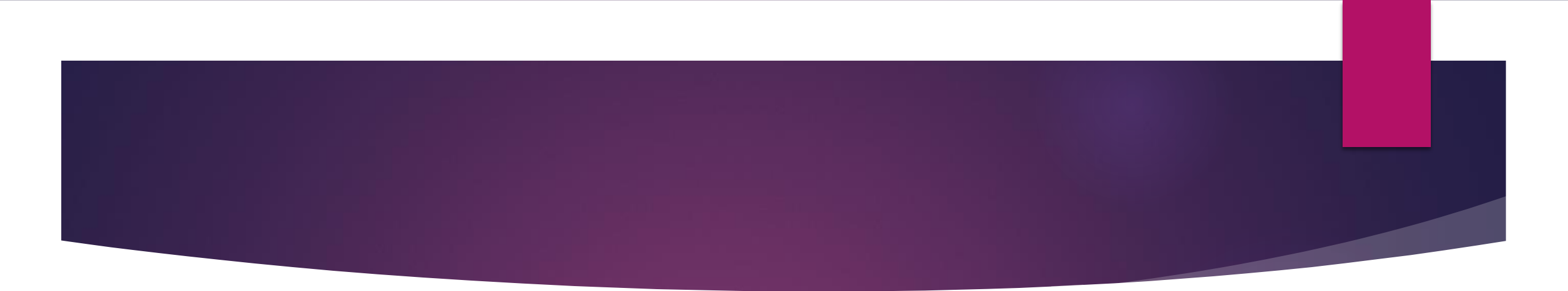


Datenschutzschulung

für die APH, das psib
und das JRI

Aufbau der Schulung

1. Grundlagen
2. Datenschutzziele der Institute / Praxen
3. Wie schützen und verwahren Sie die Daten ihrer Patienten?
4. Wie ist bei einem Datenschutzvorfall vorzugehen?

- 
1. Grundlagen
 2. Datenschutzziele der Institute / Praxen
 3. Wie schützen und verwahren Sie die Daten ihrer Patienten?
 4. Wie ist bei einem Datenschutzvorfall vorzugehen?

Verarbeitung Personen-bezogenen Daten

Personen bezogene Daten, wie der Name, das Alter, der Familienstand, das Geburtsdatum, die Anschrift, die Telefonnummer, sowie Gesundheitsdaten*

*(Anamnesen, Diagnosen, Berichte, Befunde, mitbehandelnde Ärzte)

werden mit oder ohne Hilfe automatisierter Verfahren erhoben, erfasst, gespeichert, angepasst, verändert, ausgelesen, abgefragt, verknüpft, verwendet, bereitgestellt, gelöscht oder vernichtet.

Verbotsprinzip mit Erlaubnisvorbehalt

Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten,

... es sei denn, die Datenverarbeitung ist aufgrund einer gesetzlichen Vorschrift zulässig

... oder der Betroffene hat in diese eingewilligt.

Grundlage der Verarbeitung in der Praxis und im Institut

- ▶ Die Datenverarbeitung erfolgt aufgrund gesetzlicher Vorgaben, um den Behandlungsvertrag und die damit verbundenen Pflichten zu erfüllen.
- ▶ Die Erhebung von Gesundheitsdaten ist Voraussetzung für die Behandlung der Patienten. Werden die notwendigen Informationen nicht bereitgestellt, kann eine sorgfältige Behandlung nicht erfolgen.

Besonderheit eines Aus- und Weiterbildungs-Instituts

Um die Qualität der Aus- und Weiterbildung
und damit der Therapie zu gewährleisten,

werden Informationen über die Therapiesitzungen
an die Ausbilder/Dozenten weitergegeben.

Dokumentation der Patienteninformation

- ▶ Der Patient ist über die Speicherung personenbezogener Daten zum Zwecke der Behandlung zu informieren.
- ▶ Ein Hinweis auf den Aushang „Patienteninformation“ genügt.
Wenn der Patient einen Ausdruck wünscht, sollte dieser über das Sekretariat erhältlich sein.
- ▶ In der Patientenakte muss dokumentiert werden, dass der Patient auf die Patienteninformation zum Datenschutz hingewiesen worden ist.



