ärzte genossenschaft **Nord eG**

**Medizin verbindet.** menschlich | politisch | wirtschaftlich

# Sicherer Umgang mit den Daten in Ihrer Praxis -

# 11 kritische Praxissituationen


**Ärztliche Leitung:**

Herr Dr. med. Klaus Bittmann, äg Nord

**Referenten:**

Frau Nicole Schwäbe, Trainingsakademie LAT

Herr Lars Konuralp, ONKOCONSULT



LAURENTIS ONLINE-SEMINARE von: Lernen und anwenden TRAININGSAKADEMIE LAT & ONKOCONSULT

# Heute geht es um .....

ärzte genossenschaft **Nord eG**
**Medizin verbindet.** menschlich | politisch | wirtschaftlich

## Datenschutz und Datensicherheit in Arztpraxen
## Ein Tag in den Praxen Dr. Sorglos und Dr. Obacht

**Hinweis**: Unsere Empfehlungen stellen keine abschließende Darstellung von Maßnahmen für den Einzelfall dar. Es ersetzt nicht die individuelle eigene Analyse und Maßnahmenfestlegung.

**Haftungsausschluss**

Trotz sorgfältiger Prüfung sämtlicher Inhalte dieser Präsentationen sind Fehler und Irrtümer der Quellen und der Inhalte nicht auszuschließen. Die Richtigkeit, Vollständigkeit und Aktualität des Inhalts sind daher ohne Gewähr. Eine Haftung der Referenten, auch für die mit dem Inhalt verbundenen potenziellen Folgen, insbesondere wirtschaftliche Verwertbarkeit und Vermögensschäden, ist ausgeschlossen.

Bildmaterial: Freepic, Eigenes Fotoarchiv

LAURENTIS
ONLINE-SEMINARE

# Gesetzliche und normative Anforderungen

- BDSG
- DSGVO
- MBO
- Vertragsarztrecht
- BGB
- StGB
- SGB V

**Es besteht eine Nachweispflicht / Rechenschaftspflicht** bei der Umsetzung der gesetzlichen Anforderungen!

Das bedeutet:
Alles was die Praxis zum Datenschutz und Datensicherheit tut, **sollte dokumentiert werden**

LAURENTIS
ONLINE-SEMINARE

# MFAs starten die Rechner an der Anmeldung

## Das 2 Türen-Prinzip:

Frau Tide, MFA Anmeldung

**Tür 1**: Hier melden sich alle MA und Ärzte bei Windows mit einem gemeinsamen Kennwort an – *PraxisSORGlos123*

**Tür 2**: Für Turbomed hat jede MA und jeder Arzt sein individuelles Passwort.

Frau Tide z.B. 123*schönerTag*

## Das 3 Türen Prinzip:

Frau Bulut, MFA Anmeldung

**Tür 1**: Rechner werden entschlüsselt mit einem einheitlichen Passwort: *211r09Xz!*

**Tür 2 und 3**: Jede Ärztin hat ein eigenes Passwort für Windows. Für die MFAs gibt es Arbeitsplatz-Zugänge, z.B. Anmeldung, Diagnostik, Labor. Für Turbomed hat jeder Mitarbeiter sein individuelles Passwort.

Passwörter müssen mind. 10 Zeichen haben, Sonderzeichen, Zahlen und Buchstaben (s. BSI Empfehlungen)

# Ein sicheres Passwort – einfach erstellen

Passwörter etwa für E-Mail-, Social Media- und Cloud-Accounts schützen sensible persönliche Daten vor unerlaubtem Zugriff. Deshalb sollten sie besonders komplex und schwierig zu erraten sein.

## Dos

- ✓ Je länger, desto besser: Passwortlänge von mindestens acht Zeichen wählen
- ✓ Groß- und Kleinbuchstaben verwenden
- ✓ Sonderzeichen wie ?, !, %, +, _ etc. nutzen
- ✓ Mehrere Ziffern hinzufügen

## Don'ts

- ✗ Passwort-Kombinationen vermeiden, die Geburtstage bzw. Namen des Haustiers enthalten oder in einem Wörterbuch stehen.
- ✗ Auf gängige Wiederholungs- und Tastaturmuster wie asdf, 1234, abcd, 666 etc. verzichten.
- ✗ Nicht ein simples Passwort wählen, das nur um ein Sonderzeichen am Wortanfang oder -ende ergänzt ist, zum Beispiel: !Pizza.

*Bei Reisen ins Ausland können Umlaute auf landestypischen Tastaturen eventuell nicht genutzt werden.*

# Risiken in der Praxis Dr. Sorglos

- PC und Server sind nicht verschlüsselt
  → Diebstahl, Entwendung der Hardware
- Passwörter sind nicht sicher genug
- Zugangsrechte sind teilweise nicht ausreichend geregelt:

  Für größere Praxen empfiehlt es sich ein **zentral verwaltetes Benutzermanagement** zu verwenden. Die Administrationsrechte und die Benutzerrechte sind getrennt.

  **Dies ist wichtig, weil:** Mitarbeiter können **keine** Änderungen vornehmen, keine Software installieren, keine Einstellungen ändern, nicht auf vertrauliche Ordner zugreifen, keine Dokumente löschen

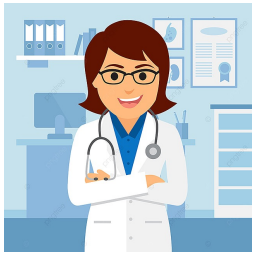
ABER : PVS-Zugang ist gut geregelt: **Nachweisbarkeit der MFA-Tätigkeiten** bei Delegation von ärztlichen Leistungen (Einarbeitung und Qualifikation der Mitarbeiterinnen, Nachvollziehbarkeit der durchgeführten Tätigkeiten, z.B. Blutentnahme, Injektionen, EKG)

# MFAs melden sich ab

Frau Tide, MFA Anmeldung

2 MFA an der Anmeldung

- Zugang zum Turbomed bleibt offen, wenn MFA den Arbeitsplatz kurz verlässt; es wird der Bildschirmschoner aktiviert
- Andere MFA nutzen teilweise den Account von Frau Tide
- Abmelden nur am Feierabend oder Mittagspause



Frau Bulut, MFA Anmeldung

3 MFA an der Anmeldung

- MFA melden sich beim Verlassen des Arbeitsplatzes bei Turbomed immer ab, Windows +L
- Klare Anweisung: Fremde Accounts dürfen nicht genutzt werden
- Neue MA werden eingewiesen, Arbeitsanweisung An- und Abmelden PC

# Risiken in der Praxis Dr. Sorglos

- Eingaben im Terminkalender, Abrechnungsziffern, Einträge in der Patientenakte können nicht eindeutig zugeordnet werden. Haftungsrechtlich kritisch – *Welche MFA hat was gemacht?*
- Bei den diag. Untersuchungen / Labortätigkeiten kann nicht eindeutig nachgewiesen werden, wer die Tätigkeit gemacht hat (qualifiziert, eingewiesen, eingearbeitet?)
- Zugriff von Unbefugten auf PC (z.B. im Untersuchungszimmer)

