PSYCHOTHERAPEUTENKAMMER BERLIN

# DATENSCHUTZ IN DER PSYCHOTHERAPEUTISCHEN PRAXIS

STAND 13.06.2018

Detlev Achhammer
Im Auftrag der Psychotherapeutenkammer Berlin

# Gesetzliche Grundlagen



- **Europäische Datenschutzgrundverordnung (EU-DSGVO) seit 25.05.2018**
- Bundesdatenschutzgesetz (BDSG)
- Berliner Datenschutzgesetz (BlnDSG)
- Sonstige Gesetze (z.B. SGB, Berufsordnung und andere mehr)

# Regelungsbereich



- Automatisierte Verarbeitung personenbezogener Daten
- Nichtautomatisierte Verarbeitung nur, wenn personenbezogene Daten in einem Dateisystem gespeichert werden
  - Karteien zur Verwaltung von Patientendaten sind ein Dateisystem (sortiert z.B. nach Namen, Jahr usw.)
  - Patientenakten (nach Namen sortiert) sind ein Dateisystem
  - Papierbasierte Notizen ohne systematisches Ordnungssystem sind **kein** Dateisystem

# Verarbeitung



- Erheben (Beschaffen)
- Speichern (Erfassen, Aufnehmen, Aufbewahren auf Datenträgern/Papier)
- Verändern (Inhaltliches Umgestalten)
- Übermitteln (Bekanntgabe an Dritte)
- Sperren (Verhindern weiterer Verarbeitung)
- Löschen (Beseitigen)
- Nutzen (jede sonstige Verwendung)

personenbezogener Daten

# Personenbezogen



sind Angaben, die bei Zuordnung zu einer natürlichen Person Einblicke ermöglichen in deren physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität

# Beispiele personenbezogener Daten



- allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer usw.)
- Kennnummern (Sozialversicherungsnummer, Steueridentifikationsnummer, Nummer bei der Krankenversicherung, Personalausweisnummer, Matrikelnummer usw.)
- Bankdaten (Kontonummern, Kreditinformationen, Kontostände usw.)
- Online-Daten (IP-Adresse, Standortdaten usw.)
- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usw.)
- Werturteile (Schul- und Arbeitszeugnisse usw.)
- Und vieles mehr…..

# Besonders schützenswerte Daten
## (Art. 9 DSGVO)



- Angaben über rassische sowie ethnische Herkunft
- politische Ansichten
- religiöse sowie philosophische Überzeugung
- Gewerkschaftszugehörigkeit
- Angaben über die Gesundheit einer Person
- Daten zur Sexualität eines Menschen

**dürfen im Regelfall gar nicht erhoben werden**

➢ **AUSNAHMEN (Folien 9 und 10)**

# Grundsatz der (Un-) Zulässigkeit



- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist grundsätzlich verboten, es sei denn, es besteht eine Erlaubnis
  - Aus einem Gesetz
  - Aus rechtlicher Verpflichtung bzw. zur Wahrung von Rechtsansprüchen
  - Aus einer Einwilligung des Betroffenen

# Gesetzliche Grundlagen im Gesundheitsbereich 1



- Art. 9 Abs.2 lit. h) DSGVO i.V. mit § 22 Abs. 1 Nr. 1 lit. b) BDSG:

  **Zum Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich…….**

- **Erlaubt sind damit alle Datenverarbeitungs-vorgänge im Zusammenhang mit Prävention, Diagnostik, Therapie, Nachsorge**

# Gesetzliche Grundlagen im Gesundheitsbereich 2



- Zulässig im Zusammenhang mit sozialrechtlichen Pflichten aus dem SGB
  - Im Bereich der gesetzlichen Krankenversicherung, Pflegeversicherung, Unfallversicherung, Rentenversicherung
  - Mitteilungen aus diesen Pflichten gegenüber KV, Krankenkassen, MdK, Unfallversicherung usw.
- Pflichten im öffentlichen Interesse (Abwehr von schwerwiegenden Gefahren)
- Zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit des Patienten

# Aus rechtlicher Verpflichtung bzw. zur Wahrung von Rechtsansprüchen



- Art. 9 DSGVO:
  - Erfüllung privatrechtlicher Verträge (Privatpatienten)
  - Geltendmachung, Ausübung, Verteidigung von Rechtsansprüchen
    - Honorarforderung
    - Verteidigung gegen Vorwürfe im Berufsrecht, Strafrecht, Zivilrecht usw.

