Anleitung zum Erarbeiten eines
Datenschutzkonzeptes nach DSGVO
Für die Einzelpraxis eines Therapeuten/in

|  |
| --- |
| Dies ist die Anleitung als PDF |
| Die Vorlage zum Ausfüllen finden Sie hier: [www.dataprivacydoctors.at/vorlagen/](http://www.dataprivacydoctors.at/vorlagen/)  |

Stand des Dokuments: 22.06.2018

# Datenschutz ist ein Prozess

Vieles betreffs der DSGVO ist unklar und es gibt viele unterschiedliche, auch juristische Meinungen zu einzelnen Punkten, aber vor allem gibt es noch keine letztinstanzliche Gerichtsentscheidungen, die strittige Fragen klären könnten und fast jedes Monat gibt es neue Erkenntnisse, Verordnungen, Gesetze, Urteile usw. zur DSGVO.

Die personenbezogen Daten Ihrer Klienten dürfen Sie aufgrund des Beratungsvertrages verarbeiten, die Dokumentation der pb Daten müssen Sie aufgrund eines Gesetzes machen. Übertragen dürfen Sie die pb Daten aufgrund gesetzlicher Regelung oder weil es zur Vertragserfüllung notwendig ist. Die einzigen Einwilligungen, die Sie brauchen finden Sie im Anhang der Vorlage „7.1.Informationsblatt über sensible Daten (Art 9 DSGVO)“ bzw wenn Sie Newsletter versenden wollen auch im Anhang.

Wir, Christopher Temt und Michael Werzowa, bemühen uns als Autoren all diese Änderungen ein zu arbeiten. Sollte sich daher etwas betreffs der DSGVO ändern, so würden wir Ihnen gerne die dafür notwendigen Ergänzungen, Änderungen oder Streichungen in Ihrem Datenschutzkonzept per Email zukommen lassen. Nutzen Sie dieses unentgeltliche Service, halten Sie Ihr Datenschutzkonzept aktuell und melden Sie sich bitte bei unserem Newsletter an, siehe <https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung>

Im weiteren die notwendigen Schritte, um als Therapeut/in einen **ersten Entwurf** für eine DSGVO-konforme Dokumentation erstellen zu können.

Der Besuch von DSGVO-Workshops und/oder die **Beiziehung eines Datenschutz-Beraters** (ct@dataprivacydoctors.at ) **IT-Experten** (mw@dataprivacydoctors.at) und möglicherweise auch eines Rechtsanwaltes **um die Dokumentation und die TOMs fertig zu stellen, wird angeraten.**

Wir danken Ihnen für Ihr Verständnis
*Christopher Temt und Michael Werzowa*

*P.S.: Lesen Sie bitte unbedingt den Disclaimer auf der letzten Seite.*

## Deckblatt und allgemeiner Teil

* Bitte die gelb markierten Felder mit Ihren Daten ersetzen
* Disclaimer löschen
* Wenn fertig, Inhaltsverzeichnis erstellen
* Regelmäßige Weiterbildung m Bereich des Datenschutzes ist anzuraten
* Bei allen Punkten, die noch nicht geklärt sind, es unterschiedliche Meinungen bzw. Ansätze gibt oder wir noch auf Klarstellung seitens der Datenschutzbehörde warte, haben wir [**Newsletter**](https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung)dazu geschrieben, so dass wir Sie über Änderungen informieren können.

## Sichere und verschlüsselte Kommunikation

Die **Übertragung** von sensiblen Informationen iSd Art 8, Art 9 und Art 10 DSGVO muss **ausnahmslos sicher und verschlüsselt** erfolgen. Auch die Kommunikation mit Klienten nicht nur in der Praxis sondern heutzutage auch über Telefon, SMS, ... bzw. bei Datenübertragung (Gutachten , ...) soll **sicher und vertraulich gestaltet** sein.

