrages bzw des Psychotherapiegesetz verarbeite.

|  |  |  |
| --- | --- | --- |
| Betroffene Personengruppen: | Nr.: | Datenarten (samt Historie): |
| KlientInnen | 01 | Klientennummer, Protokollnummer |
| 02 | Namen, frühere Namen (Namensteile) |
| 03 | Anschrift |
| 04 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben |
| 05 | Geburtsdatum, Geburtsort |
| 06 | Staatsangehörigkeit |
| 07 | Geschlecht |
| 08 | Buchhaltungsunterlagen |
| 09 | Sozialversicherungsträger |
| 10 | Sonstige Daten zur Sozialversicherung (insbesondere der Name, das Geburtsdatum und die Sozialversicherungsnummer des Hauptversicherten sowie das Verwandtschaftsverhältnis zum Hauptversicherten bei mitversicherten Patienten/Klienten ) |
| 11 | Vorgeschichte der Problematik und der allfälligen Erkrankung sowie die bisherigen Diagnosen und den bisherigen Krankheitsverlauf, |
| 15 | Beginn, Verlauf und Beendigung der psychotherapeutischen Leistungen, |
| 16 | Art und Umfang der diagnostischen Leistungen, der beratenden oder behandelnden Interventionsformen sowie Ergebnisse einer allfälligen Evaluierung, |
| 17 | vereinbartes Honorar und sonstige weitere Vereinbarungen aus dem Behandlungsvertrag |
| 18 | erfolgte Aufklärungsschritte und nachweisliche Informationen, |
| 19 | Konsultationen von Berufsangehörigen oder anderen Gesundheitsberufen, |
| 20 | Übermittlung von Daten und Informationen an Dritte, insbesondere an Krankenversicherungsträger, |
| 21 | allfällige Empfehlungen zu ergänzenden ärztlichen, klinisch-psychologischen, gesundheitspsychologischen oder musiktherapeutischen Leistungen oder anderen Abklärungen, |
| 22 | Einsichtnahmen in die Dokumentation sowie |
| 23 | Begründung der Verweigerungen der Einsichtnahme in die Dokumentation. |
| Kontaktperson (nach Angabe des Klienten oder gesetzlicher Vertreter des Klienten : | 26 | Name |
| 27 | Anschrift |
| 28 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben |
| 29 | Zustimmung des gesetzlichen Vertreters zur Behandlung |
| 30 | Keine Zustimmung des gesetzlichen Vertreters notwendig |

**Die Höchstdauer der zulässigen Datenaufbewahrung beträgt:**

Die Daten der Patienten/Klienten sind gemäß §16a (3) Dokumentationsplicht Psychotherapiegesetz 1990 zehn Jahre aufzubewahren. Weiters ist es zulässig, alle Daten bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden, aufzubewahren.

**Ich verwende Ihre Daten für folgende Zwecke:**

* Führung und Pflege von Klientenkarteien zur Dokumentation gemäß §16a (3) Dokumentationsplicht Psychotherapiegesetz 1990
* Erstellung von medizinischen Gutachten und Honorarverrechnung durch Therapeuten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenz) in diesen Angelegenheiten zur Erfüllung des Behandlungsvertrages

**Ihre Daten werden an folgende Empfänger weitergeleitet:**

|  |  |
| --- | --- |
| **Rechtsgrundlage** | **Empfängerkategorien** |
| gesetzlich | Sozialversicherungsträger (einschließlich Betriebskrankenkassen), MA11 und sonstige Kostenträger im Rahmen ihrer rechtlichen Befugnisse auf Grund von Gesetzen oder Sozialversicherungsabkommen; |
| gesetzlich | Auftraggeber von Gutachten, soweit die rechtlichen Voraussetzungen für die Erstellung des Gutachtens vorliegen; |
| Nur im Anlassfall (gesetzl. Regelung bzw. Einwilligung des Klienten) | Mit der Rechtsdurchsetzung, Streitschlichtung und Klärung von Beschwerden der Patienten/Klienten und Abrechnungsansprüchen (des Auftraggebers) betraute Stellen, insbesondere Rechtsanwälte, Gerichte, Schlichtungsstellen und Patientenanwälte, |
| Im Falle der Karenz,Pensionierung, Arbeitsunfähigkeit oder Todesdes Therapeut/in | ist der Erbe oder sonstige Rechtsnachfolger unter Wahrung des Datenschutzes verpflichtet, die Dokumentation für die der Aufbewahrungspflicht entsprechende Dauer gegen Kostenersatz 1. einem genannten Berufsangehörigen, der in diese Benennung und Pflichtenübernahme schriftlich eingewilligt hat, andernfalls2. vom Bundesministerium für Gesundheit zu bestimmenden Dritten zu übermitteln. |