IT-Sicherheitsrichtlinie KBV nach 75b SGB V, Anlage 1, **Ziffer 13** (Abmelden nach Aufgabenerfüllung) und **Ziffer 17** (Endgeräte mit Betriebssystem Windows: Datei- und Freigabeberechtigung; *Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person)*

BMV-Ä, Anlage 24, Vereinbarung über die Delegation ärztlicher Leistungen an nichtärztliches Personal in der ambulanten vertragsärztlichen Versorgung gemäß § 28 Abs.1 SGB V, Stand 1.1.2015

# Einarbeitung der neuen Mitarbeiterinnen

- Praxismanagerin Frau Reimers ist verantwortlich für die Einarbeitung
- Eigene Übersicht, um nichts zu vergessen
- Alle Kolleginnen arbeiten die neue Kollegin mit ein
- Ausgebildete MFA, weiß was zu tun ist
- Bei Rückfragen ist Frau Reimers ansprechbar
- In den Teamsitzungen lernt die Neue auch dazu

- Frau Seibert als PM nutzt ausführliche Checkliste und Einarbeitungsplan
- Durch einen Behandlungsfehler sensibilisiert zum Thema Nachweisbarkeit
- Willkommensmappe mit: QM-Dokumenten wie AA, Datenschutz, Hygieneplan, etc.
- Neue MA müssen CL unterschreiben
- Auch angestellte Ärztinnen durchlaufen die Einarbeitung

# Risiken in der Praxis Dr. Sorglos

- Ohne Einarbeitungskonzept keine strukturierte Einarbeitung
- Themen können vergessen werden
- Zuständigkeiten sind nicht klar geregelt - Jede macht ein bisschen was
- Kein Nachweis der Einarbeitung (Unterschrift der Mitarbeiterin)
- Keine Überprüfung der Qualifikation der neuen Mitarbeiterin
- Haftungsrechtlich kritisch - DSGVO Artikel 24 und Delegation ärztliche Leistungen an nichtärztliches Personal
- Im Schadensfall könnte es zum Verlust des Versicherungsschutzes kommen

DSGVO, Art 24, Art. 32 - BMV-Ä, Anlage 24, Vereinbarung über die Delegation ärztlicher Leistungen an nichtärztliches Personal in der ambulanten vertragsärztlichen Versorgung gemäß § 28 Abs. 1 S. SGB V, Stand 1.1.2015, M-BO (Muster-Berufsordnung), Vertragsarztrecht

| Praxis<br>*LOGO einfügen* | Checkliste<br>**Einarbeitung neue Mitarbeiter** | | | |
|---|---|---|---|---|
| | Erstellt:<br>Datum: | Freigabe: | Version & Datum: V1.0 – 12.10.2021<br>Gültig bis: | Seite 1 |

Diese Einarbeitungscheckliste ist Teil der Einarbeitungsdokumentation.

| | |
|---|---|
| Bereich: | Datenschutz und -sicherheit in der Praxis |
| Verantwortlich: | Praxismanagerin |

**Die Verantwortung kann auch aufgeteilt werden: IT-Abteilung/ Dienstleister, DSB, Praxisleitung**

**Mitarbeiterin: Frau** **Beginn am:**

| Themen und Inhalte der Einarbeitung | Datum | Verantwortlich | Unterschrift neue MA |
|---|---|---|---|
| **Thema Datenschutz und Datensicherheit** | | | |
| **Belehrung und Verpflichtung Schweigepflicht**<br>(QM-Dokument: Belehrung über die Verschwiegenheit (Schweigepflicht) und die Verpflichtung auf die Wahrung des Datengeheimnisses) | | | |
| **Zugangsrechte und Passwortvergabe:** Entschlüsselung der Rechner, Windows, PVS, Online-Terminkalender<br>Sichere Passwörter | | | |
| Einweisung in die Arbeitsanweisungen zur **Nutzung der EDV** (Netzwerk, Internet, Mail, etc.) und den Umgang mit Geschäftsgeheimnissen | | | |

| Praxis<br>*LOGO einfügen* | Checkliste<br>**Einarbeitung neue Mitarbeiter** | | | |
|---|---|---|---|---|
| | Erstellt: | Freigabe: | Version & Datum: V1.0 – 12.10.2021 | |
| | Datum: | | Gültig bis: | |

**Die Verantwortung kann auch aufgeteilt werden: IT-Abteilung/ Dienstleister, DSB, Praxisleitung**

| Themen und Inhalte der Einarbeitung | Datum | Verantwortlich | |
|---|---|---|---|
| **Einwilligungserklärung** zur Veröffentlichung von Fotos und Profil auf Praxis-Website | | | |
| **Schulung / Unterweisung** zur Datensicherheit und zum Datenschutz planen | | | |
| **Arbeitsplatz Anmeldung**<br>• Patienteninformation zum Datenschutz, inkl. Rechte<br>• Auskünfte über Patienten<br>• Auskünfte am Telefon<br>• Patientenidentifikation<br>• Umgang mit Patientendokumentation<br>• Vernichtung von Daten (Shredder, sichere Papiertonne)<br>• Umgang Fax<br>• Sicherer Umgang E-Mail<br>• Umgang Internet<br>• Online-Terminvergabe | | | |
| **Verhalten im Notfall**, Datenpanne oder Verstoß gegen den Datenschutz | | | |
| Verhalten bei **Auskunfts- und Einsichtsverlangen der Patienten** | | | |
| **Bei Home-Office**: Datensicherheit gem. Richtlinie sicherstellen, Zugang, BYOD-Vereinbarung (eigene Gerätenutzung) | | | |
| ..... | | | |

# Ausscheiden / Kündigung der Mitarbeiterinnen

- Langjährige MFA verlässt die Praxis
- Vertrauensverhältnis verwässert manchmal den Einsatz von Checklisten

- Frau Yilmaz hat Fortbildung zum On- und Offboarding besucht.
- Gute Grundlage für ein strukturiertes Personalmanagement
- Zusammen mit PM, QMB, IT und DSB wurde Checkliste erstellt

# Risiken in der Praxis Dr. Sorglos

- Zugangsdaten und Passwörter könnten missbräuchlich verwendet oder weitergeben werden
- Ggf. personenbezogene oder private Daten der ausgeschiedenen Mitarbeiterin im System für alle sichtbar

# Nicht vergessen

- Personalakte prüfen: Fortbildungsnachweise, Einweisungsnachweise der letzten 2 – 3 Jahre sollten vorliegen
- Newsletter, Zugang zu fachlichen Portalen abmelden
- Zugänge und Passwörter
- Mailkonto (Weiterleitung der Mail oder Autoresponder)
- Neues Bitlocker Kennwort (Entschlüsselung der PC)
- Website: Mitarbeiterprofil, Fotos
- Kommunikations-APP der Praxis

**Diese Checkliste ist Teil der Checkliste *Ausscheiden von Mitarbeitern***

| | |
|---|---|
| Bereich: | Personalmanagement |
| Verantwortlich: | Personalverantwortliche |