Es gibt mehrere sehr gute und vertrauenswürdige Anbieter von verschlüsselten und sicheren Kommunikations-Apps, wie zB telegram, wire oder signal.Wir verwenden schon seit Jahren [www.signal.org](http://www.signal.org/) sowohl auf unseren Handys als auch auf unseren Desktops und sind zufrieden damit, aber die anderen Anbieter sind sicher genauso gut – **Ihre Wahl!**

Mehr zu signal.org: <https://support.signal.org/hc/en-us/articles/212477768-Is-it-private-Can-I-trust-it-> Da [www.signal.org](http://www.signal.org/) keinen Zugang zu den gesendeten Daten, SMS und Gesprächen hat und ebenso nicht zu den Telefonnummern, werden keine pb Daten an signal.org übertragen und es bedarf daher auch keiner Vereinbarung gemäß Art 28 DSGVO Sollte die Datenschutzbehörde zu einer anderen Meinung gelangen, siehe [**Newsletter**](https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung).

## Rechnungswesen und Geschäftsabwicklung:

### Kategorien der verarbeiten Daten

* Die Datenkategorien decken die üblichen Daten betreffs Rechnungswesen ab und können so verwendet werden.
* Sollten Sie aber in der Praxis noch zusätzlich verwenden, so geben Sie sie hier dazu oder wenn Sie bestimmte Daten nicht benötigt, einfach die entsprechende Zeile löschen.
* Wie Sie sehen können, haben wir die Empfänger **9**-Provider/Hoster/IT-Dienstleister/Software-Anbieter (mit Fernwartung), …. nicht in der rechten Spalte eingetragen, da wir nicht wissen können, welche Daten genau übermittelt werden.

**ABER,** da Sie mit diesen Dienstleistern eine Vereinbarung gemäß Art 28 (siehe Anhang) abschließen müssen, werden die übertragen Daten dort am Besten **vom Dienstleister selber aufgelistet,** denn die Dienstleister wissen genau, welche Daten sie von Ihnen erhalten, und Sie können dann die Empfänger 9 ganz am Schluss bei den entsprechenden Daten in der rechten Spalte und unten bei der Kategorie der Empfängern eintragen. Viele bieten schon vorgefertige Verträge zum Downloaden an.

### Kategorien der Empfänger

* + Falls Sie Fernwartung Ihres Computer zulassen, so müssen Sie es hier dokumentieren. Den notwendigen Vertrag dafür finden Sie hier, bitte an die österr. Gesetze anpassen: <https://www.datenschutz-guru.de/wartungsvertrag>
	+ Bitte tragen Sie hier das Kommunikations-App ihrer Wahl ein. Die Ziffer 10 müssen Sie aber in keine Spalte eintragen, da der Datendienst zB signal.org keinen Zugang zu pb Daten hat!

|  |  |  |  |
| --- | --- | --- | --- |
| 10 | Datendienst verschlüsselt und sicher |  | Nein |

### TOMs

* + Ob Sie sensible Daten Ihrer Klienten per eingeschriebenen Brief oder am sichersten per Ident-Brief versenden und ob Sie oder der Empfänger die Kosten tragen soll, liegt bei Ihnen.
	+ Genauso ist es Ihre Entscheidung, ob Sie bei allen Unterlagen, die Sie Ihrer Steuerberatung/Bilanzbuchhaltung schicken, die sensiblen Daten unkenntlich machen/schwärzen. Im Sinne der Datensicherheit und Datenminimierung legen wir es Ihnen nahe (siehe Disclaimer)

## Klientenverwaltung und Dokumentation

**Archivierung**.
Hier können Sie entscheiden ob Sie nach  **x Jahr/ 6 Monate/ 3 Monate / gleich** nach Beendigung der Beratung/Behandlung gemäß § 15 Verschwiegenheit und § 16b Dokumentationspflicht Psychotherapiegesetz, die sensiblen Daten archivieren und so aus Verarbeitung entfernen.

**Kategorien der verarbeiteten Daten**
Entsprechend dem Psychotherapiegesetz und Sie brauchen Sie nicht zu ändern oder zu streichen.

### Spalte: Daten für ArchivierungKreuzen sie die pB Daten an, die sie gemäß dem Psychotherapiegesetz archivieren müssen und die, die Sie darüber hinaus auch archivieren wollen.