**Die Weiterleitung an folgende Empfängern bedarf der
Einwilligung des Klienten/in durch Ankreuzen:**

|  |  |
| --- | --- |
| Bitte ankreuzen | Privatversicherungen zum Zweck der Abwicklung des Versicherungsanspruches |
| Bitte ankreuzen | Die Abrechnung mit der Privatversicherung übernimmt der Klient/In selber und erhält die dafür notwendigen Unterlagen |
| Bitte ankreuzen | Ärzte, Vertreter von sonstigen Gesundheitsberufen und medizinische oder soziale Einrichtungen, sowie nicht-ärztliche Gesundheitsberufe in deren Behandlung der Patient steht oder überwiesen wird.  |
| Bitte ankreuzen | *Bitte hier Ihren Honorar-Abrechnungs-Verein eintragen* |

**Ich habe den Klienten/in darauf hingewiesen worden, dass**

* wenn er/sie die Daten nicht an meinen Honorar-Abrechnungs-Verein weiterleiten will und die Therapie auch nicht von einer Sozialversicherung übernommen wird, er/sie die Therapie privat zu bezahlen hat.
* die im Rahmen der vorstehenden genannten Zweck erhobenen persönlichen Daten unter Beachtung des DSGVO und des DSG erhoben, verarbeitet, genutzt und nur sicher sowie verschlüsselt übermittelt werden.
* die Erhebung, Verarbeitung und Nutzung der Daten auf freiwilliger Basis erfolgt und dass der Klient/in sein/ihr Einverständnis verweigern oder jederzeit mit Wirkung für die Zukunft widerrufen kann
* er/sie jederzeit berechtigt ist kostenfrei Einsicht in die Dokumentation über die zu seiner/ihrer Person gespeicherten Daten oder einmalig die Herstellung von Abschriften zu verlangen, soweit diese das Vertrauensverhältnis zwischen mir als Therapeuten/in und ihm/ihr als Klient/in nicht gefährden. (§ 16a. (2) Psychotherapiegesetz 1990)
* sie/er jederzeit berechtigt ist, die Berichtigung, Löschung oder Einschränkung einzelner personenbezogener Daten zu verlangen.
* seine/ihre Daten vollständig anonymisiert für wissenschaftliche Zwecke verwendet werden können.
* sie/er im Falle der Einsicht, des Widerrufes oder der Löschung dies als Antrag schriftlich bzw. per Email an mich *Name, Adresse* zu richten hat
* ich ihm/ihr den Aushang „Datenschutzerklärung“ ebenso zur Kenntnis gebracht habe.

Im Falle des Widerrufes oder Antrag auf Löschung werden die pB Daten mit dem Zugang der Willenserklärung gelöscht und nur

* Daten aus dem Behandlungsvertrag, die für eine ordnungsgemäße Buchhaltung aufgrund der gesetzlichen Aufbewahrungsfristen notwendig sind, sicher für 7 Jahre aufbewahrt und dann gelöscht.
* die sensiblen Daten werden gemäß §16a (3) Dokumentationspflicht Psychotherapiegesetz 1990 an einem sicheren Ort - getrennt von den Buchhaltungsunterlagen – archiviert und nach Ablauf der gesetzlicher Fristen von 10 Jahren dann endgültig gelöscht
* vollständig anonymisiert für wissenschaftliche Zwecke verwendet werden

Ich werde den Widerruf an die o. g. Dritten weiterleiten, die ihrerseits dann die Daten löschen, ausdrücklich ausgenommen davon sind die Sozialversicherungen\*.