PATIENTENINFORMATION ZUM DATENSCHUTZ

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 das:

John-Rittmeister-Institut

Stresemannplatz 4

24103 Kiel

Telefon: 0431/8886295

sekretariat@john-rittmeister-institut.de


Sie erreichen den zuständigen Datenschutzbeauftragten unter:

Name: Dr. Thomas Pudelko

E-Mail: Datenschutz@t-pudelko.de

2. ZWECK DER DATENVERARBEITUNG

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



Hierzu verarbeiten wir Ihre personenbezogenen Daten, insbesondere Ihre Gesundheitsdaten. Dazu zählen Anamnesen, Diagnosen, Therapievorschlage und Befunde, die wir oder andere Therapeuten erheben. Zu diesen Zwecken konnen uns auch andere Arzte oder Psychotherapeuten, bei denen Sie in Behandlung sind, Daten zur Verfugung stellen (z.B. in Arztbriefen).

Die Erhebung von Gesundheitsdaten ist Voraussetzung fur Ihre Behandlung. Werden die notwendigen Informationen nicht bereitgestellt, kann eine sorgfaltige Behandlung nicht erfolgen.

In unserem Institut wird die Behandlung hauptsachlich durch Therapeuten in fortgeschrittener Ausbildung (Ausbildung von Psychotherapeuten oder Arzten) durchgefuhrt. Um die Qualitat von Ausbildung und Therapie zu gewahrleisten, werden Informationen uber die Therapiesitzungen an die entsprechenden Ausbilder/Dozenten weitergegeben.

3. EMPFANGER IHRER DATEN

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

Empfanger Ihrer personenbezogenen Daten konnen vor allem andere Psychotherapeuten, Arzte, Kassenarztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Kammern und privatarztliche Verrechnungsstellen sein.

Die ubermittlung erfolgt uberwiegend zum Zwecke der Abrechnung der bei Ihnen erbrachten Leistungen, zur Klarung von therapeutischen und sich aus Ihrem Versicherungsverhaltnis ergebenden Fragen. Im Einzelfall erfolgt die ubermittlung von Daten an weitere berechnigte Empfanger.

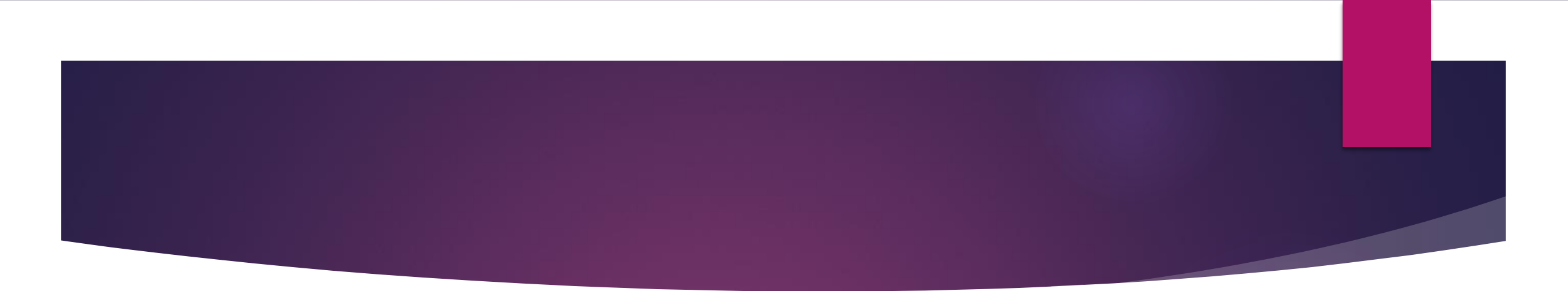
4. SPEICHERUNG IHRER DATEN

Wir bewahren Ihre personenbezogenen Daten nur solange auf, wie dies fur die Durchfuhrung der Behandlung erforderlich ist.