# Keine Einwilligung notwendig bei gesetzlicher Grundlage



Wenn die Datenverarbeitung auf Grund eines Gesetzes erlaubt ist, bedarf es keiner zusätzlichen Einwilligung des Patienten

# Datenschutzrechtliche Einwilligung



- Erforderlich nur bei Fehlen gesetzlicher Grundlage
- Für Abrechnung über private Verrechnungsstelle immer notwendig
- Weitere Fälle – in der therapeutischen Praxis eher von untergeordneter Bedeutung.
  (z.B. § 295a Abs. 1 SGB V – besondere hausärztliche Versorgung)

# Wirksame Einwilligungserklärung



- Setzt umfassende Information des Patienten voraus
  - Patient muss erkennen können, zu welchem Verarbeitungs-zweck er sie abgibt und gegenüber welchen Personen
  - Verbot der Pauschaleinwilligung („Willige ein, dass meine Daten gespeichert und verarbeitet werden“ = unzulässig)
  - Ausdrücklichkeit (Erklärung!)
  - Freiwilligkeit (Kopplungsverbot)
    - Ohne Zwang, Druck oder Täuschung
  - Schriftlich, mündlich (!), elektronisch („opt-in“)
  - Einwilligung von Minderjährigen
    - Gültig nur bei Einsichtsfähigkeit (noch unklar, evtl. ab 15 Jahren)
    - Sonst Erklärung d. Sorgeberechtigten (Eltern, Vormund, Pfleger) erforderlich

# Informationspflichten bei Selbsterhebung und bei Datenübernahme von Dritten 1



- Identität und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (so vorhanden)
- Verarbeitungszweck und Rechtsgrundlage
- Rechte des Betroffenen
  - Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung,
- Ggf.: Empfänger der Daten (Auftrags-DV!!)
- Widerrufbarkeit von Einwilligungen
- Beschwerderecht bei der Aufsichtsbehörde

# Informationspflichten bei Selbsterhebung und bei Datenübernahme von Dritten 2



- Dauer der Speicherung
- Verpflichtung zur Bereitstellung, bzw. Folgen der Nichtbereitstellung erläutern
- Bei Übernahme von dritter Seite: Aufklärung darüber, woher die Daten stammen
- Keine Informationspflicht
  - bei unverlangt übersandten Daten, wenn diese sogleich wieder gelöscht werden
  - wenn der Betroffene bereits über alle Informationen verfügt (Vorsicht!)
  - Über die Weitergabe, wenn diese gesetzlich vorgeschrieben ist

# Art und Weise der Information



- Einfache, verständliche, klare Sprache
- Mündlich oder schriftlich, auch durch Aushändigung eines standardisierten Formblatts
- Durch deutlich sichtbaren Aushang in der Praxis

# Rechte des Betroffenen



- Auskunftsrecht über alle ihn betreffenden Daten
  - Welche Daten, Verarbeitungszweck, Rechtsgrundlage, Dauer der Speicherung und einiges mehr (Art. 15 DSGVO) -nicht verwechseln mit Einsichtsrecht in Patientenakte-
- Recht auf Berichtigung, Löschung, Einschränkung
  - Löschungsrecht, wenn Widerspruch erhoben wurde oder Speicherung unzulässig ist
  - Aber: kein Recht auf Löschung, solange andere gesetzliche Aufbewahrungsfristen bestehen ( z.B. 10 Jahre für Behandlungsunterlagen nach der BO, BGB usw.)

# Muster Einwilligungserklärung



- Kassenärztliche Bundesvereinigung -
  gut und kostenlos
  http://www.kbv.de/html/datensicherheit.php
- „Institut für Wissen in der Wirtschaft“ (IWW)
  gut, aber kostenpflichtig (Tagespass 6 €)
  https://www.iww.de/pp/recht/muster-einwilligungserklaerung-in-die-datenverarbeitung-d56851

# Grundsätze der Datenverarbeitung



- Datensparsamkeit
  - nur Daten, die man wirklich braucht
- Zweckbindung
  - Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben wurden
- Datenrichtigkeit
  - Daten müssen sachlich richtig (aktuell!) sein
- Datensicherheit

# Pflichten zum Datenschutz/Datensicherheit



- Festlegung eines Verantwortlichen
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten
- Evtl. Vornahme einer Datenschutz-Folgenabschätzung
- Evtl. Benennung eines Datenschutzbeauftragen (Art. 37)

# Verantwortlicher (Art. 24)



- Ist verantwortlich für den Einsatz technischer und organisatorischer Maßnahmen und zur Sicherstellung und Nachweiserbringung, dass die Verarbeitung gemäß DSGVO erfolgt.
- Eine Person muss dazu bestimmt werden (In Einzelpraxis: der Inhaber)