**Mitarbeiterin: Frau** **Arbeitsvertrag endet am:**

| Themen | Was ist zu tun | Erledigt / Notizen | Unterschrift |
|---|---|---|---|
| **Thema EDV, Endgeräte und Datensicherheit** | | | |
| Zugang zur IT<br>Zugangsrechte sperren | Vertragsende der Mitarbeiterin an IT-Dienstleister mitteilen zur Sperrung des Zugangs zu Windows und Turbomed<br>Autoresponder einrichten für Mail-Postfach | | |
| Rückgabe der Endgeräte (Diensthandy, Laptop, Tablet, USB-Stick, Festplatten, Token) | Sicherstellen, dass die Passwörter der Praxis zur Verfügung stehen<br>PIN und PUK der SIM-Karte | | |
| Schlüsselabgabe<br>Elektronische Zeiterfassung, Token | Abgabe mit Rückgabeprotokoll und Unterschrift | | |
| Website | Mitarbeiterprofil und Fotos der Mitarbeiterin löschen | | |





| Themen | Was ist zu tun | Erledigt / Notizen | Unterschrift |
|---|---|---|---|
| Personalakte | Zusätzliche Aufbewahrung:<br>Fortbildungsnachweise<br>Unterweisungsnachweise<br>Schulungsnachweise | | |
| Zugänge der Mitarbeiterin sperren<br>Bekannte Passwörter ändern | Abos, Newsletter, Datenbanken,<br>Mailinglisten,<br>Kommunikation-APP (Sijlo, Signal) | | |
| ..... | | | |

# Anforderung eines Befundberichts aus einer anderen Praxis ohne Überweisung

- Man kennt sich
- Zeitdruck an der Anmeldung
- Das haben wir schon immer so gemacht

- Anrufe werden in der Telefonzentrale angenommen
- Klare Anweisung der MA zum Datenschutz
- Lösungsvorschlag

# Risiken in der Praxis Dr. Sorglos

- Keine klare Identifizierung der Patientin – Verwechselungsgefahr
- Verletzung der Schweigepflicht ohne Einwilligung der Patientin
- Kritischer Versandweg: Das FAX
- Datenschutzschulung durchgeführt, aber Mitarbeiterin hält sich nicht daran

DSGVO, Art. 7,9, BDSG § 22, MBO

# Praxis Dr. Obacht fordert Unterlagen in einer anderen Praxis an

Diese Inhalte müssen in einer Erklärung zur Schweigepflichtentbindung enthalten sein:

- **Wer übermittelt?** (Name, Anschrift der anderen Praxis / KH)
- **Wessen Daten?** (Name des Patienten)
- **An wen?** (Name, Anschrift Dr. Obacht)
- **Welche Daten?** (Was wird konkret angefordert / Datenumfang)
- **Wofür?** Zu welchem Zweck (Mit- oder Weiterbehandlung)
- Für Patient: **Hinweis auf Freiwilligkeit**
- Für Patient: Hinweis auf **Möglichkeit des Widerrufes**

  Beispiel: *Ich gebe diese Erklärung freiwillig ab. Mir ist bekannt, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft ohne Angabe von Gründen widerrufen kann.*

Quelle: ULD, Unabhängiges Landeszentrum für Datenschutz, SH

# Auszug BÄK KBV

## Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

Stand: 9.3.2018

**2.4.1. Schweigepflichtentbindung durch Einwilligung**

Die ausdrücklich oder konkludent erteilte Einwilligung des Patienten ist nur wirksam, wenn sie auf der freien Willensbildung und Entscheidung des Patienten beruht. Hierzu muss der Patient wissen, zu welchem Zweck er den Arzt legitimiert, patientenbezogene Informationen weiterzugeben. Die Einwilligung ist nur gültig, wenn sie hinreichend konkret bestimmt ist. Nicht ausreichend ist es daher, wenn beim Abschluss eines Behandlungsvertrages pauschal für alle denkbaren Fälle der Datenweitergabe eine vorweggenommene Einwilligungserklärung des Patienten eingeholt wird.

**Keine pauschale Einwilligungserklärung für Datenweitergabe**

***Keine Schriftform, Hervorhebung, Widerrufbarkeit***

Die Einwilligung kann schriftlich, in Textform, elektronisch oder mündlich erteilt werden. Wegen der Nachweis- und Rechenschaftspflicht[45] ist es jedoch ratsam, dass die Einwilligung schriftlich eingeholt wird.

**Schriftliche Einwilligung ratsam**

# Übermittlung von Patientendaten aufgrund gesetzlicher Bestimmungen (Offenbarungspflicht)

- Kassenärztliche Vereinigungen (Abrechnungsdaten, Befunde bei Plausibilitätsprüfungen, Stichproben zur Qualitätssicherung)
- Gesetzliche Krankenkassen – ABER nur auf dem vereinbarten Vordruck! (Wiedereingliederungsplan, Fortbestehen AU, etc.)
- MDK (Befunde nur direkt mit Vordruck)
- Weitergabe an BG
- ..... weitere ausführliche Informationen unter:

# Auskünfte nur mit Schweigepflichtsentbindung

Sozialamt

Arbeitsgeber

Eltern bei Einsichtsfähigkeit des Jugendliche / keine starre Altersgrenze

Privatärztliche Verrechnungsstellen

Hausarztzentrierte Versorgung

Agentur für Arbeit

Ehepartner

Rentenversicherung

Übermittlung bei Praxisverkauf

.....

LAURENTIS
ONLINE-SEMINARE

# Datenschutz am Telefon & Identifikation von Anrufern

- Ungenügende Abstandsregelung im Anmeldebereich
- Wartende Patienten hören Telefongespräche mit
- Ansprache des Patienten mit Namen
- Abfrage des Geburtsdatums mit Wiederholung der Angaben
- Offenbarung der Diagnose
- Wiederholung der persönlichen Daten des Anrufers, inkl. Grund des Anrufs bei Durchstellung zum Arzt

- Anrufer wird durch festgelegtes Verfahren geprüft und identifiziert
- Wahrung der Verschwiegenheit
- Überprüfung der Telefonnummer des Patienten
- Rückrufvereinbarung
- Rückruf vom der Ärztin

# Risiken der Praxis Sorglos

- Ungenügende Feststellung der Identität des Anrufers
- Offenbarung von persönlichen Daten des Anrufers an Patienten im Anmeldebereich
- Unberechtigte telefonische Übermittlung von Gesundheitsdaten an Dritte
- **Achtung:** Datenschutzverstoß kann vom betroffenen Patienten bei der Aufsichtsbehörde angezeigt werden
- Überprüfung der Praxis auf Einhaltung und Umsetzung der DSGVO seitens Aufsichtsbehörde:
  1. **Bitte um Stellungnahme**
  2. **Prüfung der Schutzmaßnahmen (z. B. TOMs)**
  3. **Festlegung von Bußgeld**

**Die angezeigte fahrlässige Herausgabe oder Offenbarung von personenbezogenen Daten an unberechtigte Dritte zieht gemäß Art. 83 DSGVO, hier insbesondere Absatz b), g) und h) i.d.R. eine Geldbuße nach sich**