Aufgrund rechtlicher Vorgaben sind wir dazu verpflichtet, diese Daten mindestens 10 Jahre nach Abschluss der Behandlung aufzubewahren. Nach anderen Vorschriften konnen sich langere Aufbewahrungsfristen ergeben, zum Beispiel 30 Jahre.

5. IHRE RECHTE

Sie haben das Recht, uber die Sie betreffenden personenbezogenen Daten Auskunft zu erhalten. Auch konnen Sie die Berichtigung unrichtiger Daten verlangen.

- 
1. Grundlagen
 2. Datenschutzziele der Institute / der Praxen
 3. Wie schützen und verwahren Sie die Daten ihrer Patienten?
 4. Wie ist bei einem Datenschutzvorfall vorzugehen?

Grundsätzliche Datenschutzziele der Institute / Praxen

- ▶ Unbedingte Einhaltung der Vorgaben der EU-Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes, institutseigenen Datenschutzvorschriften und des Telemediengesetzes

durch alle Mitarbeiter, Funktionsträger, Praktikanten, Honorarkräfte, AWT's, Dozenten, Supervisoren und Lehranalytiker sowie Mitglieder.

- ▶ Strikte Verpflichtung zur Geheimhaltung und Vertraulichkeit
- ▶ Unbedingter Schutz vor Dateneinsicht durch Unbefugte
- ▶ Datenschutzkonforme Arbeitsplatzgestaltung

Konkrete Schutzziele der Institute / Praxen

|

Vertraulichkeit und Datensicherheit sind zu gewährleisten!

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden

und

durch angemessene organisatorische und technische Maßnahmen (TOMs) geschützt werden.

Was soll verhindert werden?

- ...ein unberechtigten Zugriff,
- ...eine unrechtmäßige Verarbeitung,
- ...eine Weitergabe,
- ...ein versehentlicher Verlust,
- ...eine Veränderung oder Zerstörung

Konkrete Schutzziele der Institute / Praxen

II

► **Rechtevergabe**

Wo es angezeigt ist, werden Verschlüsselungen, Passwortschutz, Zugriffsrechtevergabe, Zugriffskontrollverfahren und eine Protokollierung administrativer Tätigkeiten durchgeführt.

► **Zeitliche Verfügbarkeit** (Gesicherter Zugriff auf Information innerhalb einer festgelegten Zeit)

Daten werden immer nur den Mitarbeiter, Funktionsträger, Patienten, Praktikanten, Honorarkräfte, Ausbildungskandidaten, Dozenten, Supervisoren und Lehranalytiker oder Mitglieder zur Verfügung gestellt. Sie haben Zugriff auf diese, wenn die Bearbeitung dieser zu den zugewiesenen Aufgaben gehört. Die zuvor Genannten haben unmittelbar auf alle Prozesse und Daten Zugriff, die sie für die Erledigung ihrer Aufgaben benötigen.

Konkrete Schutzziele der Institute / Praxen

III

▶ **Transparenz**

Personenbezogene Verfahren sollen mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können. Die Quelle der Daten ist stets nachvollziehbar und jedem Dateninhaber kann innerhalb kurzer Zeit Auskunft über die sie betreffenden Daten gegeben werden.

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- ▶ die Identität der verantwortlichen Stelle
- ▶ den Zweck der Datenverarbeitung
- ▶ die hinterlegten Aufbewahrungsfristen
- ▶ Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

Konkrete Schutzziele der Institute / Praxen

IV

▶ **Löschung und Speicherbegrenzung**

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden.

▶ **Nichtverkettbarkeit**

Personenbezogene Verfahren müssen so eingerichtet sein, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. Die Zweckbindung wird über alle Prozesse eingehalten.

Konkrete Schutzziele der Institute / Praxen

V

▶ **Intervenierbarkeit**

Personenbezogene Verfahren benötigen Maßnahmen, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen. Neben der Auskunft über die sie betreffenden Daten ist gewährleistet, dass eine Korrektur einer angemahnten falschen Information unverzüglich an allen Stellen des Systems erfolgen kann.