# Verarbeitungsverzeichnisse (Art. 30)



- Verzeichnis anlegen für jede Datenverarbeitungstätigkeit - automatisiert und nichtautomatisiert
- Bei Gesundheitsdaten obligatorisch
- Schriftlich oder elektronisch
- Sind vorzuhalten und auf Anforderung der Datenschutzbeh. vorzulegen
- Bei Verstoß drohen hohe Geldbußen

# Verarbeitungsverzeichnis-Inhalt



- Enthält Angaben zum Verantwortlichen, Art und Zeck der Verarbeitung, Schutzmaßnahmen und vieles mehr
- Muster und Ausfüllbeispiele im Netz leicht zu finden, z.B. bei der KBV und der BÄK

**www.kbv.de/html/datensicherheit.php**

**www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Bekanntmachung_Datenschutz-Check_09.03.2018.pdf**

# Datenschutz-Folgenabschätzung-Art. 35



- Ist durchzuführen, wenn Datenverarbeitung ein hohes Risiko für Rechte und Freiheiten der Betroffenen besteht, z.B. bei
  - besonders umfangreicher DV
  - Verarbeitung hochsensibler Daten (z.B. Gesundheitsdaten)
  - Systematischer Videoüberwachung öffentlicher Bereiche

# Datenschutz-Folgenabschätzung-Art. 35



**Nach telefonischer Vorab-Mitteilung* des Berliner Landesdatenschutzbeauftragten müssen trotz Verarbeitung sensibler Daten Einzelpraxen PP/KJP keine DSFA vornehmen.**

*Die angekündigte schriftliche Mitteilung wird auf der Homepage der PTK veröffentlicht

# Datenschutzbeauftragter-Art. 37



- Vorgeschrieben in bestimmten Fällen
  - Wenn i.d.R. mindestens 10 Personen in der Praxis ständig mit der Datenverarbeitung beschäftigt sind
  - Wenn eine Datenschutz-Folgenabschätzung notwendig ist
- Extern oder intern möglich

# Maßnahmen zur Datensicherheit-Art. 32



- Der Verantwortliche trifft (auf Grundlage der Verarbeitungsverzeichnisse) geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten unter Berücksichtigung des Stands der Technik
  - Zur Sicherheit der Systeme und Dienste auf Dauer
  - Zur schnellen Wiederherstellbarkeit nach physischen oder technischen Störungen
  - Regelmäßige Überprüfung der Schutzmaßnahmen nötig

# Meldepflichten



- Datenpannen müssen i.d.R. innerhalb 72 Stunden der Aufsichtsbehörde (Landesbeauftragter für Datenschutz) gemeldet werden, z.B.
  - Hacking-Angriffe, Verlust von Datenträgern, Missachtung des Datenschutzes durch Mitarbeiter u.ä.
  - Bei meldepflichtigen Datenpannen ist der betr. Patient auch dann zu benachrichtigen, wenn keine Risiken für ihn zu befürchten ist
- Ausnahmen von der Meldepflicht, weil die vorhandenen Schutzmaßnahmen nachweislich gewirkt haben.
- Schutzmaßnahme: z.B. Verschlüsselung

# Mögliche Sanktionen



- Erheblich erhöhte Bußgeldandrohungen
  - Bis zu 10 Mio € oder 2% des Jahresumsatzes
  - Bei besonders schwerwiegenden Verstößen (z.B. bei Gesundheitsdaten) bis zu 20 Mio € oder 4 %
- Vorstufen zur Bußgeldfestsetzung
  - Erteilung von Verwarnungen, Verweisen u.ä.
- Wichtiger ist das Vertrauensverhältnis zum Patienten

# Auftragsverarbeitung-Art. 28



- Datenverarbeitung durch externe Dienstleister
  - IT-Verwaltung
  - Vernichtung von Akten oder Datenträgern
  - Abrechnungsbüro
- Bedarf keiner besonderen Erlaubnis aus einem Gesetz bzw. keiner Einwilligung des Betroffenen, wenn wirksamer Vertrag mit Dienstleister
  - 

**Dies gilt nur für das Datenschutzrecht, § 203 StGB ist auch hier zu beachten!**

# Vertrag Auftragsverarbeitung 1



- Vertragspartner sorgfältig auswählen
- Schriftlicher Vertrag mit bestimmten Regelungen
  - Gegenstand, Art und Dauer, beteiligte Personen
  - Daten dürfen nur entspr. der Weisung des Verantwortlichen verarbeitet werden
  - Zusicherung der Vertraulichkeit
  - Art der Datenschutzmaßnahmen
  - Keine Weitergabe an Unterbeauftragte ohne ausdrückliche Zustimmung des Verantwortlichen
- Auftragsverarbeiter müssen im Verarbeitungsverzeichnis genannt werden