# Checkliste Telefon

- **Eindeutige Anruferidentifikation**
  Abfrage des Namens, Geburtsdatums und des Patientenkennworts bzw. letzten 4 Ziffern der Versichertenkarte
- **Passive Identifizierung**
  Name, Geburtsdatum, Telefonnummer werden nicht aktiv kommuniziert. Der Patient ist der Informationsüberbringer
- **Wahrung der Verschwiegenheit**
  Keine Herausgabe von Diagnosen oder anderen medizinischen Daten ohne Rücksprache mit Praxisverantwortlichen oder behandelnden Arzt/Ärztin
- **Rückruf vereinbaren**
  Sofern eine datenschutzkonforme Telefonie am Anmeldebereich nicht möglich ist - Patient ist älter, Name muss von MFA wiederholt werden - Durchstellung ins Back Office bzw. Verweis auf Rückruf

# Umgang mit Emails - Kommunikation mit den Patienten

- Anhänge werden ungeprüft geöffnet, gespeichert und verarbeitet
- Keine Überprüfung der Identität des Versenders
- Medizinische Auskünfte per Mail
- Arztbriefe und medizinischen Daten werden an Patienten versendet
- Kein standardisierter Prozess zur Verarbeitung und Beantwortung von E-Mails

- Praxis-E-Mails auf dem praxiseigenen Notebook
- Anhänge werden nicht geöffnet
- Prüfung und Abgleich der Identität des Absenders mittels PVS
- Klare Handlungsanweisung zur Bearbeitung von eingehenden Anfragen
- Einrichtung von Rückruflisten

# Risiken der Praxis Dr. Sorglos

- Schadsoftware in E-Mail Anhängen führt zur Infizierung des PCs, ggfs. der gesamten Praxis-IT
- Unberechtigte Dritte haben Zugriff auf das Postfach des Patienten (Familie, Ehepartner)
- Offenbarung von Patientendaten an Unberechtigte
- Keine eindeutige Identifikation des Patienten
- Datenschutzverstoß bei fahrlässigem Umgang mit Patientendaten

**Hinweis:**
Das Thema Kommunikation mit Patienten per E-Mail wird von den Aufsichtsbehörden der Länder teilweise unterschiedlich ausgelegt. Aktuell gibt es keine gemeinsame abschließende Empfehlung.
Im Zweifel ist der Verzicht auf diesen Kommunikationsweg oder die Rückspracht mit der zuständigen Behörde die sichere Variante.

# E-Mail Archivierung Good to know

**Was muss archiviert werden?**
Alle Daten, die für die Besteuerung relevant sind

(z. B. Buchungsbelege, Geschäftskorrespondenz, Eingangsrechnungen)

**Wie muss archiviert werden?**
Elektronisch und rechtssicher mittels Softwarelösungen, die eine vollständige, manipulationssichere und jederzeit verfügbare Archivierung von E-Mails ermöglichen

**Wie lange muss archiviert werden?**
Je nach Art der E-Mail bis zu 10 Jahre

**Gesetzesgrundlagen:**
- § 90 Absatz 3, 141 bis 144 AO
- 22 UStG, § 4 Absatz 3 Satz 5, § 4 Absatz 4a Satz 6, § 4 Absatz 7
- 41 EStG

**Was darf nicht archiviert werden?**
Bewerbungen – Löschung nach max. 6 Monaten, E-Mails mit schützenswerten Inhalten

Grundlage für die Archivierung ist die **GoBD**
(Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff)

https://www.arzt-wirtschaft.de/praxis/buchhaltung/e-mails-ab-ins-elektronische-archiv/
https://www.it-recht-kanzlei.de/recht-archivierung-email.html?print=1

# Ransomware - Blick nach Draußen

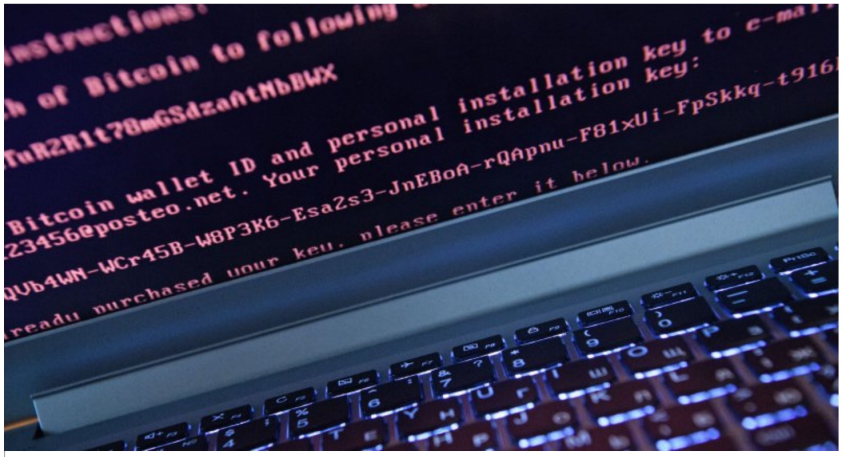
## Ransom - Lösegeld

Vermischtes

### Lösegeldforderung: Rechner in Arztpraxis verschlüsselt

Donnerstag, 1. August 2019

Newsletter abonnieren | Zur Startseite




/dpa

Kaiserslautern – Unbekannte Täter haben den Computer in einer Arztpraxis in Kaiserslautern sabotiert und Lösegeld verlangt. Wahrscheinlich sei Ransomware in einer E-Mail mit angeblichen Bewerbungsunterlagen versteckt gewesen, teilte die Polizei heute mit.

Als der Arzt die Datei vorgestern geöffnet habe, verschlüsselte das Schadprogramm Daten auf dem PC. Für die Entsperrung wurde Lösegeld in elektronischer Währung verlangt.

Der Arzt nahm vorsichtshalber den Computer vom Netz. Ob noch andere Rechner in der Praxis betroffen sind, war zunächst unklar. Derzeit gibt es laut Polizei noch keinen Hinweis, dass Daten gestohlen wurden.

heise online

### Ransomware legt Verwaltung von Schwerin und benachbartem Landkreis lahm

15.10.2021 16:43 Uhr Volker Briegleb


(Bild: aslysun/Shutterstock.com)

**In der Nacht wurde auf Systemen des kommunalen IT-Dienstleisters eine Ransomware entdeckt und daraufhin alles heruntergefahren. Bürgerämter sind geschlossen.**

In Schwerin und dem angrenzenden Landkreis Ludwigslust-Parchim hat offenbar ein Verschlüsselungstrojaner weite Teile der öffentlichen Verwaltung lahmgelegt. Die Schadsoftware wurde in der vergangenen Nacht auf den Systemen des kommunalen Unternehmens KSM/SIS entdeckt, das die IT-Dienste für die Verwaltung der Landeshauptstadt Mecklenburg-Vorpommerns und den Landkreis sowie Versorgungsbetriebe stellt. In Schwerin tagt ein Krisenstab, die Sicherheitsbehörden wurden hinzugezogen.