▶ **Qualitative Verfügbarkeit**

Die Arbeit des John-Rittmeister-Instituts stützt sich auf eine reibungslos funktionierende Datenverfügbarkeit. Durch redundante Speichersysteme, Sicherheitskopien, Clustersysteme oder Ausweichzentren ist eine hohe Qualität der Verfügbarkeit gewährleistet.

Konkrete Schutzziele der Institute / Praxen

VI

▶ **Fairness und Rechtmäßigkeit**

Bei der Verarbeitung personenbezogener Daten muss das informationelle Selbstbestimmungsrecht des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

▶ **Zweckbindung**

Daten werden nur für den Zweck ihrer Erhebung verarbeitet und gespeichert. Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

Konkrete Schutzziele der Institute / Praxen

VII



Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.



Rechenschaftspflicht

Die oberste Leitung kann jederzeit die Einhaltung der hier beschriebenen Datenschutzziele nachweisen. Die oberste Leitung kann jederzeit über Datenverarbeitungszwecke, den Verbleib von Daten bei Weitergabe und Löschfristen einzelner Dateninhaber Auskunft geben.

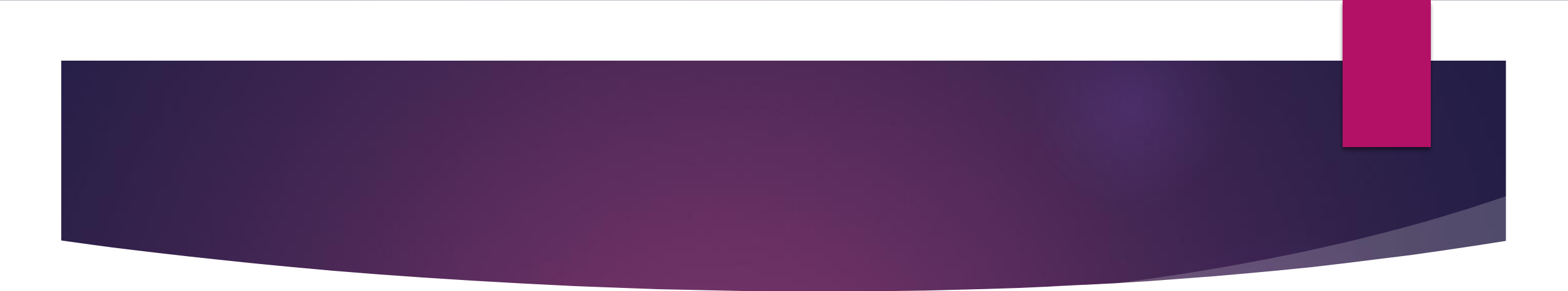
Konkrete Schutzziele der Institute / Praxen

VIII

- ▶ **Zuständigkeit**

Im Institut / in der Praxis sind die Aufgaben und Zuständigkeiten hinsichtlich der Erreichung dieser Ziele klar geregelt.

- ▶ Es gibt es eine Datenschutzleitlinie die allgemein bekannt ist und deren Umsetzung wird durch Organisationsregeln gewährleistet.

- 
1. Grundlagen
 2. Datenschutzziele des JRI
 3. Wie schützen und verwahren Sie die Daten ihrer Patienten?
 4. Wie ist bei einem Datenschutzvorfall vorzugehen?

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Organisatorische Maßnahmen I

- ▶ Bewahren Sie Aufzeichnungen über Patienten oder sonstige im Behandlungskontext stehenden Materialien stets verschlossen auf (Zwei-Schranken-Prinzip).
- ▶ Patientendaten werden niemals unverschlüsselt über das Internet versendet, beispielsweise per E-Mail.
- ▶ Verwenden Sie für die Kommunikation über und mit Patienten nur sichere Kommunikationswege.
- ▶ Beachten Sie: öffentlicher W-LAN-Netze sind in der Regel unsicher und ein Einfallstor für Hackerangriffe.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten Organisatorische Maßnahmen II

