PSYCHOTHERAPEUTENKAMMER BERLIN

DATENSCHUTZ IN DER PSYCHOTHERAPEUTISCHEN PRAXIS

STAND 05.09.2018

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

Aus einem Gesetz

- **Erlaubt ist die DV zum Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich…….**

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

Für die psychotherapeutische Praxis heißt das:

Erlaubt sind alle Datenverarbeitungsvorgänge

im Zusammenhang mit Prävention, Diagnostik, Therapie, Nachsorge und zur Erfüllung vertragspsychoth. Pflichten

- **Auskunftspflicht gegenüber Leistungsträgern (Kranken- Unfall- Rentenversicherung - § 100 SGB V)**
- **KV und Krankenkasse (§ 295 SGB V)**
- **MdK (§ 276 SGB V)**

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.

Datenschutzrechtliche Einwilligung

- **Erforderlich nur bei Fehlen gesetzlicher Grundlage, z.B.**
  - **Wenn mit der neuen elektr. Gesundheitskarte freiwillige digitale Anwendungen genutzt werden (Z.B. Patientenakte, Patientenfach d. Telematik)**

- **Für Abrechnung über private Verrechnungsstelle immer notwendig**

Keine Einwilligung notwendig bei gesetzlicher Grundlage

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

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 16 Jahren)
    - Sonst Erklärung d. Sorgeberechtigten (Eltern, Vormund, Pfleger) erforderlich

Muster Einwilligungserklärung

- Kassenärztliche Bundesvereinigung - www.kbv.de/html/datensicherheit.php

- Datenschutz Org www.datenschutz.org/einwilligungserklaerung

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

Rechte der Betroffenen (hier: Patienten)

- Auskunftsrecht über alle sie 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.)

Die Betroffenen sind zu informieren über

- den Namen und die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten,
- den Zweck der Datenverarbeitung,
- die Empfänger der Daten, falls die Daten weitergegeben werden,
- die Dauer der Speicherung der Daten,
- die Rechtsgrundlage,
- die Betroffenenrechte (Artikel 15 bis 21 DSGVO

Art und Weise der Information

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

- Muster Patienteninformation: www.kbv.de/media/sp/Praxisinformation_Datenschutz_Patienteninformation_Muster.docx

PATIENTENINFORMATION ZUM DATENSCHUTZ

MUSTER FÜR IHRE PRAXIS

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach der EU-Datenschutz-Grundverordnung (DSGVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck unsere Praxis Daten erhebt, speichert oder weiterleitet. Der Information können Sie auch entnehmen, welche Rechte Sie in puncto Datenschutz haben.

1. VERANTWORTLICHKEIT FÜR DIE DATENVERARBEITUNG

Verantwortlich für die Datenverarbeitung ist:

Praxisname:

Adresse (Straße, Hausnummer, Postleitzahl, Ort):

Kontaktdaten (z.B. Telefon, E-Mail):

Sie erreichen die/den zuständige/n Datenschutzbeauftragte/n unter:

Name:

Anschrift:

Kontaktdaten:

2. ZWECK DER DATENVERARBEITUNG

Die Datenverarbeitung erfolgt aufgrund gesetzlicher Vorgaben, um den Behandlungsvertrag zwischen Ihnen und Ihrem Arzt und die damit verbundenen Pflichten zu erfüllen.

Hierzu verarbeiten wir Ihre personenbezogenen Daten, insbesondere Ihre Gesundheitsdaten. Dazu zählen Anamnesen, Diagnosen, Therapievorschläge und Befunde, die wir oder andere Ärzte erheben. Zu diesen Zwecken können uns auch andere Ärzte oder Psychotherapeuten, bei denen Sie in Behandlung sind, Daten zur Verfügung stellen (z.B. in Arztbriefen).

Die Erhebung von Gesundheitsdaten ist Voraussetzung für Ihre Behandlung. Werden die notwendigen Informationen nicht bereitgestellt, kann eine sorgfältige Behandlung nicht erfolgen.

3. EMPFÄNGER IHRER DATEN

Wir übermitteln Ihre personenbezogenen Daten nur dann an Dritte, wenn dies gesetzlich erlaubt ist oder Sie eingewilligt haben.

