Newsletter DSGVO

Mit 25. März 2018 tritt die Datenschutzgrundverordnung (DSGVO) in Österreich in Kraft. Der STLP hat sich in den letzten Wochen und Monaten intensiv mit dieser Thematik auseinandergesetzt.

In zwei Workshops mit gesamt über 180 TeilnehmerInnen wurde praktisches Wissen zur Umsetzung der DSGVO vermittelt. Der folgende Newsletter soll noch einmal zusammengefasst die wichtigsten Fragen zur DSGVO beantworten. Im Anhang finden Sie Vorlagen zum notwendigen Verarbeitungsverzeichnis sowie eine Einwilligungserklärung zur Datenverarbeitung für Ihre KlientInnen / PatientInnen.

Achtung: Diese Vorlagen müssen noch an Ihre jeweiligen Gegebenheiten angepasst werden. Dafür notwendige Felder wurden rot markiert. Es ist nicht möglich eine allgemein gültige Vorlage zu erstellen, da die Inhalte von Ihren jeweiligen Arbeitsprozessen abhängen.

**Rechtsgrundlage**

Der psychotherapeutische Beruf wird auf Basis des Psychotherapiegesetzes (PthG) ausgeführt. Dieses Gesetz definiert nicht nur Rahmenbedingungen für die Ausübung des Berufs, sondern regelt auch schon den Umgang mit Informationen, die im Zuge einer Psychotherapie bekannt werden. § 15 – die Verschwiegenheitspflicht – verpflichtet PsychotherapeutInnen zu einer umfassenden Verschwiegenheit über alle Geheimnisse, die ihnen im Zuge ihrer Tätigkeit bekannt geworden sind. Somit wird bereits hier Datenschutz im PthG maßgeblich vorgegeben.

Weiters regelt § 16a die Dokumentationspflicht. PsychotherapeutInnen sind zur Dokumentation verpflichtet. Die Art der Dokumentation, ob digital oder analog, wird nicht näher vorgegeben, beide Dokumentationsarten sind zulässig. Wohl aber sind die Inhalte vorgegeben. Informationen hierzu finden Sie auch noch im Berufskodex für PsychotherapeutInnen vom BMG: <https://www.bmgf.gv.at/cms/home/attachments/7/0/5/CH1002/CMS1415709133783/berufskodex_psychotherapie.pdf>

 Die DSGVO kommt zu diesen ohnehin vorhandenen Pflichten hinzu. Sie regelt wie mit Daten umzugehen ist und stärkt die Rechte von (durch Datenverarbeitung) Betroffenen.

**DSGVO**

**Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)**

Die DSGVO schützt natürlich Personen (Menschen). Ihr Anwendungsbereich ist die automatisierte (zB. mittels Computer oder Handy) und die nicht-automatisierte (zB. handschriftliche) Verarbeitung personenbezogener Daten in einem Dateisystem.

Dateisystem: jede strukturierte Sammlung personenbezogener Daten

Personenbezogene Daten: alle Informationen zu einer bestimmten oder identifizierbaren Person

Gesundheitsdaten: personenbezogene Daten betreffend die körperliche oder geistige Gesundheit, den Gesundheitsdienstleistungsbezug und Information über den Gesundheitszustand.

Verarbeitung von Daten meint jeden ausgeführter Vorgang im Zusammenhang mit personenbezogenen Daten (Erheben, Speichern, Löschen, Ordnen, Übermitteln ...).

Dies bedeutet, dass sowohl digitale Aufzeichnungen als auch handschriftliche Aufzeichnungen und Dokumentation in den Anwendungsbereich der DSGVO fallen.

Die DSGVO unterscheidet weiters zwischen VerantwortlicheR und AuftragsverarbeiterIn.

VerantwortlicheR sind eine Person oder Stelle, die über Zweck und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im selbstständigen Setting der Psychotherapie ist davon auszugehen, dass der / die einzelne PsychotherapeutIn VerantwortlicheR ist.

AuftragsverarbeiterIn ist eine Person oder Stelle, die personenbezogene Daten im Auftrag der Verantwortlichen verarbeitet. Beispiele hierfür wären Steuerberatung, aber auch die Firma Dropbox, falls PsychotherapeutInnen dort Dateien abgelegt haben. Ein weiteres Beispiel wäre mein Emailprovider, zB. A1 oder Google / Gmail.

**Grundsätze der Datenverarbeitung**

Die DSGVO gibt Grundsätze für jede Form der Datenverarbeitung vor. Auf diese soll im Folgenden in ihrer Relevanz für die Psychotherapie eingegangen werden.