*\*Die Löschung seiner Daten bei der Sozialversicherung muss der Klient von sich aus beantragen, da möglicherweise alle auf Grundlage dieser Daten von den Sozialversicherungen bisher erbrachten Leistungen der Sozialversicherung binnen vier Wochen ab Tilgung der Daten vom Antragsteller zurückzuzahlen sind.*

Diese Informationsblatt wurde der/m Klienten/in: ………………...Name………………

am ………………………… in meiner Praxis vorgelegt, besprochen und wird im Archiv abgelegt.

Auf Wunsch des Klienten ist eine Kopie zu übergeben

## Muster Datenschutzverletzung (WKO) an Behörde bzw Betroffene

**Datenschutzverletzung**

Art 33 EU-Datenschutzgrund-Verordnung (DSGVO) -

Meldung an die Aufsichtsbehörde:

Österreichische Datenschutzbehörde,

Hohenstaufengasse 3, 1010 Wien

E-Mail:dsb@dsb.gv.at

1. Name und Kontaktdaten des **Verantwortlichen:**
	1. **Name und Anschrift:**

|  |
| --- |
|  *Titel / Vor-und Zuname* |
|  *Straße PLZ-Ort* |
|  |

* 1. **E-Mail-Adresse, Tel.Nr.:**

|  |
| --- |
| *Email: …………...@…………………….* |
| Tel |

**2.** Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

|  |
| --- |
|  |
|  |
|  |

 a. soweit möglich Kategorien und ungefähre Zahl der **betroffenen Personen**:

|  |
| --- |
|  |
|  |
|  |

 b. soweit möglich betroffene Kategorien und ungefähre Zahl der personenbezogenen Datensätze:

|  |
| --- |
|  |
|  |
|  |

**3.** Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten aufgrund einer Risikoanalyse:

|  |
| --- |
|  |
|  |
|  |

**4.** Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

|  |
| --- |
| Siehe TOMs |
|  |
|  |
|  |

1. ggf **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

|  |
| --- |
|  |
|  |
|  |
|  |

**5**. **Datum und Uhrzeit** des Vorfalls:

|  |
| --- |
|  |
|  |
|  |

**□ Begründung**, falls die Meldung länger als 72h nach dem Vorfall erfolgte:

|  |
| --- |
|  |
|  |
|  |

Wien, am ………………….

…………………………………………………………….
Unterschrift

## Mustervertrag Auftragsverarbeitung (WKO)

**Vereinbarung** **über eine** **Auftragsverarbeitung nach Art 28 DSGVO**

|  |  |  |
| --- | --- | --- |
| Der Verantwortliche: |  | Der Auftragsverarbeiter: |
| *Titel / NameAdressePLZ-OrtEmail* |  | **Siehe Anleitung**[*Anschrift*] |
| (im Folgenden Auftraggeber) |  | (im Folgenden Auftragnehmer) |

### Gegenstand der Vereinbarung

1. Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: [*möglichst detaillierte Beschreibung der Aufgaben des Auftragnehmers, einschließlich Art und Zweck der vorgesehenen Verarbeitung].*

{Falls es einen weitergehenden Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, udgl gibt} Diese Vereinbarung ist als Ergänzung zu [*Vertrag, etc samt Datum ergänzen*] zu verstehen.

1. Folgende Datenkategorien werden verarbeitet: [*Datenkategorien möglichst detailliert aufzählen, zB Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, usw. bzw. als Anhang*.
2. Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung: [*Betroffenenkategorien ergänzen wie zB Klienten, Lieferanten, Ansprechpartner, Kollegen, Beschäftigte, usw.*]

### Dauer der Vereinbarung

**□** {Einmalige Durchführung} Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten.

**□** {Befristete Laufzeit} Die Vereinbarung ist befristet abgeschlossen und endet mit [*Fristende eintragen*]

**□** {Unbefristete Laufzeit} Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von [*Kündigungsfrist eintragen, zB ein Monat*] zum [*Kündigungstermin eintragen, zB Kalenderviertaljahr*] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