- ▶ Zugriffsberechtigungen sind vergeben. Somit ist klar geregelt, wer in der Praxis auf Dateien und Ordner zugreifen kann.
- ▶ In den Praxisräumlichkeiten wird auf Diskretion geachtet: Die Anmeldung ist getrennt vom Wartebereich.
- ▶ Patientenunterlagen werden so positioniert, dass andere Patienten diese nicht einsehen können. Wenn der Behandler nicht im Raum ist, werden Patientenakten generell unter Verschluss gehalten.
- ▶ Jede Person, die in Ihrer Praxis Daten verarbeitet, muss sich nach der Nutzung eines Gerätes abmelden oder das Gerät sperren.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Organisatorische Maßnahmen III

- ▶ Es ist festgelegt, wann und durch wen personenbezogene Daten gelöscht beziehungsweise vernichtet werden. Patientenakten werden nach DIN-Normen vernichtet.
- ▶ Es ist festgelegt, was bei Datenpannen und Datenschutzverstößen zu tun ist und wer die Meldung übernimmt (Meldung in der Regel an die zuständige Aufsichtsbehörde innerhalb von 72 Stunden).
- ▶ Die Mitarbeiter in der Praxis wurden über die Einhaltung von Schweigepflicht und Datenschutz informiert.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Technische Maßnahmen I

- ▶ Schutz vor Verlust von Daten: Es ist notwendig regelmäßige Backups auf eine externe verschlüsselte Festplatte zu erstellen (nach Möglichkeit automatisiert).

Für den Fall von z.B. Bränden und Wasserschäden ist es idealerweise sinnvoll das Backup und den Computer nicht am gleichen Ort zu lagern.

- ▶ Nutzerprofil (Konto) sollte mit einem starken Passwort versehen sein.

Passwortrichtlinie

- ▶ Passwörter sind geheim zu halten (nicht in Dateien speichern oder in einer Weise vorhalten, die eine Kenntnisnahme Dritter möglich macht).
- ▶ Die Passwörter sind im Hinblick auf ihre Länge und ihre Komplexität entsprechend den Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) zu wählen.
- ▶ Ein passwortgeschützter Bildschirmschoner ist zu aktivieren. Er muss so konfiguriert sein, dass er nach kurzer Zeit den Zugriff auf das angemeldete Endgerät verhindert. Der Bildschirmschoner ist ggf. manuell zu aktivieren.

BSI- Passwort Empfehlung

▶ **Kurzes, komplexes Passwort:**

Mindestens acht Zeichen, vier Zeichenarten (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen)

▶ **Langes, weniger komplexes Passwort:**

Mindestens 25 Zeichen, nur zwei Zeichenarten (z.B. Groß- und Kleinbuchstaben)

Umsetzungsbeispiel: tisch_himmel_kenia_blau_pfannkuchenteig_lachen

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Technische Maßnahmen II

- ▶ Richten Sie sich auf Ihren Computer für Patientendaten im Kontext Ihrer Ausbildung-Weiterbildung einen besonders geschützten Bereich ein (sog. Containerlösung), der separat verschlüsselt und mit einem zusätzlichen starken Passwort versehen ist.

Container erstellen

- ▶ Für Windows Rechner z.B mit dem kostenlosen Programm „VeraCrypt“

Anleitung für die Installation: <https://www.rz.uni-wuerzburg.de/dienste/it-sicherheit/it-arbeitsplatzsicherheit/schritt-fuer-schritt-anleitung-veracrypt/>

- ▶ Für Apple Rechner folgender Hinweis:

Das APFS-Dateisystem (Apple File System) ordnet den Festplattenspeicher bedarfsorientiert zu. Das System kann passwortgeschützt werden.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Technische Maßnahmen III

- ▶ Der Computer mit einem Nutzerprofil ohne Administratorenrechte verwenden.
- ▶ Grundsätzlich: Firewall und Defender nutzen, regelmäßige Updates, alles ausstellen, was Daten erhebt!
- ▶ Für Windows Rechner: Windows pro nutzen.
Unter dem Menüpunkt „Einstellungen können Sie den Bereich „Datenschutz“ und Bereich „Sicherheit“ anwählen.
- ▶ Für Apple Rechner: Systemeinstellungen / „Sicherheit“