### Spalte: Wissenschaft, anonymisiertHier haben wir Ihnen eine erste Anleitung gegeben, welche Daten auf jeden Fall gelöscht bzw anonymisiert werden müssen.Falls Sie die Daten nicht für wissenschaftliche Zwecke verwenden, so löschen Sie diese Spalte.

### Kategorien der Empfänger

|  |  |  |
| --- | --- | --- |
| 5 | Nur mit ausdrücklicher Einwilligung des Klienten | Honorar-Abrechnungs-Verein eintragen*wie zB: Wiener Gesellschaft für psychotherapeutische Versorgung, (Verein) Lustkandlgasse 23/3-4, 1090-Wien* |

### **TOMs**

* Bei Archivierung oder bei **Antrag auf Löschung** der pb Daten seitens des Betroffenen,
	+ werden alle pb Daten gelöscht, ausgenommen sind Daten, die für die Buchhaltung aufgrund der gesetzlichen Aufbewahrungsfrist von 7 Jahre aufbewahrt werden müssen
	+ werden alle für Archivierung angekreuzten sensiblen Daten aus „Klientenverwaltung und Honorarabrechnung“ wie folgt behandelt:

### Prozess-Alternativen

**1. Analog**
Die angekreuzten sensiblen Informationen des betroffenen Klienten aus dieser Verarbeitung „Klientenverwaltung“ werden in ein pdf umgewandelt und ausgedruckt. Das digitalen Daten werden nachher unwiderruflich gelöscht und die Ausdrucke werden getrennt von den Buchhaltungsunterlagen an einem sicheren Ort aufbewahrt.

**2. Digital-Intern**
Die angekreuzten sensiblen Informationen aus dieser Verarbeitung Klientenverwaltung werden verschlüsselt und soweit als technisch möglich pseudonymisiert auf zwei verschiedene Datenträger gespeichert – wenn Sie zwei Datenträger vom gleichen Produzenten kaufen, besteht die Gefahr, dass sie auch (fast) gleichzeitig kaputt gehen - und abschließend von meinem Computer/Laptop unwiderruflich gelöscht. Die Datenträger werden getrennt von den Buchhaltungsunterlagen an einem sicheren Ort für 10 Jahre aufbewahrt.

**3. Digital-Extern**Die angekreuzten sensiblen Informationen aus dieser Verarbeitung Klientenverwaltung werden verschlüsselt und soweit als technisch möglich pseudonymisiert bei einem Anbieter Datentresor für 10 Jahre aufbewahrt. Ein entsprechender Vereinbarung über eine „Auftragsverarbeitung nach Art 28 DSGVO“ wird mit dem Datenverarbeitern abgeschlossen [**Newsletter**](https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung)

**4. Mikroverfilmung**
Die angekreuzten sensiblen Informationen aus dieser Verarbeitung Klientenverwaltung werden auf einem Mikrofilm oder vergleichbarem Medium archiviert und an einem sicheren Ort für 10 Jahre aufbewahrt und dann vollständig anonymisiert für wissenschaftliche Zwecke verwendet. Die Daten auf meinem Computer/Laptop werden unwiderruflich gelöscht. Ein entsprechender Vereinbarung über eine „Auftragsverarbeitung nach Art 28 DSGVO“ wird mit dem Datenverarbeitern abgeschlossen

### Verarbeitungsverzeichnisse Personalwesen

Sollten Sie auch nur einen Mitarbeiter haben, selbst wenn er oder sie nur halbtags oder geringfügig beschäftigt ist, so müssen Sie auch ein Verarbeitungsverzeichnis „Personalwesen“ erstellen. Bitte schicken Sie uns ein Email und Sie bekommen eine Vorlage dafür.

## Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

Bitte gehen Sie die wirklich hilfreiche IT-Checkliste für EPUs unter <https://itsafe.wkoratgeber.at/> durch und Sie können feststellen, ob und wo es Probleme in Ihrem IT-Bereich geben könnte.