### Pflichten des Auftragnehmers

1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.
2. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.
4. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
5. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
6. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
8. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
9. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

### Ort der Durchführung der Datenverarbeitung

**X** Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

### Sub-Auftragsverarbeiter

**X** Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

|  |  |  |
| --- | --- | --- |
| Wien am [*Datum*] |  | [*Ort*], am [*Datum*] |
| *Für den Auftraggeber:* |  | *Für den Auftragnehmer:* |
| ...................................................*Titel / Name* |  | ....................................................[*Name samt Funktion*] |

## Vorlage: Fernwartung und Pflege von IT-Systemen & Datenschutz

Bei der (Fern-) Wartung und Pflege von IT-Systemen ist auch das Thema Datenschutz zu berücksichtigen. Hintergrund hierfür ist, dass auch bei der Wartung oder Pflege von IT-Systemen eine „Verarbeitung“ von personenbezogenen Daten im Auftrag vorliegen kann.

Und dazu stelle RA Stephan Hansen-Oest kostenfrei nachfolgendes Muster auf Basis der DSGVO zur Verfügung. Das Muster ist so gestaltet, dass es eine gute Ausgangsgrundlage für gängige Fälle von Wartungen von IT-Systemen sein sollte.

Das bedeutet natürlich für den Auftraggeber, nicht, dass man den Auftragnehmer nicht sorgfältig vor der Beauftragung prüfen sollte. RA Stephan Hansen-Oest kann gerade im Bereich der IT-Dienstleister nur empfehlen, mal genauer hinzuschauen, wie der Dienstleister im Bereich der Datensicherheit so aufgestellt ist. Schließlich erhält der Dienstleister ggf. Zugangsdaten zu IT-Systemen des Auftraggebers. Und diese sind besonders gesichert zu verwahren.

[***https://www.datenschutz-guru.de/wartungsvertrag/***](https://www.datenschutz-guru.de/wartungsvertrag/)

## Zusatz Verzeichnis: Kundenbetreuung und Kommunikation

Diese Verzeichnis bitte nur in Ihr Datenschutzkonzept aufnehmen, wenn Sie Newsletter versenden wollen!

Verantwortliche(r)

Name
Adresse
Email
Tel:
Zweck
Als Psychotherapeut/in unter der Verpflichtung, bei Werbung und Ankündigungen in der Öffentlichkeit fachlichen Gesichtspunkten strikt den Vorrang vor kommerziellen Gesichtspunkten einzuräumen, ist der Zweck der Werbung oder Ankündigungen zB per Newsletter auf das sachlich Gebotene beschränkt. Daher beinhalten meine Newsletter und Ankündigungen nur ausreichende Information über Art und Umfang der angebotenen Leistungen (Supervision, Coaching, Teamberatung,  Workshops, Seminare, Fort- und Weiterbildung, … ;sowie Veranstaltungen, für die die Teilnehmer Fort-/Weiterbildungs-Bestätigungen bekommen) sowie über die geforderten Entgelte und die Rechte der Klienten bzw Aus-/Fortzubildenden und dies nur insoweit ich als Psychotherapeut/in die dafür notwendige (Zusatz) Qualifikation und Kompetenz erworben habe.

Ausdrücklich enthalten meine Newsletter zB keine Werbung für gewerbliche Produkte wie zB Bücher, Videos, DVDs, … und gewerbliche Dienstleistungen oder gewerbliche Veranstaltungen und sind von der Anzahl der Aussendungen auf das aller Notwendigste begrenzt.

Die kommerziellen Informationen können über Ihren Verband/Verein kommuniziert werden.
Kategorien der betroffenen Personen

|  |  |
| --- | --- |
| Lfd. Nr. | Beschreibung der Kategorien betroffener Personen |
| 1 | Klienten, Aus-/Fortzubildende und Interessenten |
| 2 | Kontaktpersonen beim Klienten, Aus-/Fortzubildenen und Interessierten |