* Rechtmäßigkeit der Verarbeitung
Personenbezogene Daten dürfen nur auf rechtmäßiger Basis verarbeitet werden. Hierzu gibt es folgende Möglichkeiten:
	+ Einwilligung der Person zur Datenverarbeitung für bestimmte Zwecke (muss nachgewiesen werden). Für diese Form der Einwilligung finden Sie eine Vorlage im Anhang dieser Email.
	+ Zur Vertragserfüllung erforderlich. (Ein Tischler / eine Tischlerin benötigt meine Daten zur Rechnungslegung)
	+ Eine rechtliche Verpflichtung wird erfüllt. (Gemäß PthG müssen bestimmte Daten dokumentiert werden)
	+ Lebenswichtige Interessen werden berührt. (Der Notarzt / die Notärztin dürfen die Daten meiner eCard ansehen, ohne meine vorherige Zustimmung)
* Zweckbindung
Erhobene Daten müssen einen bestimmten Zweck dienen und sind an diesen gebunden. Falls auf einem Stammdatenblatt die Telefonnummer einer PatientIn erhoben wird, darf diese nicht für Werbeanrufe verwendet werden, sondern ausschließlich für den vorher angegebenen Zweck, beispielsweise zur Terminkoordination.
* Datenminimierung & Speicherbegrenzung
Es dürfen nur Daten erhoben werden, die für die Erbringung der Leistung unbedingt notwendig sind. Für KollegInnen im Status in Ausbildung unter Supervision, wo ein Zuschuss durch die Krankenkasse nicht möglich ist, bedeutet dies beispielsweise, dass am Stammdatenblatt keine Sozialversicherungsnummer erhoben werden darf, da diese nicht unbedingt notwendig ist. Auch eine Email-Adresse könnte ein Beispiel für ein nicht notwendiges Datum sein.
Speicherbegrenzung bedeutet, dass Daten nur solange aufbewahrt werden dürfen, wie unbedingt notwendig. Das PthG Gibt hier eine Aufbewahrungsdauer von 10 Jahren vor.
* Richtigkeit
Betroffene haben Recht auf Richtigkeit ihrer Daten und somit auch auf Richtigstellung, falls Daten falsch erhoben worden sind oder sich geändert haben. Was dies für die Praxis bedeutet, wird sich erst zeigen.
* Integrität und Vertraulichkeit
PsychotherapeutInnen haben auf Integrität und Vertraulichkeit zu achten. Der Zugang zu den Daten ist entsprechend zu kontrollieren und sind technische und organisatorische Maßnahmen zu treffen um die Beständigkeit der Daten über den Speicherzeitraum und deren Vertraulichkeit sicherzustellen.
* Rechenschaftspflicht
PsychotherapeutInnen sind über diese personenbezogenen Daten und ihre Verarbeitung Rechenschaftspflichtig.
* Technikgestaltung (Privacy by Design 🡪 **Pseudonymisierung**)
Die gewählten organisatorischen und technischen Maßnahmen sollen so ausgerichtet sein, dass sie Datenschutz von Anfang an mitdenken. Dies betrefft sowohl die papierbasierte Unterlagen als auch elektronische Dateien .
* Datenschutzfreundliche Voreinstellungen
Ein Beispiel hierfür wären Newsletter. Diese dürfen nur noch als sogenanntes opt-in Modell angeboten werden. PatientInnen müssen also explizit zustimmen, falls sie den Newsletter ihrer PsychotherapeutIn abonnieren wollen.

Anmerkung: Für PsychotherapeutInnen gelten strenge Werberichtlinien. Sollten Sie Newsletter versenden oder dies Vorhaben wird empfohlen sich diese genau anzuschauen. Sie finden diese online unter <https://www.bmgf.gv.at/cms/home/attachments/7/0/5/CH1002/CMS1415709133783/werberichtlinie.pdf>

**Besondere Kategorien von Daten (sensible Daten)**

PsychotherapeutInnen arbeiten täglich mit sogenannten besonderen Kategorien von Daten bzw. sensiblen Daten. Dies sind Daten über Gesundheitszustand einer Person, sexuelle Orientierung, Religionszugehörigkeit usw. Die DSGVO untersagt die Verarbeitung solcher Daten allgemein, schafft jedoch gleichzeitig Ausnahmen, wie beispielsweise für den (psychotherapeutischen) Gesundheitsbereich. Diese Daten gelten als besonders schützenswert, erfordern also ein besonderes Level an Schutz.

**Die Umsetzung der DSGVO in der psychotherapeutischen Praxis**

PsychotherapeutInnen sind nach derzeitiger Rechtsauffassung **nicht** verpflichtet eine datenschutzbeauftragte Person zu benennen. Weiters sind PsychotherapeutInnen nach derzeitiger Rechtsauffassung **nicht** verpflichtet eine Datenschutzfolgeabschätzung vorzunehmen.