### Selbstschutz

Ich versuche mein Such- und Surfverhalten soweit wie möglich „sicher“ zu gestalten und verwende daher zB den europäischen Open Source Browser <https://cliqz.com/> inklusive Ghostery (verhindert und zeigt mir die Trackingversuche) und zB die europäische Suchmaschine: [https://www.startpage.com](https://www.startpage.com/) statt Google .

### Handy

Ich habe ein Handy (für die private Kommunikation und ein Handy ausschließlich) für meine berufliche Kommunikation. Statt WhatsApp verwende ich zB <https://www.signal.org/>

Mein berufliches Handy ist durch 6-stelliges Passwort bzw. Biometrie geschützt. Es gibt die Möglichkeit die Daten „fern zu löschen“ bei Apple, bei anderen Handys bitte Security-App downloaden. Bluetooth-Funktion ist nur beim Autofahren eingeschaltet. WLAN ist abgeschaltet. In öffentliche WLAN-Netze wähle ich mich nicht ein und es gibt auch keine automatische Verbindung mit mir bekannten WLANs. Wenn ich ein neues Handy/Laptop/Computer kaufe, so lasse ich mein altes Handy Laptop/Computer von meinem IT-Fachmann immer vollständig löschen (Vereinbarung gemäß Art 28 DSGVO). Falls ich USB-Sticks verwende, so sind die Daten darauf verschlüsselt und ein Passwort ist notwendig, um auf die Daten zu zugreifen.

Sehen Sie die Absätze Selbstschutz und Handy als Anregung. Bitte beschreiben Sie in der Vorlage bei den TOMs, welchen Selbstschutz Sie treffen und wie Sie konkret mit Ihrem Handy DSGVO-konform umgehen.

### Impressum

* Mit dem [ECG-Service](https://firmen.wko.at/Web/ECGHint.aspx) können Sie mit ein paar Klicks ein rechtlich gültiges Impressum
* Wir raten Ihnen ausdrücklich von http://www…… zu [**http**](https://www/)**s://............** zu wechseln.
* Wenn Ihre Homepage mit WordPress erstellt wurde, so findet Sie oder der Ersteller/Betreiber hier wichtige Tipps: <https://www.blogmojo.de/wordpress-plugins-dsgvo>

### Datenschutzerklärung

Hier finden Sie einen ausgezeichneten, für Sie möglicherweise kostenpflichtigen, Datenschutz-Generator mit dem Sie Ihre Datenschutzerklärung für Ihre **Homepage** erstellen können und ausgedruckt als **Aushang** in Ihrer Praxis verwenden können:

[https://datenschutz-generator.de](https://datenschutz-generator.de/)

### Email

Bitte gebe Sie ab jetzt in allen Ihren Emails unter Ihrem Namen, Adresse usw. auch einen Link zu Ihrer Datenschutzerklärung dazu:
P.S.: Zur werten Kenntnisnahme meine Datenschutzerklärung

### TOMs- Einzelne Maßnahmen

In der Vorlage finden sie eine Excel-ToDo-Liste, eine Liste der Maßnahmen, die Sie umsetzten sollten. Wenn sie eine Maßnahme umsetzen, sollten Sie aus der TOM-Beschreibung einen Fließtext, also ganze Sätze machen, ähnlich wie Ärzte es in ihrer Dokumentation machen, siehe Link: [http://www.aekwien.at/documents/4771581/22586874/DSGVO+Verzeichnis+Muster+EP/c8ddf437-3f23-4020-9b74-278915cc608f](http://www.aekwien.at/documents/4771581/22586874/DSGVO%2BVerzeichnis%2BMuster%2BEP/c8ddf437-3f23-4020-9b74-278915cc608f))

 Am Beispiel der Zugangskontrolle:

### 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 |

Es müssen keine Benutzerrechte vergeben und keine Benutzerprofile erstellt werden, da der Verantwortliche als Einzelpraxis, der einzige ist, der Zugriff auf die pb Daten hat.

Meine Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.