Rechtsgrundlagen

* Newsletter + Fotos: Art 6 Z 1 lit a (Einwilligung der Betroffenen)
* Ansonsten: Art: 6 Z 1 lit b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen)
* 151 GewO 1994
* Psychotherapiegesetz
* Telekommunikationsgesetzes
* [Berufskodex für Psychotherapeutinnen und Psychotherapeuten](https://www.sfu.ac.at/wp-content/uploads/berufskodex_fuer_psychotherapeutinnen.pdf)
* „SA022 Kundenbetreuung und Marketing für eigene Zwecke“ siehe Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: [II Nr. 312/2004](https://www.ris.bka.gv.at/eli/bgbl/II/2004/312)
* [Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV), BGBl. II Nr. 108/2018](https://www.ris.bka.gv.at/eli/bgbl/II/2018/108/20180525)
somit keine Folgeabschätzung für diese Verarbeitung notwendig

Verträge, Zustimmungserklärungen oder sonstige Unterlagen
Zustimmungserklärungen bzw. Verträge sowie Verträge mit Auftragsverarbeitern usw. sind im Archiv abgelegt.
Kategorien der verarbeiteten Daten

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Kategorien derbetroffenenPersonengruppe | Lfd.  Nr.: | Datenkategorien | Besondere Datenkategorien im Sinne der Art 9 und Art 10 DSGVO | Rechtsvertreterim Anlassfall | Gerichtim Anlassfall | ExternesNewsletter-Toll |
| 1. Klienten, Aus-/Fortzubildende und Interessenten | 01 | Ordnungs-/Klienten-/Auszubildendennummer | Nein | X | X |   |
| 02 | Name bzw. Bezeichnung | Nein | X | X | X |
| 03 | Anrede/Geschlecht | Nein | X | X | X |
| 04 | Anschrift bzw. Lieferadresse | Nein | X | X |   |
| 05 | Telefon-, Handy-, Faxnummer, Emails, | Nein | X | X | Email |
| 06 | IP-Adressse | Nein | X | X |   |
| 07 | Einwilligung nach Art 4 abgelegt | Nein | X | X |   |
| 08 | Berufs-, Branchen-  Geschäftsbezeichnung | Nein | X | X |   |
| 09 | Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Kunden gegenüber dem Auftraggeber) | Nein | X | X |   |
| 10 | Art der Leistung | Nein | X | X |   |
| 11 | Umfang der Leistung | Nein | X | X |   |
| 12 | Gefordertes Entgelt | Nein | X | X |   |
| 13 | Rechte der Klienten bzw Aus-/Fortzubildenden | Nein | X | X |   |
| 14 |  Newsletter-Sperre | Nein | X | X |   |
| 15 | Auftragssperre= Recht auf Einschränkung geltend gemacht | Nein | X | X |   |
| 16 | Fotos | Nein | X | X |   |
| Kontaktpersonen bei Klienten, Aus-/Fortzubildende und Interessenten | 17 | Ordnungs-/Klienten-/Auszubildendennumme | Nein | X | X |   |
| 18 | Name bzw. Bezeichnung, | Nein | X | X | X |
| 19 | Anrede/Geschlecht | Nein | X | X | X |
| 20 | Zugehöriger Kunde oder Interessent (Bezeichnung und Anschrift) | Nein | X | X |   |
| 21 | Telefon-, Handy-, Faxnummer, Emails, … | Nein | X | X | Email |
| 22 | Funktion oder betreutes Aufgabengebiet beim Kunden oder Interessenten | Nein | X | X |   |
| 23 | IP-Adressse | Nein | X | X |   |
| 24 | Einwilligung nach Art 4 abgelegt | Nein | X | X |   |
| 25 | Berufs-, Branchen-  Geschäftsbezeichnung | Nein | X | X |   |
| 26 | Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Kunden gegenüber dem Auftraggeber) | Nein | X | X |   |
| 27 | Art der Leistung | Nein | X | X |   |
| 28 | Umfang der Leistung | Nein | X | X |   |
| 29 | Gefordertes Entgelt | Nein | X | X |  |
| 30 | Rechte der Klienten bzw Aus-/Fortzubildenden | Nein | X | X |  |
| 31 |  Newsletter-Sperre | Nein | X | X |  |
| 32 | Auftragssperre= Recht auf Einschränkung geltend gemacht | Nein | X | X |  |
| 33 | Fotos | Nein | X | X |  |