Empfänger Ihrer personenbezogenen Daten können vor allem andere Ärzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern und privatärztliche Verrechnungsstellen sein.

Die Übermittlung erfolgt überwiegend zum Zwecke der Abrechnung der bei Ihnen erbrachten Leistungen, zur Klärung von medizinischen und sich aus Ihrem Versicherungsverhältnis ergebenden Fragen. Im Einzelfall erfolgt die Übermittlung von Daten an weitere berechtigte Empfänger.

4. SPEICHERUNG IHRER DATEN

Wir bewahren Ihre personenbezogenen Daten nur solange auf, wie dies für die Durchführung der Behandlung erforderlich ist.

Aufgrund rechtlicher Vorgaben sind wir dazu verpflichtet, diese Daten mindestens 10 Jahre nach Abschluss der Behandlung aufzubewahren. Nach anderen Vorschriften können sich längere Aufbewahrungsfristen ergeben, zum Beispiel 30 Jahre bei Röntgenaufzeichnungen laut Paragraf 28 Absatz 3 der Röntgenverordnung.

5. IHRE RECHTE

Sie haben das Recht, über die Sie betreffenden personenbezogenen Daten Auskunft zu erhalten. Auch können Sie die Berichtigung unrichtiger Daten verlangen.

Darüber hinaus steht Ihnen unter bestimmten Voraussetzungen das Recht auf Löschung von Daten, das Recht auf Einschränkung der Datenverarbeitung sowie das Recht auf Datenübertragbarkeit zu.

Die Verarbeitung Ihrer Daten erfolgt auf Basis von gesetzlichen Regelungen. Nur in Ausnahmefällen benötigen wir Ihr Einverständnis. In diesen Fällen haben Sie das Recht, die Einwilligung für die zukünftige Verarbeitung zu widerrufen.

Sie haben ferner das Recht, sich bei der zuständigen Aufsichtsbehörde für den Datenschutz zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Die Anschrift der für uns zuständigen Aufsichtsbehörde lautet:

Name:

Anschrift:

6. RECHTLICHE GRUNDLAGEN

Rechtsgrundlage für die Verarbeitung Ihrer Daten ist Artikel 9 Absatz 2 lit. h) DSGVO in Verbindung mit Paragraf 22 Absatz 1 Nr. 1 lit. b) Bundesdatenschutzgesetz. Sollten Sie Fragen haben, können Sie sich gern an uns wenden.

Ihr Praxisteam

Pflichten der Praxisbetreiber zum Datenschutz/Datensicherheit

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

Verantwortlicher für den Datenschutz ist zu benennen

- V. ist verantwortlich
  - für die Gewährleistung des Datenschutzes durch den Einsatz notwendiger technischer und organisatorischer Maßnahmen
  - für die Nachweiserbringung gegenüber der Aufsichtsbehörde
- Eine Person muss dazu bestimmt werden (In Einzelpraxis: der Inhaber)

Verarbeitungsverzeichnisse

- 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 1

Verarbeitungsverzeichnis enthält:

- Name und Kontaktdaten des Verantwortlichen,
- gegebenenfalls Datenschutzbeauftragter
- Zweck der Verarbeitung
- Kategorien betroffener Personen
- Kategorien personenbezogener Daten
- Kategorien von Empfängern und
- vorgesehene Fristen zur Löschung

Verarbeitungsverzeichnis-Inhalt 2

- Pro „Verarbeitungsart“ ein Verzeichnis, z.B.
  - Patientenverwaltung
  - Personalverwaltung
- Verzeichnis verbleibt in der Praxis
- Muster:

www.kbv.de/html/datensicherheit.php

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

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

AUSFÜLLBEISPIEL

Das Muster ist beispielhaft ausgefüllt; aufgeführt sind zwei Verarbeitungstätigkeiten.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN
Rechtliche Grundlage: Artikel 30 Absatz 1 Datenschutz-Grundverordnung
Angaben zum Verantwortlichen
Name: Praxis am Europaplatz Anschrift: Europaplatz 1a, 23456 Platzstadt Telefon: 0123 456789 E-Mail: praxis@europaplatz.de Internet-Adresse: www.europaplatzpraxis.de
Angaben zur Person des Datenschutzbeauftragten
Vorname und Name: Sabine Müller Anschrift: Europaplatz 1a, 23456 Platzstadt Telefon: 0123 456788 E-Mail: datenschutzbeauftragte@europaplatz.de
Verarbeitungstätigkeit
Datum der Anlegung: 20. März 2018 Datum der letzten Änderung: 21. März 2018
Bezeichnung der Verarbeitungstätigkeit
Einsatz und Nutzung des Praxisverwaltungssystems
Zwecke der Verarbeitung
Ärztliche Dokumentation, Abrechnung der ärztlichen Leistungen, Qualitätssicherung, Terminmanagement
Beschreibung der Kategorien betroffener Personen
Patienten
Beschreibung der Datenkategorien
Gesundheitsdaten, gegebenenfalls auch genetische Daten
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden
Intern: Praxispersonal Extern: andere Ärzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern, privatärztliche Verrechnungsstellen

Fristen für die Löschung
10 Jahre nach Abschluss der Behandlung
Verarbeitungstätigkeit
Datum der Anlegung: 18. März 2018 Datum der letzten Änderung: 22. März 2018
Bezeichnung der Verarbeitungstätigkeit
Führen von Personalakten
Zwecke der Verarbeitung
Durchführung von Beschäftigungsverhältnissen
Beschreibung der Kategorien betroffener Personen
Beschäftigte
Beschreibung der Datenkategorien
Personaldaten
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden
Intern: Praxisinhaber Dr. Max Mustermann Extern: Krankenkassen, Finanzämter, Rentenversicherer
Fristen für die Löschung
10 Jahre nach Beendigung des Beschäftigungsverhältnisses

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.
- Im Zweifel rechtlich beraten lassen
- Auf Muster zurückgreifen

Vertragsmuster Auftragsverarbeitung 1

- Berufsverband der Datenschutzbeauftragten Deutschland (bvd) –Arbeitskreis Medizin- (kostenlos)

  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-Folgenabschätzung

- 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
- Beinhaltet eine besondere Abwägung zwischen Notwendigkeit und den Risiken für den Betroffenen bei Verletzung des Datenschutzes

Datenschutz-Folgenabschätzung-Art. 35

Nach Mitteilung der Berliner Landesdatenschutzbeauftragten müssen trotz Verarbeitung besonders sensibler Daten Einzelpraxen PP/KJP keine DSFA vornehmen.

Die schriftliche Mitteilung ist auf der Homepage der PTK veröffentlicht

Datenschutzbeauftragter

- 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
- Für die Einzelpraxis i.d.R. nicht notwendig
- Falls erforderlich:
  Extern oder intern möglich

Datenschutzbeauftragter

- 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
- Für die Einzelpraxis i.d.R. nicht notwendig
- Falls erforderlich:
  Extern oder intern möglich

Zweck des Datenschutzes

- Im Fokus stehen Vertraulichkeit und Integrität der Daten (Art. 32 DSGVO) :
- Vertraulichkeit
  - Information vor Unbefugten verbergen
- Integrität
  - Daten nicht beabsichtigt oder unbeabsichtigt Verändern/Löschen

Maßnahmen zur Datensicherheit

- 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

Maßnahmen im Einzelnen für elektronische und analoge Daten 1

- Datenschutzkonzept für die Praxis aufstellen
  - Wer darf auf welche Daten/Unterlagen zugreifen, wer darf wann löschen/verändern, wie reagiert wer auf Datenpannen
- Mitarbeiter zur Einhaltung zur Einhaltung von Datenschutz und zur Schweigepflicht verpflichten
- Patientendaten nur auf PC, der nicht mit dem Internet verbunden ist, sonst besonders verschlüsseln und leistungsstarke Firewall nutzen
- WLAN mit hohem Sicherheitsstandard (WPA2) und sicherem Passwort (Voreinstellung ändern!)