Passwörter werden alle 90 Tage gewechselt. Ausgenommen hiervon sind Passwörter, die über eine Mindestlänge von 32 Zeichen verfügen. Hier ist ein automatischer Passwortwechsel nicht indiziert.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

**Der Vorteil:** Sie sehen mit einem Blick, was Sie schon umgesetzt haben (Fließtext) und was noch zu tun ist (Excel-Liste).

**Erstgespräch**

Wir legen Ihnen als verantwortliche/r Therapeut/in nahe, im Erstgespräch das **Informationsblatt über sensible Daten (Art 9 DSGVO)** (siehe im Anhang der Vorlage) mit dem Klienten gemeinsam durchzugehen, offenen Fragen zu klären, Einwilligungen einholen und darüber aufzuklären, dass die Kommunikation nicht nur in Ihren Räumlichkeiten sondern auch per Telefon, SMS, Email usw. immer nur sicher und vertraulich erfolgen kann. Der Vergleich eines unverschlüsselten Emails mit einer Postkarte mag hilfreich sein. So ein verschlüsseltes Kommunikations-App am Handy zu installieren ist schnell und einfach erledigt

Bitte – auch in Absprache mit IT-Berater bzw Software-Anbieter – umgesetzten TOMs ankreuzen und anderen entfernen

Ein Kontroll- und Verbesserungsprozess sollte mindestens 1x jährlich durchgeführt werden, so auch die DSGVO. Datenschutz ist ein Prozess!

## Prozesse betreffs Betroffenenrechte

**Feststellung der Identität:**

* „Sehr geehrte Frau/Herr …!
Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen, wie zB pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zukommen zu lassen. Diese Kopie werde ich nach Identitätsüberprüfung sogleich löschen.

Ich danke Ihnen für Ihr Verständnis

**oder**
* Das sicherst wäre den Betroffenen zu bitten, seinen Ausweis/Führerschein vor die Handykamera zu halten. Dies mag bei sensiblen Daten nach Art 9 und vor allem bei Erziehungsberechtigten wohl der einzige gangbare Weg sein, die Identität sicher fest zu stellen.

Wir raten Ihnen daher hier **Ihre eigene Risikoanalyse** (siehe dort) zu machen und dann entsprechend Ihrer Einschätzung vorzugehen und dies in der Vorlage zu dokumentieren.

Sollte Ihnen Ihr Programm bessere Möglichkeiten bieten, als die (Stamm) Daten des Betroffenen per Screenshot zu erfassen, so verwenden sie natürlich diesen Weg. Leider können aber die meisten Programme dies (noch) nicht.

## Risikoanalyse

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

Wir haben Ihnen hier eine Teil-Risikoanalyse gemacht.
ABER Sie müssen sie trotzdem für sich noch einmal machen bzw vervollständigen, da es immer vom
konkreten Fall, den individuellen Umständen
UND den gesetzten TOMs abhängig ist!

## Schutzbedarfsanalyse

Meine Vorabanalyse ergab, dass es sich bei folgende pb Daten der Klienten, Auszubildenden, Lieferanten, Geschäftspartner und an der Geschäftsabwicklung mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit vernachlässigbaren bis geringem Schutzbedarf handelt, 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 und auch allgemeine TOMs gemäß DSGVO gesetzt wurden:

*Öffentlich zugängliche Daten, Ordnungsnummer, Name, Firma oder sonstige Geschäftsbezeichnung, Anrede/Geschlecht, Anschrift, Homepage, Kontaktdaten (Tel., Skype, Mail, Fax,), Berufs-, Branchen- und Geschäfts­bezeichnung, Firmenbuchdaten, Kenn-Nummern für Zwecke amtlicher Statistik wie UID-Nummer und Intrastat-Kenn-Nummer, Korrespondenz­sprache, Namen der Kontaktpersonen/Erziehungs­berechtigte, Kontakt­daten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.), Funktion/Rolle der Kontaktperson usw.)*

Weiters ergab meine Vorabanalyse, dass es sich bei folgende pb Daten der Klienten, Lieferanten, Geschäftspartner und an der Geschäftsabwicklung mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit einen **hohen** und **sehr hohen** Schutzbedarf handelt und daher eine erweiterte Risiko-Analyse durchgeführt werden muss.