Löschungs- und Aufbewahrungsfristen

|  |  |
| --- | --- |
| Daten (Lfd. Nr.) | Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen |
| 1 –  33 | Bei einem bestehenden oder abgeschlossenem Vertrag aufgrund der gesetzlichen Aufbewahrungsfristen wie z. B. § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüberhinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen |
| Interessenten | 2 Jahre nach letztem Kontakt (-versuch) |
| Newsletter, Fotos | Recht auf Widerspruch (Art 21 DSGVO) |
| IP-Adresse | Zu eigenen Sicherheitszwecken:Speicherfrist von maximal 7 Tagen(siehe Datenschutzerklärung auf Homepage) |

Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

|  |  |  |
| --- | --- | --- |
| Empfängerkategorien | Drittstaat(d.h. Staaten außerhalb der EU) | Internationale Organisation |
| 1.Rechtsvertreter im Anlassfall | Nein | Nein |
| 2.Gericht im Anlassfall | Nein | Nein |
| 3. Externer Newsletter-Tool-Anbieter | ? | Nein |
|  |  |  |

Es erfolgt keine Übermittlung an Drittstaaten,
wenn Sie es mit Ihrem Emailprogramm selber machen,

Ansonsten schauen Sie bitte im Vertrag mit dem Newsletter-Tool-Anbieter nach (siehe Pkt. 4) Eine sehr gute Liste der DSGVO-konformen Newsletter-Tool-Anbieter findet Sie hier: <https://www.blogmojo.de/adv-vertraege/>, die Ihnen auch gleich Datenverarbeitungsverträge zum Downloaden fürs Archiv anbieten,

#### zusätzliche TOMs: E-Mail-Marketing – Recht auf Widerspruch (Art 21 DSGVO)

Vorab beachte ich Name des Verantwortlichen  die sogenannte Robinson-Liste und setzte ein Hackerl bei „Keine Zusendungen von Werbematerial, Newsletter erwünscht“ für alle natürlichen und juristischen Personen, die in dieser Liste ausdrücklich auf die Zusendung von Werbematerial sowie Werbemails verzichten, siehe <https://www.rtr.at/de/tk/TKKS_ECGListe>
Referenz: [§ 7 E-Commerce-Gesetz (ECG)](https://www.rtr.at/de/tk/WeitereGesetze)

Die Newsletter-Abonnenten, die ihre klare Einwilligung nach Art 4 DSGVO nachweislich abgegeben haben, werden hinreichend sowohl über Zweck, Art und Umfang der Datenverarbeitung als auch über ihre Rechte als Betroffene wie Recht auf Information, auf Auskunft und Richtigstellung, Widerspruchsrecht, auf Löschung und Einschränkung im E-Mail-Newsletter informiert.
Darüber hinaus gibt es in jedem E-Mail-Newsletter die einfache und rasche Möglichkeit für den Betroffenen, sich vom E-Mail-Newsletter abzumelden (mit einem automatisierten Email, dass er von der Newsletter-Liste gelöscht wurde) und einen Hinweis auf meine Datenschutzerklärung als Link.

Sollte dieses Mail-Newsletter-Tool von einem Dritten bereitgestellt sein, so gibt es dazu eine Vereinbarung mit diesem Auftragsverarbeiter nach Art 28 DSGVO.

Individuelles Tracking der Newsletter, auch über eine Übermittlungs- bzw. Lesebestätigung, wird nicht gemacht, da dafür eine eigene Einwilligungserklärung notwendig ist.

