V•PP

Data Privacy Doctors
Expert Network

DSGVO

EU-Datenschutzgrundverordnung

im Gesetzesrang, gültig ab 25.05.2018

Inklusive Korrekturen/Ergänzungen
(2018-05-04)

Konzepte: USA vs. EU

- **USA: »Meine Daten gehören mir«**
- Eigentumsbegriff
- Verletzung ist Hausfriedensbruch
- Geringe Strafen
- Wenig Rechte
- Vorteil: handelbar

- **EU: »Ich bin meine Informationen«**
- Identitätsbegriff
- Verletzung ist Raub bzw. »Körperverletzung«*
- Hohe Strafen bis 20.000.000,–
  oder 4% des Konzernumsatzes**
- Ich kann jederzeit widerrufen
  Recht auf Vergessen (Löschung)
- Vorteil: Grundrecht

*) Luciano Floridi, »Wie die Infosphäre unser Leben verändert – die 4. Revolution«

) in **D lt. Gesetzesentwurf (nat. Anpassung) 50.000 bis 300.000, bzw. mehr, so der Nutzen durch die Datenschutzverletzung die Strafe übersteigt. In **Ö**: Verwaltungsstrafe bis 50.000, strafrechtlich bis 720 Tagessätze

Was ist Datenschutzrecht?

- **Daten von Personen dürfen grundsätzlich nicht verarbeitet werden**
  = **Grundrecht**
- Datenschutzrecht schützt keine Daten!
- Datenschutzrecht schützt den Betroffenen betreffs der Verarbeitung seiner Daten!
- Datenschutz nur für **personenbezogene Daten**

Wann darf ich pb* Daten verarbeiten?

- **Nur wenn es eine gesetzliche Grundlage dafür gibt:**

1) Einwilligungserklärung des Betroffenen
2) für die Erfüllung eines Beratungsvertrags notwendig
3) zur Erfüllung einer rechtlichen Verpflichtung (Dokumentationspflicht)
4) Um lebenswichtige Interessen des Betroffenen zu schützen
5) Wahrung der berechtigten Interessen des Verantwortlichen
   Gilt aber nicht für sensible Informationen

*) pb = personenbezogene

Wann darf ich pb Daten verarbeiten?

Wenn es rechtmäßig ist und offengelegt wird

1) was der Zweck der Verarbeitung ist und der Verantwortliche dazu befugt ist
2) dass der Zweck sich nicht ändern wird
3) wie lange sie gespeichert werden
4) welche Verarbeitungsvorgänge und -verfahren angewandt werden
5) an wen die Daten warum wie übermittelt werden
6) welche technische und organisatorische Maßnahmen betreffs Datenschutz und -sicherheit getroffen werden

Was ist das Besondere bei PsychotherapeutInnen?

Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung pb Daten von PatientInnen oder von MandantInnen betrifft und durch eine einzelne ÄrztIn, sonstigen Angehörigen eines Gesundheitsberufes (einzelnen PsychotherapeutInnen) oder RechtsanwältIn erfolgt. In diesen Fällen sollte eine Datenschutz- Folgenabschätzung nicht zwingend vorgeschrieben sein (Art 35, Erwägungen 91)

Bei Gemeinschaftspraxen muss dies aber immer für den konkreten Einzelfall überprüft werden (Datenschutzbeauftragter?)

Welche Kategorien der personenbezogenen Daten gibt es?

- **„normale“ pb Daten**
  von KlientInnen, LieferantInnen, Dritten

- Name, Firma, sonstige Geschäftsbezeichnung
- Anschrift, Lieferadresse
- Email, Telefonnummer,
- Bankverbindung
- Kontaktperson
  Erziehungsberechtigter
- Sozialversicherungsnummer

- **Sensible Informationen**
  iSd Art 9 DSGVO

- Gesundheitsdaten (körperlich, geistig)
- Genetische Daten bzw. Krankheiten
- Diagnostik (früherer, gegenwärtiger und zukünftiger Gesundheitszustand)
- Daten zum Sexualleben oder sexuelle Orientierung, sowie Religion

- Kinder unter 14 Jahren gem. § 8 DSG
- (strafrechtliche Daten gem. Art 10)

Verarbeitungsverzeichnisse – Systematisierung

1. Rechnungswesen

hier werden **personenbezogene** (pb) **Daten der Betroffenen** verarbeitet und übertragen (Buchhaltungsdaten)

Ausdrücklich keine sensiblen Informationen.

Aufbewahrung 7 Jahre

2. Klientenverwaltung und Honorarabrechnung

hier werden **sensible Informationen der Betroffenen,** auch von Kindern, verarbeitet und übertragen,

3. Dokumentation

Kann **1 Jahr/ 6 Monate/ 3 Monate / gleich** nach Beendigung der Beratung/Behandlung archiviert werden

Aufbewahrung 10 Jahre

1. Abrechnung

Rechnungslegung DSGVO-konform gestalten

Dies bedeutet unter anderem, dass in den Unterlagen, wie z.B. Rechnungen, die ich an Auftragsverarbeiter wie meine Bilanzbuchhaltung/Steuerberatung bzw. ans Finanzamt weiterleite, sich **keine Diagnosen (nach ICD-10) und sensible Informationen befinden dürfen bzw. sie geschwärzt sind**.