*Alle Daten gemäß* iSd*Art 8, Art 9 und möglicherweise Art 10 des DSGVO, Personenstand, Geburtsdatum, Bankverbindungen, Kreditkartennummern und -unternehmen, (Behandlungs-) Vertragstext und Korrespondenzen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch und Mitschriften* *und Fotos*

## Risikoanalyse ohne Maßnahmen

Analysieren Sie bitte Ihre Daten und tragen Sie sie in die entsprechenden **Risikokategorien** in die Vorlage ein.

Wir haben schon Kategorie 1+2+3 in die **Risiko-Matrix** eingetragen, die anderen machen Sie bitte gemäß Ihrer Einschätzung (siehe unten Schwere und Eintrittswahrscheinlichkeit) selber!

### Bewertungsmaßstäbe

Hier die Bewertungsmaßstäbe um die Daten in das entsprechende Feld der **Risiko-Matrix** eintragen zu können:

### Schwere:

|  |  |  |  |
| --- | --- | --- | --- |
| **Schwere** | **Auswirkung auf Betroffene** | **Folgen überwinden** | **Beispiele** |
| **Vernachlässigbar** | Nicht betroffen oder nur kleine Unannehmlichkeiten | Unannehmlichkeiten sollten sich beheben lassen | Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, … |
| **Begrenzt** | Wesentliche Unannehmlichkeiten | Unannehmlichkeiten sollten sich – trotz Schwierigkeiten – überwinden lassen | Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, … |
| **Wesentlich** | Wesentliche Folgen | Unannehmlichkeiten sollten sich – trotz großer Schwierigkeiten – überwinden lassen | Kategorien und Klassifizierungen werden bekannt, Missbrauch von Geldern, Vorladungen, Verschlechterung eines Verhältnisses, Weitergabe der Passwörter, Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte, Gerüchte, … |
| **Existenz-gefährdend** | Irreversible Folgen | Irreversible Folgen kaum bzw. nicht überwindbar | **Bekanntwerden zB der Diagnose führen zu finanzielle Not, Kündigung, Familientragödien, Selbstmord, …** und/oder vertrauliche Mitschriften werden Öffentlichkeit bekannt und gefährden Betrieb; Beruf, Identitätsdiebstahl; … langfristige Beschwerden, Tod, … |

### Eintrittswahrscheinlichkeit:

|  |  |  |
| --- | --- | --- |
| **EWK** | **Wahrscheinlichkeit** | **Beispiele** |
| **Vernachlässigbar** | 0-24% Wahrscheinlichkeit | zB Diebstahl von Unterlagen aus einem Safe |
| **Möglich** | 25-69% Wahrscheinlichkeit | Zb gezielter und koordinierter Angriff durch einen Hacker, Verlust des Hardware bzw pb Daten durch Diebstahl oder durch fahrlässiges Handeln |
| **Sehr wahrscheinlich** | 70-99% Wahrscheinlichkeit | zB Eindringung eines Schädigungs-Mails, |
| **Garantiert** | 100% Wahrscheinlichkeit garantiert | zB Ausfall durch einen Festplattenausfall, Festplatten halten ca 3 – 5 Jahre!Datenverluste durch technische Fehler |

Sie müsst schauen, dass Sie die Kategorien in der Risiko-Matrix **von rechts oben in Rot => nach links unten in Grün mit Hilfe Ihre Maßnahmen bekommen!**Risiko-Matrix mit Maßnahmen
Bitte hier die Kategorien 1 - 3 gemäß Ihrer Maßnahmen eintragen!

# Anhang

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

Dies ist eine umfassende und ausführliche Information betreffs der sensiblen Daten und es mag (bald) kürzere geben. Die DSGVO normiert, dass Ihr Klient **vorab** das Recht hat umfassend von Ihnen informiert zu werden.

Wenn der Klientin betreffs der Weiterleitung an Privatversicherung bzw andere Gesundheitsberufe einwilligt, dies bitte dort ankreuzen und archivieren.