"Unser kommunale IT-Dienstleister KSM/SIS hat seit heute Nacht einen Angriff mit einer Schadsoftware registriert und musste daraufhin sämtliche IT-Systeme des Verbundes herunterfahren", sagte der Schweriner Oberbürgermeister Rico Badenschier (SPD). Zu weiteren Einzelheiten machen die Verantwortlichen derzeit noch

# Schadsoftware in E-Mails – Ransomware

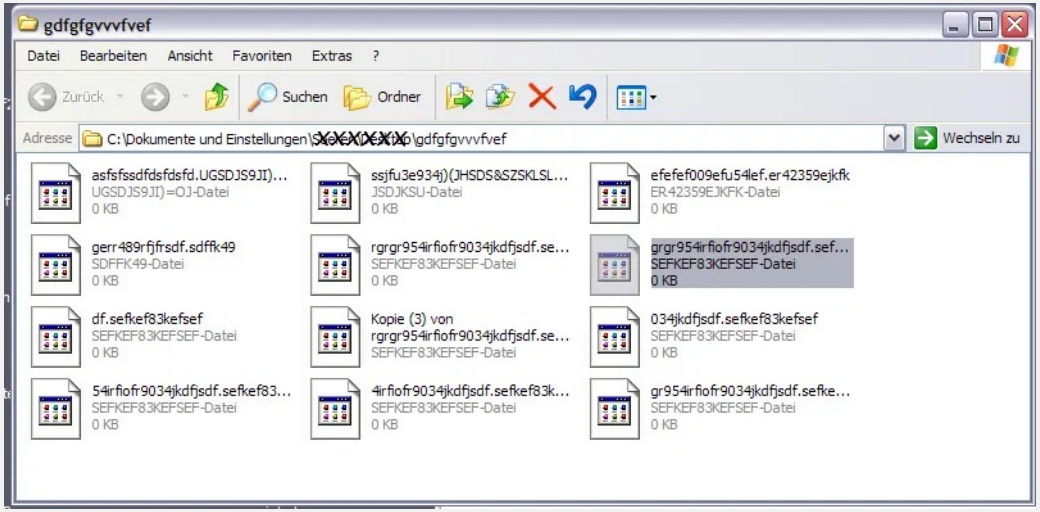
Die Praxen haben online und in der lokalen Presse eine Stellenanzeige geschaltet. Gesucht wird eine MFA. Bewerbungen können postalisch und via E-Mail geschickt werden.

- Routinemäßige Sichtung von eingegangene E-Mails in Outlook auf Arbeitsplatz-PC
- PC ist mit dem Praxisnetzwerk verbunden
- E-Mail Eingang inkl. Anhang mit dem Betreff „Bewerbung“
- Öffnen des Anhangs (Bewerbung.docx) nach erster Sichtung des Anschreibens
- Bestätigung zur Aktualisierung der Word-Version, um den Anhang lesen zu können
- Das Word-Dokument bleibt leer bzw. enthält nicht lesbare Zeichen
- Aktivierte Schadsoftware beginnt unbemerkt mit der Infizierung des Systems und des Netzwerks

- Sichtung von E-Mails auf dem praxiseigenen Notebook in Outlook
- Getrennter Zugang: Praxisnetzwerk und Internet
- Prüfung von E-Mails auf Plausibilität durch Checkliste
- Fehlende Kontaktdaten im Anschreiben der Mail als Negativ-Merkmal
- Online Recherche nach Namen der Bewerberin ergebnislos
- Anhänge im Word-Format werden gemäß Arbeitsanweisung grundsätzlich nicht geöffnet.
- Die E-Mail wird verworfen

# Makro Aktivierung in schadhaftem Office-Dokument

# Folgen einer Infektion durch Ransomware




## Systemverschlüsselung durch Schadsoftware

Mögliche Folgen:

- Auslesen von Passwörtern
- Datendiebstahl


## Lösegeldforderung der Hacker zur Herausgabe des Entschlüsselungskeys

# Prüfen Sie **BAAA**

- **Prüfung des Betreffs!**
  Ist dieser zu allgemein gehalten? Rechtschreibfehler? Kein Betreff?
- **Prüfung des Absenders!**
  Passt der Name des Absenders zur E-Mail-Adresse? Wirkt die Adresse plausibel?
- **Prüfung des Anschreibens!**
  Ist der Inhalt fehlerfrei, sowohl grammatikalisch als auch inhaltlich? Enthält das Anschreiben Kontaktdaten des Absenders? Wenn ja, telefonische Rückversicherung beim Absender einholen (bestenfalls über Festnetz)
- **Prüfung des Anhangs!**
  Sind der E-Mail-Dokumente angehängt worden? Welche Formate haben diese? Wirken die Bezeichnungen der Anhänge plausibel?
  Keine Aktivieren von Makros bei Aufruf eines Anhangs!