Maßnahmen im Einzelnen für elektronische und analoge Daten 2

- PCs stets mit sicherem Passwort schützen
  www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
- Betriebssystem und Virenscanner stets aktualisieren
- Schnelle Wiederherstellung der Daten bei Systemproblemen gewährleisten, tägliche Sicherungskopien
- Bildschirme so aufstellen, dass sie nicht von Unbefugten eingesehen werden können (passwortgeschützte Bildschirmsperre mit geringer Zeitspanne!)
- Keine Papierbearbeitung, wenn Unbefugte mitlesen können
- Behandlung grundsätzlich im geschlossenen Raum ohne Mithörmöglichkeit von außen!

Patientendokumentation

- Vor unbefugtem Zugriff sichern (verschlossen aufbewahren)
- Auch vor Beschädigung/Vernichtung schützen
- Aufbewahrungsfrist: 10 Jahre
- Bei elektronischer Führung: PC durch ausreichendes Passwort sichern, System ständig aktualisieren (s.o.), bei unverschlüsselter Ablage PC ohne Internetverbindung

Digitale Kommunikation

- E-Mail
- SMS
- WhatsApp
- Skype
- Internet-Telefonie

E-Mail

- Email-Verkehr unverschlüsselt immer unzulässig
  - Für „unsensiblen“ Inhalt genügt Transportverschlüsselung (z.B. Termin-absprachen ohne Hinweis auf eine psychoth. Behandlung u. mit neutralem Betreff)
  - Für Gesundheitsdaten nur „end-to-end“-Verschlüsselung
    Ersatz: verschlüsselte Datei als Anhang
- Achtung: Einwilligung der Pat. in unverschlüsselten Email-Versand genügt nicht.

SMS und Skype

- SMS Unzulässig –Texte werden auf dem Server der Provider gespeichert
- Skype Unzulässig– Datenweitergabe
- Alternativen für sichere Videoübertragung: Videodienste
  Hinweise unter
  http://www.kbv.de/html/videosprechstunde.php

WhatsApp

- WhatsApp trotz behaupteter Verschlüsselung unzulässig, weil
  - Gesprächsmetadaten gespeichert werden
  - Kontakte ausgelesen und verwendet werden
- Alternativen zu WhatsApp
  - Threema
    - kostenpflichtig (einmalig 3 €)
  - Signal (bedingt)
    - kostenlos

Weitere Infos

- Zur WhatsApp-Thematik allgemein:
  https://www.datenschutzbeauftragter-info.de/whatsapp-sicherheitsrisko-beim-einsatz-im-unternehmen/
- Zu Alternativen:
  Artikel in „connect“
  https://www.connect.de/ratgeber/messenger-dienste-sicherheit-verschluesselung-datenschutz-3197444.html

  und Verbraucherzentrale
  https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-die-datenschutzregeln-im-ueberblick-13055

Telefon und Fax

- Internet-Telefonie (VoIP):
  keine Bedenken bei Telekom-Unternehmen aus Deutschland und der EU (bei Anbietern außerhalb der EU unzulässig)
- Bei Telefonaten Identität des Gesprächspartners sicherstellen (Rückfragen, Rückrufe u.ä.)
- Fax: Sicherstellen, dass nur der „richtige“ Empfänger Kenntnis nehmen kann

Webseite

- **Datenschutzerklärung und Impressum sind an DSGVO anzupassen.**
- **Kontaktformular verschlüsseln**

- **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

Meldepflichten bei Datenpannen

- Datenpannen müssen i.d.R. innerhalb 72 Stunden der Aufsichtsbehörde (Landesbeauftragte für Datenschutz) gemeldet werden, z.B.
  - Hacking-Angriffe, Verlust von Datenträgern, Missachtung des Datenschutzes durch Mitarbeiter u.ä.
  - Bei meldepflichtigen Datenpannen sind betr. Patienten auch dann zu benachrichtigen, wenn keine Risiken für sie zu befürchten sind
- 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

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

- **Infoblatt der Bundespsychotherapeutenkammer**
  https://www.bptk.de/uploads/media/20180727_bptk_praxisinfo_datenschutz-web.pdf

  Beide enthalten viele weitere nützliche links

Hinweis

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