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Technische Maßnahmen IV

- ▶ Deaktivieren Sie die in Office Produkten integrierten Cloud-Speicher zur Speicherung personenbezogener Informationen.
- ▶ Verwenden Sie kein Microsoft 365 (ehemals Office 365) und kein OneDrive.
- ▶ Vermeiden Sie Office-Produkte, die Rohdaten sammeln und per automatischer Datenübertragung durch einen im Hintergrund laufenden Dienst an den Entwickler übertragen.
- ▶ Nutzen Sie lokal installierte Office-Produkte ohne „integrierte Cloud“-Speicherungen.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Technische Maßnahmen V

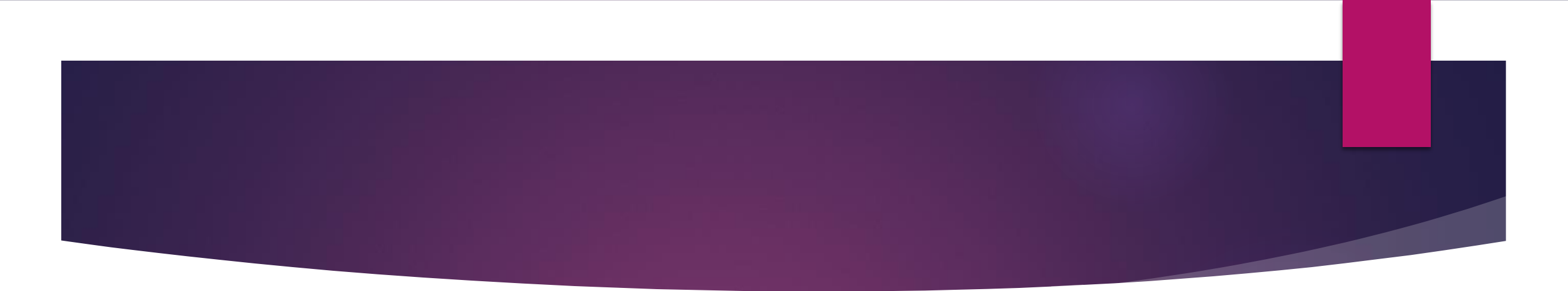
- ▶ Ihr Internet-Browser soll so eingestellt sein, dass im Browser keine vertraulichen Daten gespeichert werden.
- ▶ • Verwenden Sie zum Löschen der Browserdaten die folgenden Tastenkombinationen: „Strg“ + „Umschalt“ + „Entf“ bei Chrome, Firefox, Edge; „cmd“ + „alt“ + „E“ bei Safari.
- ▶ Verwenden Sie Browser wie “Firefox Klar“, die diese Daten mit einem Klick oder nach Beendigung der Anwendung automatisch löschen.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Technische Maßnahmen VI

- ▶ In Ihrer Praxis werden Apps nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden.
- ▶ Die Smartphones und Tablets Ihrer Praxis sind mit einem komplexen Gerätesperrcode geschützt.
- ▶ In Ihrer Praxis werden verschlüsselte Internetanwendungen genutzt. (Achten Sie auf Internetseiten, die mit „https://“ beginnen)

- 
1. Grundlagen
 2. Datenschutzziele der Institute
 3. Wie schützen und verwahren Sie die Daten ihrer Patienten?
 4. Wie ist bei einem Datenschutzvorfall vorzugehen?

Datenschutzvorfall

I

- ▶ Es besteht eine Meldepflicht innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde.
- ▶ Eine Meldepflicht wird indes nicht ausgelöst, wenn voraussichtlich kein Risiko für die Rechte und Freiheiten der betroffenen Patienten besteht, weil Maßnahmen zur Schadenseindämmung nachweisbar ergriffen worden sind.
- ▶ Sofern eine meldepflichtige „Datenpanne“ vorliegt, müssen auch die betroffenen Patienten unverzüglich in klarer und einfacher Sprache benachrichtigt werden, wenn ein Risiko für ihre persönlichen Rechte und Freiheiten wahrscheinlich erscheint.
- ▶ Eine Benachrichtigung ist entbehrlich, wenn geeignete technisch-organisatorische Maßnahmen (z. B. eine Verschlüsselung) ausschließen, dass ein Schaden für Patienten eintreten kann oder wenn wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden.