# Vertrag Auftragsverarbeitung 2



- Der Verantwortlicher und Auftragsverarbeiter haften gemeinsam für den Datenschutz
- Haftung des Auftragsverarbeiters jedoch beschränkt auf die Einhaltung der ihm im Vertrag auferlegten Pflichten
- Sie sind aus der Verantwortung, wenn Sie im Verhältnis zum Dienstleister alles Notwendige geregelt haben.
- Zertifikat vom Dienstleister vorlegen lassen z.B. ISO/IEC 27001
- Im Zweifel rechtlich beraten lassen
- Auf Muster zurückgreifen

# Vertragsmuster Auftragsverarbeitung 1



- „Institut für Wissen in der Wirtschaft“ (IWW)
  gut, aber kostenpflichtig (Tagespass 6 €)
  **https://www.iww.de/pp/recht/mustervertrag-auftragsdatenverarbeitung-d57359**
- Berufsverband der Datenschutzbeauftragten Deutschland (bvd) –Arbeitskreis Medizin-
  kostenlos aber etwas unübersichtlich
  **https://bvdnet.de/wp-content/uploads/2017/07/Muster-AV-Vertrag.pdf**

# Vertragsmuster Auftragsverarbeitung 2



- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. „Arbeitskreis Medizin“

  https://bvdnet.de/wp-content/uploads/2017/07/Muster-AV-Vertrag.pdf

  Projekt 29
  https://www.projekt29.de/vertrag-zur-auftragsdatenverarbeitung-im-gesundheitswesen/

# Datenschutz-Verhalten „digital“



- Patientendaten nicht auf dem Internet-Rechner speichern.
- Falls doch, dann müssen Patientendaten verschlüsselt abgelegt werden.
- Tägliche Sicherungskopien auf geeigneten Datenträgern herstellen
- Sicherstellen, dass bei Systemzusammenbruch Daten schnell wiederhergestellt werden können
- Bei elektronischer Datenübermittlung ist technisch sicherzustellen, dass kein Unbefugter Zugriff  hat

# Datenschutz-Verhalten „digital“



- Der Berliner Landesdatenschutzbeauftragte*:
  - Email-Verkehr stets mindestens mit Transportverschlüsselung – auch bei Terminabsprachen. (Fragen Sie Ihren IT-Dienstleister)
  - Einwilligung der Pat. in unverschlüsselten Email-Versand genügt nicht.
  - SMS und WhatsApp sind grundsätzlich unsicher und deshalb unzulässig (auch für Termine!)

* Vorab-Mitteilung, Schriftliche Info folgt auf der Homepage der PTK

# Datenschutz-Verhalten „digital“ (2)



- Es gibt sicherere Alternativen zu WhatsApp und Skype, z.B.
  - Threema
    - kostenpflichtig, keine Videoverbindung
  - Signal
    - kostenlos, Video möglich
- Weitere Dienste: Artikel in „connect“
  https://www.connect.de/ratgeber/messenger-dienste-sicherheit-verschluesselung-datenschutz-3197444.html

# Telefon und Fax



- Internet-Telefonie (VoIP):
  keine Bedenken bei Telekom-Unternehmen aus Deutschland und der EU (bei Anbietern außerhalb der EU unzulässig)
- Skype unzulässig
- Fax: Sicherstellen, dass nur der „richtige“ Empfänger Kenntnis nehmen kann

# Webseite



## Datenschutzerklärung ist an DSGVO anzupassen.

### Weitere Hinweise und Muster:

**BPTK:**

http://www.bptk.de/aktuell/einzelseite/artikel/praxishomepa.html

**Datenschutz.org:**

https://www.datenschutz.org/datenschutzerklaerung-website/

# Videoüberwachung



- **Erweiterte Informationspflicht**
- Hinweisschild vor dem Betreten des Bereiches
  - Tatsache der Überwachung, Name des Verantwortlichen, Rechtsgrundlage, Grund und Dauer der Speicherung usw.
- Zusätzlich: Informationsblatt
  - Rechte des Betroffenen auf Auskunft, Löschung usw.
  - Details:

www.lfd.niedersachsen.de/startseite/dsgvo/transparenzanforderungen-und-hinweisbeschilderung-bei-einer-videoueberwachung-nach-der-ds-gvo-158959.html