**+ Aushang**

Die Datenschutzerklärung für Ihre Homepage können Sie **ausgedruckt als Aushang in Ihrer Praxis zB beim Erstgespräch verwenden:**

[https://datenschutz-generator.de](https://datenschutz-generator.de/)

oder auch:
<https://dsgvo-informationsverpflichtungen.wkoratgeber.at/> Am Ende des Ratgebers erhalten Sie ein Merkblatt mit Textbausteinen für Ihre Informationspflicht, die Sie für Ihren Aushang, aber auch bei der Datenschutzerklärung, verwenden können.

## Mustervertrag Auftragsverarbeitung-Vereinbarung gemäß Art 28 DSGVO

Typische **Aufragsverarbeitungen für Einzelpraxen** nach Art 28 und daher eine **Vereinbarung Art 28 DSGVO mit Ihnen notwendig,** sind Dienstleistungen wie:

* + Datendiensten bzw Hosting der Webseiten
	+ IT-Anbieter
	+ Software-Anbieter mit Fernwartung
	+ Newsletter-Tool-Anbieter

weitere mögliche sind:

Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten, das Einscannen von Dokumenten, die Backup-Sicherheitsspeicherung und andere Archivierungen, Datenträgerentsorgung,…

### Wie Sie sich erinnern können, haben wir die Empfänger 9-Provider/IT-Dienstleister/Software-Anbieter mit Fernwartung und andere Dienstleister, die pB Daten für Sie verarbeiten, nicht in der rechten Spalte beim **Verzeichnis Rechnungswesen** eingetragen, da wir nicht wissen, welche Daten genau übermittelt werden. ABER, da Sie mit diesen Dienstleistern eine Einwilligung gemäß Art 28 (siehe hier) abschließen müssen, werden die übertragen Daten dort am Besten in (2) vom Dienstleister selber aufgelistet, denn die Dienstleister wissen genau, welche Daten sie von Ihnen erhalten, und Sie können dann die Empfänger 9 ganz am Schluss bei den entsprechenden Daten in der Spalte eintragen.

## Verantwortliche

Keine Aufragsverarbeitung und somit Verantwortliche und daher auch **keine Vereinbarung gemäß Art 28 DSGVO notwendig sind** die Auslagerung von Aufgaben/Funktonen oder die externe Inanspruchnahme von Fachleistungen an/von einem Dritten mit dort **eigenverantwortlicher** Wahrnehmung wie:

* + **Honorar-Abrechnungs-Vereine\***, **Steuerberatung,** Personalverwaltung, Mitarbeiterrekruterung, Vertragskundenbetreuung, Finanzberatung, Unternehmens/DSGVO-Beratung, Wirtschafsprüfung, Rechtsanwälte, Notar, Therapeuten, Apotheken, Anbieter von Telefonleitungen, bzw Internetleitungen, Post, Transport, Ärzte, Krankenhäuser, Sozialversicherung, Inkassotätgkeit mit Forderungsübertragung, Sachveständigen- bzw. Gutachterbeaufragung, usw.

=> Bei diesen, da Verantwortliche, müssen Sie nichts tun!

Es wäre aber anzuraten, das Sie sich vergewissern, dass diese Verantwortlichen auch eine Dokumentation gemäß DSGVO betreffs des Datenschutz haben.

**\*** Ob Honorar-Abrechnungs-Vereine jetzt Datenverarbeiter oder Verantwortlich sind, ist strittig. Da sie aber in Eigenverantwortung auch die Zuteilung von Behandlungs-Einheiten, nicht nur an einzelne Psychotherapeuten/innen, sondern für eine ganze Region vornehmen, behandel wir sie als „Verantwortliche“. Sollte die Datenschutzbehörde dies anders sehen, so erhalten Sie per [**Newsletter**](https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung) die dann dazu notwendigen Vereinbarung von uns.

# Ende

 **Newsletter Psychotherapeuten**

<https://www.dataprivacydoctors.at/vorlagen/#NewsletterAnmeldung>

**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 , eines DSGVO-Workshops (z.B. [https://www.dataprivacydoctors.at](https://www.dataprivacydoctors.at/) ) 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.