Betreffs Institutionen wie den Sozialversicherungen, wo die Verarbeitung auf Grund einer gesetzlichen Norm geschieht, wird das **Gespräch über die Vertretung gesucht**, um auch von dort Unterlagen für die Buchhaltung zu erhalten, die keinerlei sensiblen Informationen beinhalten.

2. Klientenverwaltung und Honorarabrechnung

Führung und Pflege von Klientenkarteien zur Dokumentation
gemäß §16a (3) Dokumentationsplicht Psychotherapiegesetz 1990

<u>Empfängerkategorien</u>

Sozialversicherungsträger (einschließlich Betriebskrankenkassen), MA11 gesetzlich

Privatversicherungen mit ausdrücklicher Einwilligung

ÄrztInnen, Vertreter von sonstigen Gesundheitsberufen und medizinische oder soziale Einrichtungen, mit ausdrücklicher Einwilligung

RechtsanwältInnen, Gerichte, Schlichtungsstellen und Patientenanwälte, gesetzlich bzw. mit ausdrücklicher Einwilligung

z.B. Wiener Gesellschaft für psychotherapeutische Versorgung, (Verein)
mit ausdrücklicher Einwilligung

Auftragsverarbeitung nach Art 28 DSGVO

Auftragsverarbeitungen für Einzelpraxen **Vereinbarung Art 28 DSGVO notwendig**	**Verantwortliche gemäß DSGVO** **keine Vereinbarung notwendig**
•Honorar-Abrechnungs-Verein (?)* •reine Lohn/Honorarverrechnung •Datendiensten bzw. Hosting der Webseiten •Anbieter verschlüsselter und sicherer Datenübertragung •IT-Anbieter (mit Fernwartung) •Software-Anbieter mit Fernwartung •Einscannen von Dokumenten •Backup-Sicherheitsspeicherung, Archivierungen •Datenträgerentsorgung	•Honorar-Abrechnungs-Verein (?)* •**Steuerberatung,** Wirtschafsprüfung, Finanzberatung •Unternehmens/DSGVO-Beratung •Rechtsanwälte, Notar •Anbieter von Telefonleitungen, bzw. Internet •Post, Transport •Ärzte, Krankenhäuser, Apotheken, Gesundheitsberufe •Sozialversicherung •Sachverständigen- bzw. Gutachterbeauftragung

*) es besteht Interpretationsspielraum, wir tendieren zu »Verantwortliche«

Risiko-Analyse

Folgende Daten wurden analysiert und in die entsprechenden Kategorien eingetragen:

Kategorie	pb Daten
1	**Besondere Datenkategorien iSd Art 9 DSGVO** sensible Daten von Klienten, wie zb Gesundheitsdaten (körperlich, geistig), Genetische Daten bzw Krankheiten, Diagnositk (früherer, gegenwärtiger und zukünftiger Gesundheitszustand), Daten zum Sexualleben oder sexuelle Orientierung ; Kinder unter 14 Jahren gem. Art 8, bzw. DSG 2018, strafrechtliche Daten gem. Art 10; sowie Mitschriften u. Fotos, Personenstand, => geheim/vertraulich
2	Schlüssel, Passwörter, ... , Vertragstext und Geschäftskorrespondenzen, sonstige Vereinbarungen => geheim
3	Geburtsdatum , Bankverbindungen, Kreditkartennummern und -unternehmen=> intern/vertraulich
4	Pb Daten mit vernachlässigbaren bis begrenzten Schutzbedarf, siehe oben Vorabanalyse

Risiko für **Betroffene ohne Maßnahmen**

Schwere					
Existenzgefährdend				1, 2	
Wesentlich				3, 4	
Begrenzt				5	
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

Folge:

Bei einer Datenschutzverletzung (Diebstahl, Verlust, Viren, Trojaner, kriminelle Angriffe, …), müssen **innerhalb von 72 Stunden** die Datenschutzbehörde sowie **alle Ihre betroffenen KlientInnen informiert** werden

Maßnahmen **um Risiko für Betroffenen zu minimieren**

8.4 Risikoanalyse mit Maßnahmen

Schwere					
Existenzgefährdend					
Wesentlich					
Begrenzt		1, 2			
Vernachlässigbar	5	3, 4,			
	Vernachlässigbar	Möglich	Sehr wahrscheinlich	Garantiert	EWK

8.5 Folgen der Maßnahmen betreffs Risiko

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

Betroffenenrechte

- Informationspflicht
- Auskunftsrecht in Verbindung mit Einsichtsrecht – kann verweigert werden
- Recht auf Berichtigung
- Recht auf Vergessenwerden und Löschung
- Recht auf Datenübertragbarkeit
- .... und weitere

Aktuell & Ausblick (in Bewegung)

Datenschutz-Deregulierungsgesetz
„Verwarnung durch die Datenschutzbehörde“

§ 11. Die Datenschutzbehörde wird den Katalog des Art. 83 Abs. 2 bis 6 DSGVO so zur Anwendung bringen, dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DSGVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen.