# Datenschutz-Verhalten „analog“



- Zugang zu DV-Anlagen schützen
  - Nur in verschließbaren Räumen
  - Mobile Datenträger sicher verwahren (Laptop, USB-stick)
  - Bei Verlust: I.d.R.: Meldepflicht (siehe Folie 29)
- Papierdokumente sicher verwahren
  - Nur in verschließbaren Räumen
  - Ausreichend gesicherte Schränke
  - Zugriff nur für Berechtigte sicherstellen
  - Auch vor „zufälliger“ Einsicht schützen!
- Papier und Datenträger sicher entsorgen
  - Aktenvernichter mind. der Stufe 4 (DIN 66399)

# Checkliste der KBV



DAS IST IN PUNCTO

DATENSCHUTZ

ZU TUN:

**www.kbv.de/media/sp/Praxisinformation_Datenschutz_Checkliste.pdf**

# CHECKLISTE: DAS IST IN PUNCTO DATENSCHUTZ ZU TUN

Ab 25. Mai 2018:
Nach der neuen Datenschutz-Grundverordnung der Europäischen Union müssen Ärzte und Psychotherapeuten nicht nur die datenschutzrechtlichen Vorgaben einhalten, sondern dies auch nachweisen.

## ALLE PRAXEN UND MEDIZINISCHEN VERSORGUNGSZENTREN

- ► Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten, die in der Praxis anfallen.
- ► Zusammenstellung der technischen und organisatorischen Maßnahmen, die die Praxis zum Schutz von personenbezogenen Daten ergreift.
- ► Bereitstellung einer Patienteninformation zum Datenschutz in der Praxis, zum Beispiel als Aushang in den Praxisräumen und auf der Praxis-Website.
- ► Verträge zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern anpassen oder neu abschließen. Solche Verträge sind notwendig, wenn Auftragnehmer auf Patienten- oder Mitarbeiterdaten zugreifen können.

## GROßE PRAXEN UND MEDIZINISCHE VERSORGUNGSZENTREN

- ► Beauftragen eines Datenschutzbeauftragten, wenn in der Praxis mindestens zehn Personen regelmäßig personenbezogene Daten automatisiert verarbeiten, zum Beispiel am Empfang oder bei der Abrechnung. Übernimmt ein Mitarbeiter diese Aufgabe, benötigt dieser eventuell eine Schulung.
- ► Melden der Kontaktdaten des Datenschutzbeauftragten der Praxis an die zuständige Aufsichtsbehörde.

## DAS KANN AUßERDEM ERFORDERLICH SEIN

- ► In seltenen Fällen kann eine Datenschutz-Folgenabschätzung nötig sein, zum Beispiel wenn große Mengen an personenbezogenen Daten verarbeitet oder die Praxisräume systematisch videoüberwacht werden. Diese Praxen benötigen unabhängig von ihrer Größe ebenfalls einen Datenschutzbeauftragten.
- ► Praxen, die mit Einwilligungserklärungen des Patienten arbeiten, zum Beispiel zur Weitergabe von Daten an eine privatärztliche Verrechnungsstelle, müssen die Erklärung um einen Hinweis auf Widerrufbarkeit ergänzen.
- ► Praxen, die eine Internet- oder Facebook-Seite anbieten, sollten die Datenschutzerklärung prüfen und gegebenenfalls anpassen; dies gilt ebenso, wenn personenbezogene Daten zum Beispiel über Kontaktformulare oder für einen Praxis-Newsletter erfasst und gespeichert werden.

**Informationen, die Ihnen bei der Erledigung der Aufgaben helfen sollen, finden Sie in der Praxisinformation der KBV „Ab 25. Mai gelten neue Vorschriften zum Datenschutz: Was Praxen jetzt wissen müssen" sowie auf der Internetseite der KBV www.kbv.de/datenschutz.**

Quelle: Kassenärztliche Bundesvereinigung, März 2018

# Online Check



- Empfehlenswert:

  Online-PraxisCheck der KBV zum Stand der Informationssicherheit Ihrer Praxis:

  http://www.kbv.de/html/6485.php

# Weitere Informationen



Infoblatt der Landespsychotherapeutenkammer Baden-Württemberg

**www.lpk-bw.de/sites/default/files/news/2018/dsgvo-lpk-bw-info-praxisinhaber.pdf**

Enthält viele weitere nützliche links

# Hinweis



**Bislang sind viele Regeln der neuen EU-DSGVO noch nicht abschließend rechtlich geklärt. Die vorstehenden Ausführungen enthalten daher teils nur unverbindliche Ratschläge und Empfehlungen. Bitte verfolgen Sie selbst die weiteren Entwicklungen, z. B. auch auf den Webseiten der PTK, der KBV, der BÄK und anderer Institutionen. Fragen Sie auch Ihren IT-Dienstleister.**