**Grundsätzlich gilt:**
**E-Mail Anhänge** von unbekannten Absendern werden nicht geöffnet

LAURENTIS
ONLINE-SEMINARE

# Schadhafte E-Mails erkennen – **Phishing**

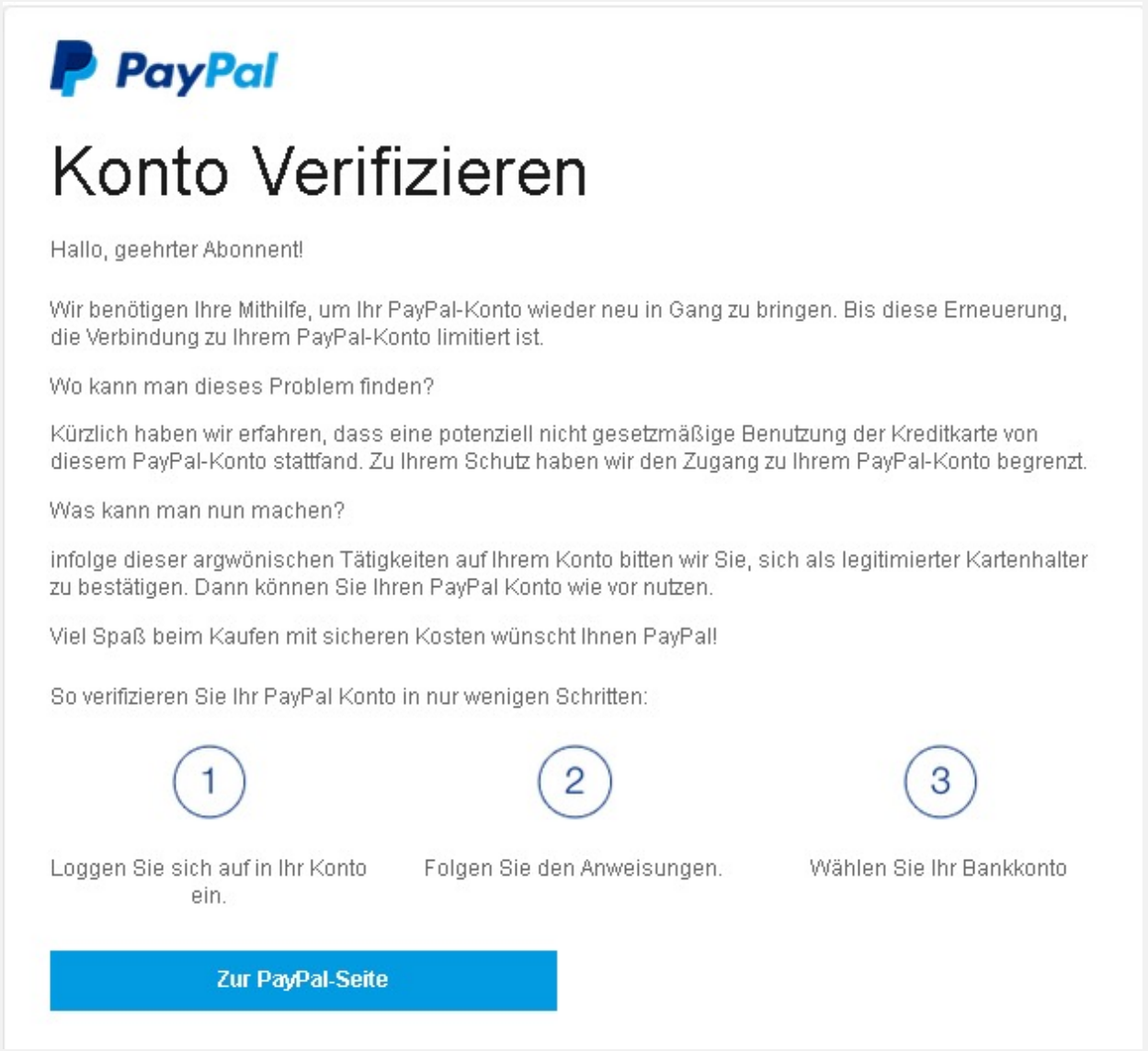
**Password harvesting fishing**

- Onlinebestellung eines Druckers
- Zahlung über PayPal
- Stunden später Mail von PayPal mit der Bitte um Kontoverifizerung
- Klick auf Verifizierungslink in der E-Mail
- Im Browser öffnet sich die vermeintliche PayPal Seite
- Eingabe der persönlichen Zugangsdaten
- Erfolgreicher Datenklau durch Cyberkriminelle

- Onlinebestellung von Drucker-Toner
- Bezahlung im Shop mittels PayPal
- Bestätigung der Zahlung mittels 2-Faktor-Authentifizerung
- Stunden später E-Mail Eingang von PayPal
- Prüfung der Absenderadresse
- Abklärung des E-Mail-Inhalts mit IT-Betreuer
- E-Mail wird verworfen

LAURENTIS
ONLINE-SEMINARE

# PayPal Phishing E-Mail



PayPal

Konto Verifizieren

Hallo, geehrter Abonnent!

Wir benötigen Ihre Mithilfe, um Ihr PayPal-Konto wieder neu in Gang zu bringen. Bis diese Erneuerung, die Verbindung zu Ihrem PayPal-Konto limitiert ist.

Wo kann man dieses Problem finden?

Kürzlich haben wir erfahren, dass eine potenziell nicht gesetzmäßige Benutzung der Kreditkarte von diesem PayPal-Konto stattfand. Zu Ihrem Schutz haben wir den Zugang zu Ihrem PayPal-Konto begrenzt.

Was kann man nun machen?

infolge dieser argwönischen Tätigkeiten auf Ihrem Konto bitten wir Sie, sich als legitimierter Kartenhalter zu bestätigen. Dann können Sie Ihren PayPal Konto wie vor nutzen.

Viel Spaß beim Kaufen mit sicheren Kosten wünscht Ihnen PayPal!

So verifizieren Sie Ihr PayPal Konto in nur wenigen Schritten:

1 Loggen Sie sich auf in Ihr Konto ein.

2 Folgen Sie den Anweisungen.

3 Wählen Sie Ihr Bankkonto

Zur PayPal-Seite

# Merkmale Phishing E-Mail

Durch geschickte psychologische Manipulation und/oder Social-Engineering soll das Phishing Opfer zum Handeln aufgefordert werden

- **Dringlichkeit** (Bitte handeln Sie umgehend! Dringender Hinweis! Wichtige Passwortüberprüfung!)
- **Interesse** wecken (Bewerbungen, Rückmeldung zur weiteren Planung, Corona-Informationen)
- **Autorität** (Absprachen, Meeting-Anfragen)
- **Routine** (Personalplanung, Gehaltsabrechnungen zur Prüfung, Steuerberatung)

**Auch hier gilt die BAAA-Regel**

# Cyberangriff

Bewerbung via E-Mail mit Word-Anhang *Bewerbungsanschreiben*

- Öffnen des Word-Dokuments
- Aktivierung der Makros
- Übersehen der Warnmeldung der Antivirensoftware
- Anzeichen einer Infektion durch fehlerhafte Programmen und verschwindende Dokumenten werden fehlinterpretiert
- Ahnungsloses Vorgehen zur Fehlerbehebung (Neustart der PCs und Server)
- Verspäteter „Hilferuf“ an die IT-Betreuung
- Rücksicherung aus fehlerhaftem Backup nur eingeschränkt möglich

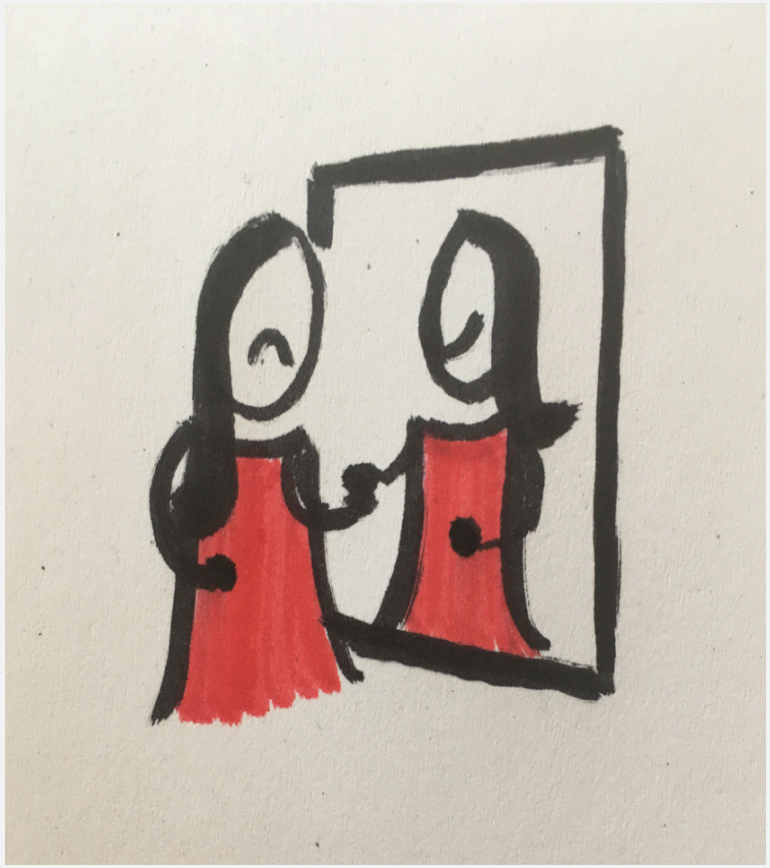
- Analyse der E-Mail auf Anzeichen für Schadsoftware (Awareness)
- Checkliste zur Überprüfung der Kriterien schädlicher E-Mails
- Löschen der E-Mail
- Rückmeldung an Team und Dr. Obacht