Es besteht jedoch die Pflicht ein sogenanntes Verarbeitungsverzeichnis anzulegen. Das Verarbeitungsverzeichnis ist eine zentrale Übersicht aller durch den / die PsychotherapeutIn vorgenommen Datenverarbeitungstätigkeiten. Im Anhang finden Sie eine Vorlage für dieses Verarbeitungsverzeichnis. Die Datenschutzbehörde darf in dieses Dokument Einsicht nehmen. Das Verzeichnis wird für jede psychotherapeutische Praxis unterschiedlich aussehen, je nachdem welche Systeme sie benutzen, ob Kassenplätze vergeben werden, ob Kommunikation mit Behörden stattfindet usw. Wichtig ist, dass Sie in diesem Dokument jede Form der Datenverarbeitung anführen. Anmerkungen zum korrekten Ausfüllen finden Sie direkt im angehängten Musterverzeichnis.

Von Ihren KlientInnen / PatientInnen benötigen Sie die Zustimmung zur Datenverarbeitung. Die Zustimmung zur Datenverarbeitung durch PatientInnen / KlientInnen ist nachweislich zu dokumentieren, zum Beispiel mit der im Anhang befindlichen Zustimmung zur Datenverarbeitung. Diese muss ebenfalls an Ihre Gegebenheiten angepasst werden. Sollten Sie beispielsweise Dokumente an Behörden übermitteln oder mit dem Netzwerk Psychotherapie Steiermark abrechnen so sind auch diese Datenübermittlungen in der Einverständniserklärung anzuführen. Alle von Ihnen erfassten Daten müssen auf dieser Zustimmungserklärung angeführt sein. In der Zustimmungserklärung müssen Sie auch anführen zu welchem Zweck diese Daten verarbeitet werden.

*Anmerkung: Die Zustimmung zur Datenverarbeitung ist ein Element der DSGVO, das rechtlich noch nicht vollständig geklärt ist. Sie sind nach PthG § 16a verpflichtet die Psychotherapie zu dokumentieren. Es besteht somit eine gesetzliche Notwendigkeit, die eine Einwilligung zur Dokumentation durch KlientInnen / PatientInnen nicht notwendig macht. Alles was über die Dokumentation nach PthG hinausgeht bedarf jedoch der Einwilligung. Hierfür braucht es die explizite Einwilligung. Deswegen vertritt die STLP die Ansicht, dass Sie mit einer entsprechenden Einwilligungserklärung abgesichert sind.*

**Exkurs: Nutzung von Instant Messaging Diensten (z.B. WhatsApp)**

Die DSGVO würde es Ihnen mit Zustimmung Ihrer PatientInnen / KlientInnen ermöglichen Dienste wie beispielsweise WhatsApp zu Zwecken der Kommunikation benutzen. In diesem Fall müssten Ihre KlientInnen der Nutzung von WhatsApp explizit auf der Einwilligungserklärung zustimmen, ebenso der Übermittlung von persönlichen Daten (Namen und Telefonnummer) an Drittländer, da WhatsApp diese Daten in die USA übermittelt.

Dennoch vertritt der STLP die Ansicht, dass die Nutzung von WhatsApp sowohl aus Gründen der Sicherheit als auch im Sinne des PthG § 15 (Schweigepflicht) nicht anzuraten ist. WhatsApp protokolliert Ihre Nutzung ausführlich mit, für das Unternehmen sind somit problemlos Rückschlüsse darauf möglich, wer bei Ihnen KlientIn / PatientIn ist. Eine Alternative, die aus derzeitiger Sicht empfehlenswert ist, ist der Messaging Dienst Signal (<https://www.signal.org>). Daten werden hier ausschließlich verschlüsselt übermittelt, es sind keine Rückschlüsse auf BenutzerInnen möglich. Dennoch können auch in dieser Software jederzeit Lücken gefunden werden. Grundsätzlich sind Telefonate und SMS empfehlenswerter als Messaging Dienste. Ein sicheres Versenden von Dokumenten ist ausschließlich per Post gegeben. E-Mail gilt nicht als sicheres Medium. Informationen hierzu finden Sie auch noch in den Internetrichtlinien für PsychotherapeutInnen: <https://www.bmgf.gv.at/cms/home/attachments/7/0/5/CH1002/CMS1415709133783/internetrichtlinie_03052012.pdf>

Die Empfehlung des STLP ist eine eigene Email-Adresse zu organisieren. Emails, die über Google oder GMX versandt werden, werden ebenfalls zu Werbezwecken ausgewertet, auch hier sind Rückschlüsse möglich. Hiermit wird es möglich eine Email-Adresse beispielsweise im Format praxis@vorname-nachname.at zu bekommen. Ein möglicher österreichischer Anbieter ist world4you – <https://www.world4you.com>

Die DSGVO ist ein komplexes Thema, viele juristische Fragen sind nicht bis ins letzte Detail geklärt (und werden eventuell noch in einigen Jahren unklar sein). Die Vorlagen und dieses Informationsmail wurden nach besten Wissen und Gewissen erstellt. Es ist davon auszugehen, dass der STLP in den nächsten Monaten und Jahren aktualisierte Informationen und Versionen dieser Vorlagen ausschicken wird.