Datum: 20.04.2018 - Beschluss im Nationalrat

Tipp: nicht komplett darauf verlassen!

V•PP

Data Privacy Doctors
Expert Network

TOMs: Technisch-organisatorische Maßnahmen

Vertraulichkeit

1) Zutrittskontrolle

Türen, Fenster, Gegensprechanlage, Empfang, Schlösser/Schlüssel, (Reinigungs-)Personal

2) Zugangskontrolle

Schlüsselregelungen, Protokollierung, Passwörter, Vorgaben f. Stärke der Passwörter, Two-Factor Authentication, Firewall, verschlüsselte Datenträger

3) Zugriffskontrolle

Zugriff nur durch Verantwortliche, Rollen & Rechte, Protokollierung

4) Klassifikationsschema

Daten: geheim/vertraulich/intern/öffentlich

Integrität

1) Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern, Löschen bei Übertragungen oder Transport (Signatur, Verschlüsselung)

2) Eingabekontrolle

Personenbezogene Daten werden ausschließlich vom Verantwortlichen verwaltet (Eingabe, Änderung, Löschung – Dokumentenmanagement)

Verfügbarkeit und Belastbarkeit

1) Verfügbarkeitskontrolle

Schutz gegen: Zerstörung (mutwillig, unbeabsichtigt), Verlust; Katastrophen (Feuer, Wasser, ...), Malware, Attacken, ...
Maßnahmen: Firewall, Malwareschutz, Backup, Notfallpläne/Recovery, Security Checks, Sicherungskonzept

2) Wiederherstellbarkeit

(Rasche) Wiederaufnahme des Betriebes – Backup/Restore, Prozeduren zur Wiederherstellung der Systeme und des Betriebs.

3) Löschungsfristen

Löschung personenbezogener Daten nach Anforderung(en) – rechtl. Grundlage

Pseudo-, Anonymisierung, Verschlüsselung

1) Pseudonymisierung

Primäre Identifikationsmerkmale getrennt speichern – Kennung oder Hash als Kennzeichen (-> Verfahrensverzeichnis)

2) Anonymisierung

Wo möglich, anonymisieren (Datensparsamkeit), z.B. Statistiken

3) Verschlüsselung

Data at Rest: Datenträger/Geräte: technologische Sicherheit, Durchgängigkeit
Data at Motion: Kommunikation, Datenaustausch – Netz & Medien
Umgang mit Schlüsselmaterial! (sicher, aber dauerhaft verfügbar)

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1) **Risikoanalyse**
2) **Datenschutzfreundliche Voreinstellungen**
3) **Kontroll- und Verbesserungsprozess (mind. 1x jährlich)**
4) **Weiterbildung**
5) **Auftragskontrolle**

Auftragsdatenverarbeitung nur mit Weisung: Vertrag, Auftragsmgmt, Auswahl der Partner, verschlüsselte Übertragung und Speicherung (Kontrollpflicht!)

Konkrete technologische Themen

eMail

eMail = Postkarte. Provider, Verschlüsselung, Signatur

Messenger

~~WhatsApp~~ , Signal, Transmit, Wire, Mattermost, ...

Online Speicher

Dropbox ? , OneDrive ?, iCloud?, Nextcloud – auf eigenem Server!

Gerätehandhabung

Festplattenverschlüsselung, USB-Sticks ???, Backuplösungen

Konkret: Übertragung Klientendaten (pb!)

Personenbezogene Daten immer ...

gesichert, verschlüsselt

verschlüsselte Datei, App, Website, ...

oder per Post

geschlossenes Couvert, eingeschrieben, Ident.Brief

Für Abrechnungen, Buchhaltung, ...

KEINE Diagnosen, besonders schützenswerte Daten!

da diese Daten länger aufbewahrt und nicht geschützt sind

Konkret: Backup und Archivierung

Backupstrategie

mehrere Kopien, regelmäßig, verschlüsselt/gesichert
z.B.: täglich + wöchentlich + monatlich ... (z.B. TimeMachine)

off-site (Feuer, Wasser, ...)

Testen!

testweise Restore

Archivierung

Strategie! Regelmäßiger Durchlauf!

Konkret: Migration -> neues Gerät

Wie werden Daten übernommen?

Verschlüsselung, SW und Versionen, Archive, Dateisystem(e)

Was geschieht mit dem alten Gerät?

alle Daten zuverlässig zerstören! (HD physisch zerstören)

Was geschieht mit Backups?

Übernahme (Verschlüsselung!), Vernichtung

V•PP

Data Privacy Doctors
Expert Network

- https://www.dataprivacydoctors.at

Christopher Temt – ct@dataprivacydoctors.at

Michael Werzowa – mw@dataprivacydoctors.at

Vorlagen & Anleitung für PsychotherapeutInnen: https://www.dataprivacydoctors.at/vorlagen/