Macht ein Betroffener seine Rechte auf Widerspruch nicht mit Hilfe des Links im Newsletter geltend, sondern in einer anderen Form, sei es z. B. mündlich, schriftlich. per Email (insbesondere datenschutz@………..) so gilt folgendes:

Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:

„Sehr geehrte Frau/Herr …… !
Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie z. B. personenbezogen Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zukommen zu lassen. Der Scann/Kopie wird sogleich nach Identitätsfeststellung gelöscht.
Ich danke Ihnen für Ihr Verständnis“

* Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits sind notwendig.
* Identität zweifelsfrei festgestellt und Verlangen ist rechtens
=> Der Betroffene bekommt betreffs Recht auf Widerspruch (Art 15 DSGVO) ehest möglich folgende Antworten:„Sehr geehrte Frau/Herr ……!
Gemäß Ihrem Wunsch habe ich Sie hiermit von der Newsletter-Verteiler-Liste gelöscht. Sie erhalten keinen Newsletter oder Werbezusendungen von mir mehr.“

Referenzen: Art 4, Art 8, Art 9 DSGVO; Erwägungsgründe: 26ff, 51ff; § 4 Abs 4 DSG 2018; Recht auf Widerspruch Art 21 DSGVO

## Muster: Einwilligungserklärung für Newsletter

Zweck: Als Psychotherapeut/in unter der Verpflichtung, bei Werbung und Ankündigungen in der Öffentlichkeit fachlichen Gesichtspunkten strikt den Vorrang vor kommerziellen Gesichtspunkten einzuräumen, ist der Zweck der Werbung oder Ankündigungen zB per Newsletter auf das sachlich Gebotene beschränkt. Daher beinhalten meine Newsletter und Ankündigungen nur ausreichende Information über Art und Umfang der angebotenen Leistungen (Therapie, Supervision, Coaching, Teamberatung, Workshops, Seminare, Fort- und Weiterbildung,…und Veranstaltungen, für die die Teilnehmer Fort-/Weiterbildungs-Bestätigungen bekommen) sowie über die geforderten Entgelte und die Rechte der Klienten bzw Aus-/Fortzubildenden.

Vorab zur werten Kenntnisnahme meine Datenschutzerklärung: www. …homepage…at /datenschutz

*Hinweise:*
Ihre E-Mail-Adresse wird nur für den Zweck der Erbringung dieses Newsletters verwendet. Ihre E-Mail-Adresse wird aber niemals für Werbezwecke an Dritte weitergegeben.

Ja, ich stimme dem Erhalt eines E-Mail Newsletters von (Psychotherapeut/in) gesendet an folgende

E-Mail-Adresse: ………………….

und Namen: ………………………..

zu. Ich kann diese Einwilligung jederzeit per Email (Ihr Email) und auch bei jedem Erhalt des Newsletters direkt dort und einfach widerrufen (Recht auf Widerspruch - Art 21 DSGVO).

Ihr Name/Anschritft/Email als Verantwortliche/r

## Muster: Auskunftserteilung

Sehr geehrte/r Frau/Herr …….!

Gemäß Ihrer Anfrage vom …………………… erteilen wir Ihnen hiermit Auskunft über:

* den Zwecke und Rechtsgrundlagen der Datenverarbeitung:

* die personenbezogener Daten von Ihnen, die ich/wir verarbeite/n:

* die Empfänger/Empfängerkreise:

* die Dauer der Speicherung:

* die Herkunft der Daten (falls nicht bei der Person erhoben):

* Eine automatisierten Entscheidungsfindung/Profiling findet nicht statt.
* Sie haben das Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung der Daten sowie ein Widerspruchsrecht gegen die Verarbeitung der Daten und das Recht auf Datenübertragbarkeit. Sie haben das Recht auf Beschwerde bei der Aufsichtsbehörde.

Betreffs dem Verzeichnis „Klientenverwaltung und Dokumentation“ gilt das Recht auf Auskunft (Art 15 DSGVO) nur in Verbindung mit Recht auf Einsicht gemäß §16a (2) Psychotherapiegesetz: „Dem Behandelten oder seinem gesetzlichen Vertreter sind unter besonderer Bedachtnahme auf die therapeutische Beziehung auf Verlangen alle Auskünfte über die gemäß Abs.1 geführte Dokumentation sowie Einsicht in die Dokumentation zu gewähren oder gegen Kostenersatz die Herstellung von Abschriften zu ermöglichen, soweit diese das Vertrauensverhältnis zum Behandelten nicht gefährden.“

Ihre Kontaktdaten als Verantwortliche/r

## Muster: Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO)

|  |
| --- |
| Diese Verpflichtungserklärung betrifft: |
| **Familienname:** |  |
| **Vornamen:** |  |

In Ausübung Ihrer beruflichen Tätigkeit bzw. Ausbildung zB als Praktikant/in erhalten Sie voraussichtlich Kenntnis über teilweise sehr sensible personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse. Alle diese Informationen sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen und europäischen Datenschutzrechts sowie des Wettbewerbsrechts.