# Risiken in der Praxis Dr. Sorglos

- Verschlüsselung des Arbeitsplatz-PCs
- **Worst Case:** Verschlüsselung aller PCs und Server
- Entschlüsselung der Systeme nur möglich nach Zahlung eines Lösegelds
- Datenklau durch weitere Schadsoftware (E-Mail Konten, Kontakte, Passwörter, Patientendaten)
- Erpressung und/oder Offenbarung von Praxisdaten (Gesundheitsdaten)
- IT-Stillstand in der Praxis. Es können keine Patienten mehr versorgt werden
- Wiederherstellung kosten- und zeitintensiv
- Defekte und veraltete Datensicherungen ungenügend zur Wiederherstellung
- Verpflichtung zur Information der betroffenen Patienten über Datenschutzvorfall
- Information an die Aufsichtsbehörde und ggfs. Bußgeldzahlung

# Verhalten Cyberangriff - Sofortmaßnahmen

- Ruhe bewahren!
- Isolierung des befallenen Gerätes vom Netzwerk
- Herunterfahren der gesamten Praxis-PCs und Server
- Parallel Kontakt zum Systemhaus bzw. IT-Betreuung
- Sofortige Überprüfung des Backup-Mediums
  und physikalische Trennung vom Server
- Offline Virenscan der gesamten Praxis-PCs und Server durch IT-Betreuung
- Feststellung der Schäden
- Falls notwendig: Wiederherstellung der Systeme mittels Backup
- Ggfs. Meldungspflicht an die Datenschutz-Aufsichtsbehörde



!!! **AWARENESS** und nichts als **AWARENESS** !!!

Das schwächste Glied der schützenden Kette von Maßnahmen zur Abwehr von Cyberangriffen sitzt direkt vor dem Bildschirm!

Ein gesundes Misstrauen ist der erste und wichtigste Schritt zur Abwehr von digitalen Angriffen!

# Good to know – Messenger

Messenger Apps für die Kommunikation im Praxisteams
werden immer beliebter!

Die Vorteile liegen auf der Hand:

- Schnelle und direkte Kommunikation untereinander
- Erstellung von Gruppen (MFAs, Ärzte, Praxismanagement)
- Einfache Absprachen (Urlaubsplan, Vertretung, Krankmeldung)
- Unterstützung Hausbesuchen  (z. B. Dokumentation der Wundheilung)

Aber auch hier gilt! Die Einhaltung des Datenschutzes ist zu gewährleisten!

**DESWEGEN: „SAY NO TO WhatsAPP“**
**WARUM**: Durch Analyse der Metadaten bei der Nutzung von WhatsApp werden Sie und Ihr Verhalten ausgeleuchtet (Social-Profiling, Geo-Tracking)
**ALTERNATIVEN:** Na klar, und das sogar DSGVO-konform
z. B. mit den Apps **Threema, Signal oder Siilo**

# Patientin fordert Patientenakte an – Auskunfts- und Einsichtsrecht

- Eingehendes Auskunftsverlagen wird unmittelbar zugesagt
- Keine tiefergehende Prüfung der Identität der Anruferin
- Kompletter Datenexport der digitalen Akte in ein ZIP-Archiv
- Versand der Akte als E-Mail-Anhang an hinterlegte E-Mail Adresse

- Anruferidentifikation
- Dokumentation der Anfrage im PVS
- Rücksprache mit Praxisleitung
- Bearbeitung des Auskunftsersuchens gemäß Arbeitsanweisung und TOMs
- Persönliche Übergabe der Patientenakte in analoger Form
- Kopie wird digital mit verschlüsseltem und passwortgesichertem USB-Stick an die Patientin übergeben

# Risiken der Praxis Sorglos

- Die Anruferin ist nicht Patientin, sondern Tochter, Bekannte, etc.
- Akte wird nicht an berechtigte Person ausgehändigt
- Gesundheitsdaten werden unberechtigten Dritten offenbart
- Unvollständige Bereitstellung der Patientenakte, da analoge „Daten“ nicht enthalten sind
- Unsicherer Versand via E-Mail, da Datenarchiv nicht verschlüsselt und passwortgeschützt ist
- Dritte könnten Zugriff auf E-Mail Anhang erhalten und Akte einsehen

**Bei unterlassener oder nicht vollständiger Auskunft sind Sanktionen seitens der Aufsichtsbehörde möglich.**
**Art. 83 Abs. 5 b) DSGVO**

**Art. 5 Abs. 1a), Art. 12, Art. 15 - 22 DSGVO im speziellen Art. 15**
**630g BGB**

LAURENTIS
ONLINE-SEMINARE

# Patientin fordert Ihre Patientenakte an – Auskunfts- und Einsichtsrecht

**Akteneinsicht gemäß § 630g BGB**

Patienten steht einklagbarer Rechtsanspruch auf **Akteneinsicht** in und Auskunft aus sämtlichen den Patienten betreffenden Krankenakten zu.

**Verweigerung** des Einsichtsrechts nur in wenigen Fällen möglich (erhebliche therapeutische Gründe oder erhebliche Rechte Dritter).

Einsichtsrecht ist nicht „ausschließliches“ personengebundenes Recht. **Übertrag der Rechte** des Patienten auf Dritte (z. B. Verwandte oder Ehepartner) mittels Vollmacht möglich.

# Prüfung des Vorgangs

# AA erstellen

| Praxis<br>*LOGO einfügen* | Arbeitsanweisung<br>Bearbeitung eines Auskunfts- und Einsichtsbegehrens von Patienten | | | |
|---|---|---|---|---|
| | Erstellt: | Freigabe: | | |
| | Gültig bis: | | Version & Datum: V1.0 - 30.06.19 | Seite 1 von 1 |

**Bearbeitung eines Auskunfts- und Einsichtsbegehrens von Patienten**

**Immer erste Rücksprache mit der Praxisleitung. Nie Daten ohne Rücksprache rausgeben!**

1. **Identitäts- und Anspruchsprüfung der Patientin**
   Abfrage des Geburtsdatums und weiterer Identitätsmerkmale
   - Bei Zweifel und/oder Unklarheit bitte um persönliche Vorstellung in der Praxis
   - Sofern keine Daten der ersuchenden Person vorhanden sind, weil die Person nie in der Praxis in Behandlung war, muss an die Person eine Rückantwort erfolgen mit dem Hinweis auf *Unbekannt in der Praxis*.

2. **Dokumentation der Anfrage in der Patientenakte**
   Wie wurde die Anfrage gestellt? Telefonisch, schriftlich, per E-Mail? Wie wurde identifiziert? Welche Patientendaten liegen vor und wo und wie sind diese gespeichert (digital & analog)?

3. **Prüfung auf Auskunftsverweigerung**
   Verletzung schutzwürdiger Rechte Dritter bei Auskunft? Auskunftsverlangen exzessiv?