Datenschutzvorfall

I

- ▶ Eine Verletzung des Schutzes personenbezogener Daten liegt in jeder Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
- ▶ Informieren Sie unverzüglich die Person Ihres Ausbildungsinstitutes / Praxis, die für solche Fälle benannt wurde.

Bitte senden Sie dieses Formular umgehend und vollständig ausgefüllt in einer Kopie auch an den Datenschutzbeauftragten. Es dient dem Nachweis gegenüber der Aufsichtsbehörde und erleichtert das Ausfüllen des Meldebogens an die Aufsichtsbehörde

Dr. Thomas Pudelko,
datenschutz@tpudelko.de

1. Detaillierte Sachverhaltsschilderung

2. Wer ist Verantwortlicher?

3. Zeitraum oder Zeitpunkt des Vorfalls

4. Zeitpunkt der Feststellung des Vorfalls

5. Ursache des Vorfalls

6. Ort des Vorfalls

7. Art der Verletzung

8. Kategorien der betroffenen Personen

9. Anzahl der betroffenen Personen / betroffenen

10. Kategorien der personenbezogenen Daten

- | | | |
|---|--|--|
| <input type="checkbox"/> Gesundheit | <input type="checkbox"/> E-Mail-Adressen | <input type="checkbox"/> Standort |
| <input type="checkbox"/> Bank- oder Kreditbereich | <input type="checkbox"/> Passwörter | <input type="checkbox"/> Fotos/Videos |
| <input type="checkbox"/> Religion | <input type="checkbox"/> Berufsgeheimnis | <input type="checkbox"/> Sonstiges |
| <input type="checkbox"/> Sexualität | <input type="checkbox"/> Adressen | <input type="checkbox"/> Straftaten oder |
| <input type="checkbox"/> Weltanschauung | <input type="checkbox"/> Biometrie | Ordnungswidrigkeiten |

11. Zu welchem Zweck wurden die in Ziffer 10 genannten Daten verarbeitet

12. Wann und wie wurden die betroffenen Personen über den Datenschutzvorfall unterrichtet?

13. Angaben zur Auftragsverarbeitung

Zur Durchführung der Verarbeitungstätigkeit werden Auftragsverarbeiter herangezogen:

Ja Nein

Falls ja: Benennen Sie die Auftragsverarbeiter

14. Mögliche Folgen und Auswirkungen der Datenschutzverletzung für die betroffenen Personen

- Verlust der Kontrolle über ihre personenbezogenen Daten
- Einschränkung ihrer Rechte
- Diskriminierung,
- Identitätsdiebstahl oder -betrug
- finanzielle Verluste
- unbefugte Aufhebung der Pseudonymisierung
- Rufschädigung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person

Ausführliche Beschreibung der möglichen Auswirkungen für die betroffenen Personen:

15. Erläuterung zu eingeleiteten Sicherheitsmaßnahmen bzw. geplanten Sicherheitsmaßnahmen nach dem Datenschutzvorfall, um die betroffenen Personen zu schützen

16. Erläuterung, in wie weit, die eingeleiteten Maßnahmen zu einer Minderung der nachteiligen Folgen für die betroffenen Personen führen

17. Erläuterung zu vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen des Verantwortlichen

Die Daten sind verschlüsselt:

Ja Nein

Falls ja: Welcher Verschlüsselungsalgorithmus wurde verwendet:

Falls nein: Nennen Sie andere technische und organisatorische Maßnahmen, die zum Schutz der in Ziffer 10 bis 14 genannten Daten ergriffen wurden:

Diesem Meldeformular sind folgende Anlagen beigefügt:

Beschreibung der Verarbeitungstätigkeit aus Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO (Verantwortlicher)

Beschreibung der Verarbeitungstätigkeit aus Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO (Auftragsverarbeiter)

Dokumentation zur Datenschutz-Folgenabschätzung nach Art. 35 DSGVO

Ort, Datum

Vorname und Nachname

Unterschrift



Vielen Dank für Ihre Aufmerksamkeit