Mit Ihrer Unterschrift verpflichten Sie sich,

1. das Datenschutzrecht zu wahren, insbesondere § 6 DSG, einschließlich entsprechender betrieblicher Anordnungen;
2. Geschäfts- und Betriebsgeheimnisse zu wahren (§ 11 UWG);
3. bei einem Verstoß gegen das Datengeheimnis oder eine Verletzung von Geschäfts- und Betriebsgeheimnissen, Schadenersatz zu leisten, und zwar ohne Rücksicht auf den tatsächlich eingetretenen Schaden durch Vereinbarung einer Konventionalstrafe pauschaliert, und zwar im Ausmaß von 3-fachen Bruttomonatsentgelten/Kooperationsvereinbarung/Werkvertrag/ oder x.000,- Euro

Die zitierten Bestimmungen sind im Anhang zu dieser Erklärung abgedruckt.

Ihnen ist bekannt, dass

* die personenbezogenen Daten natürlicher wie juristischer Personen einem besonderen Schutz unterliegen und die Verwendung solcher Daten nur unter besonderen Voraussetzungen zulässig ist;
* personenbezogene Daten, die Ihnen auf Grund Ihrer beruflichen Beschäftigung anvertraut oder zugänglich gemacht wurden, nur auf Grund einer ausdrücklichen Anordnung des jeweiligen Vorgesetzten übermittelt werden dürfen;
* es untersagt ist, Daten an unbefugte Empfänger innerhalb und außerhalb des Unternehmens zu übermitteln oder sonst zugänglich zu machen;
* es untersagt ist, sich unbefugt Daten zu beschaffen oder zu verarbeiten;
* es untersagt ist, personenbezogene Daten zu einem anderen als dem zum rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden;
* anvertraute Benutzerkennwörter, Passwörter und sonstige Zugangsberechtigungen sorgfältig verwahrt und geheim zu halten sind;
* allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten ebenfalls zu beachten sind;
* diese Verpflichtung auch nach Beendigung Ihrer Tätigkeit fortbesteht;
* Verstöße gegen die hier genannten Verschwiegenheitsverpflichtungen nicht nur arbeitsrechtliche Folgen, sondern auch (verwaltungs-)strafrechtliche Folgen haben und schadenersatzpflichtig machen.

Hiermit erkläre ich, am [Datum der Belehrung] von [Titel / Name Therapeut/in ] über das Datengeheimnis nach § 6 DSG und die Verschwiegenheitsverpflichtungen nach § 11 UWG belehrt worden zu sein.

|  |  |  |
| --- | --- | --- |
| **Ort, Datum** |  | **Unterschrift des Verpflichteten** |

### Anhang zum Datengeheimnis

**Datengeheimnis nach § 6 DSG**

**(1)** Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Daten­ver­arbei­tungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personen­bezogenen Daten besteht (Datengeheimnis).

**(2)** Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienst­ver­hältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

**(3)** Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

**(4)** Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

**(5)** Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussage­ver­weiger­ungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

**Verletzung von Geschäfts- oder Betriebsgeheimnissen und Missbrauch
anvertrauter Vorlagen nach § 11 UWG**

**(1)** Wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (BGBl. Nr. 120/1980, Art. I Z 6)

**(2)** Die gleiche Strafe trifft den, der Geschäfts- oder Betriebsgeheimnisse, deren Kennt­nis er durch eine der im Abs. 1 bezeichneten Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt.

**(3)** Die Verfolgung findet nur auf Verlangen des Verletzten statt.

1. *Die Verarbeitung personenbezogener Daten soll nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes (Psychotherapeuten) oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz- Folgenabschätzung nicht zwingend vorgeschrieben sein (Erwägungen 91).* [↑](#footnote-ref-2)