4. **Durchsicht der Akte und Ausschluss von subjektiven Eindrücken des Behandlers**
   Schwärzung von Passagen

5. **Gewährleistung von sicherer Aktenübergabe** Keine Weitergabe an unbefugte Dritte. Ggfs. Prüfung einer Vollmacht

6. **Einhaltung von Fristen** Sofern die unmittelbare Aufbereitung und/oder Herausgabe der Akte nicht möglich ist, darf eine maximale Bearbeitungszeit von einem Monat geltend gemacht werden. Die Patientin ist schriftlich über diesen Vorgang zu informieren!

# Aufbewahrungsfristen und Patientendaten löschen

QMB und DSB treffen sich auf einer Fortbildung

Sie fragen sich:

Muss man eigentlich auch die digitale Karteikarte irgendwann löschen?
Wie macht man das?

LAURENTIS
ONLINE-SEMINARE

# Aufbewahrungsfristen und Löschkonzept im Patientenverwaltungssystem

Analoge und digitale Patientendaten sind min. 10 Jahre nach Abschluss der Behandlung aufzubewahren ( eigene und externe Befunde)

z.B. Patientenkartei (nach der letzten Behandlung), z. B. ärztliche Aufzeichnungen einschließlich Untersuchungsbefunde, Laborergebnisse, Befundmitteilungen z. B. über EEG, EKG, Röntgendiagnostik, Sonographie, Durchschriften von Arztbriefen (eigene und fremde)

Die Daten sich sicher aufzubewahren.

Achtung: Digitale Daten müssen bis zur Löschung lesbar sein.

**Auslegungshinweise**



**ABER:**
Eine Aufbewahrung **aller** Patientendaten für die Dauer von 30 Jahren wegen drohender Schadenser-satzansprüche wäre nicht daten-schutz-konform. Erforderlich ist hier eine individuelle Risiko-bewertung.

| | |
|---|---|
| **Frage** | Wann darf oder muss ein Arzt die Daten seiner Patienten löschen? |
| **Norm** | Art. 17 DSGVO |
| **Stichworte** | Löschen von Patientendaten |
| **Antwort** | Die Datenlöschung richtet sich nach Art. 17 DS-GVO.<br><br>Danach sind personenbezogene Daten insbesondere zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 lit. a DSGVO). Eine Löschpflicht besteht hier auch ohne Aufforderung durch den Betroffenen.<br><br>Sollte für die Erreichung des Zwecks, für den die Daten erhoben wurden, die Aufbewahrung noch notwendig sein, muss nicht gelöscht werden. Dies kann insbesondere dann der Fall sein, wenn die Gesundheitsdaten wichtige Informationen enthalten, von denen davon ausgegangen werden kann, dass für diese auch nach Ablauf gesetzlicher Aufbewahrungsfristen das Interesse des Berechtigten an der Speicherung das an der Löschung überwiegt, beispielsweise im Hinblick auf Medikamentenunverträglichkeiten.<br><br>Nicht gelöscht werden dürfen Daten, für die eine gesetzliche Pflicht zur Aufbewahrung besteht nach Art. 17 Abs. 3 DS-GVO. Insbesondere nach § 630 f Abs. 3 BGB besteht eine gesetzliche Aufbewahrungsfrist von 10 Jahren nach Abschluss der Behandlung. Darüber hinaus gibt es Normen, die eine weitergehende Aufbewahrung gebieten, wie beispielsweise § 28 Abs. 3 RöV.<br><br>Eine Ausnahme von der Verpflichtung zur Löschung kann sich zudem aus Art. 17 Abs. 3 lit. e DS-GVO ergeben, da die objektive Verjährungsfrist für Schadensersatzansprüche wegen Körper- oder Gesundheitsverletzung gemäß § 199 Abs. 2 BGB dreißig Jahre nach Vornahme des potentiell schadensträchtigen Verhaltens beträgt. Hier ist eine Abwägung („erforderlich“) vorzunehmen unter Berücksichtigung der Interessen des Betroffenen und der Wahrscheinlichkeit der Geltendmachung von Ansprüchen. |

# 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

**Alle Löschfristen sind im Verzeichnis zur Datenverarbeitung dokumentiert**

# Digitale Karteikarten löschen

- Löschkonzept des PVS-Anbieters erfragen
- Löschung nachweisbar darstellen und dokumentieren lassen
- Jedes PVS hat einen anderes Löschkonzept

§ 630f Abs 3 BGB, DSGVO, Art. 17, § 57 BMV-Ä, § 10 Berufsordnung

LAURENTIS
ONLINE-SEMINARE

# Empfehlungen – Machen Sie **regelmäßig...**

- Prüfungen und Aktualisierung der Datenschutzdokumente wie das Verzeichnis der Datenverarbeitungsvorgänge, Technisch-organisatorische Maßnahmen (analog der QM-Dokumentation!)
- Schulungen und Unterweisungen der Mitarbeiter
- Immer wieder Thema in Teamsitzungen – Awareness
- Datenschutz-Audits
- Regelmäßige Besprechungen  zwischen DSB, QMB, IT-Dienstleister, Praxisleitung
- Kontakt zur Datenschutzbehörde

# Quellen und weitere Informationen

**Quellen:**

- Vereinbarung über die Delegation ärztlicher Leistungen an nichtärztliches Personal in der ambulanten vertragsärztlichen Versorgung gemäß § 28 Abs. 1 S. 3 SGB V - https://www.kbv.de/media/sp/24_Delegation.pdf
- KVB, Datenschutz in der Arzt- / Psychotherapeutenpraxis, Okt. 2018
- Muster Verpflichtung Mitarbeiter (Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung) https://www.kvb.de/fileadmin/kvb/dokumente/Praxis/Formulare/A-D/KVB-FORM-Verpflichtungserklaerung-Datenschutz.pdf
- BÄK, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, März 2018
- BÄK, Technische Anlage, Juni 2018
- ULD – Tätigkeitsbericht 2021, https://www.datenschutzzentrum.de/tb/tb39/index.html

**Bei Rückfragen oder Unterstützungsbedarf nehmen Sie gern Kontakt mit uns auf:**
**Nicole Schwäbe, schwaebe@trainingsadademie-lat.de**
**Lars Konuralp, info@onkoconsult.de**

LAURENTIS
ONLINE-SEMINARE

# Noch was zu lesen



# Tipps

**Tipps:**

- www.bsi-fuer-buerger.de
- KBV: Online Selbstcheck zur Datensicherheit: www.kbv.de/html/mein_praxischeck.php
- ULD, Selbst-Check für Arzt- / Zahnarztpraxen, Mai 2018, https://www.datenschutzzentrum.de/uploads/medizin/arztpraxis/SelbstcheckArztpraxisDSGVO2018-05-23.pdf
- Podcasts: Auslegungssache – der ct-Datenschutz Podcast; Rechtsbelehrung - Recht, Technik, Gesellschaft; Ärztetag –Podcast für Ärzte (Redaktion Ärztezeitung)

**Bei Rückfragen nehmen Sie gern Kontakt mit uns auf:**
**Nicole Schwäbe, schwaebe@trainingsadademie-lat.de**
**Lars Konuralp, info@onkoconsult.de**

LAURENTIS
ONLINE-SEMINARE