
# Datenschutz in Pflegeeinrichtungen

Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

Veranstaltung des bad e.V.
21.10.2019, Kiel

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



## *Überblick*

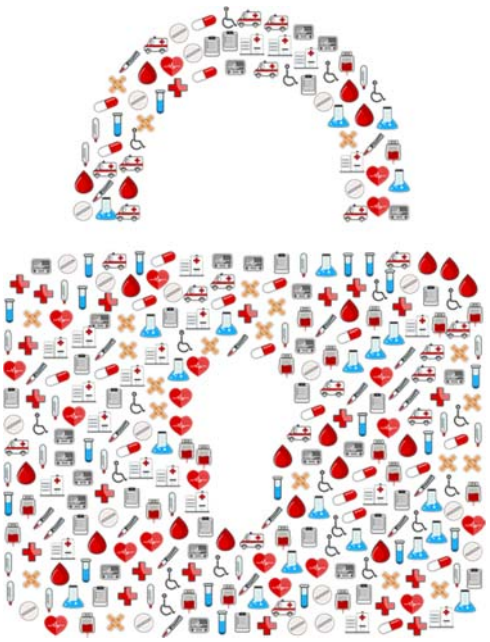


Bild: Gordon Johnson via Pixabay

1. **Datenschutz**
2. **Die Datenschutz-Grundverordnung**
3. **Hilfestellung zur Umsetzung in der Pflege**
4. **Fazit**

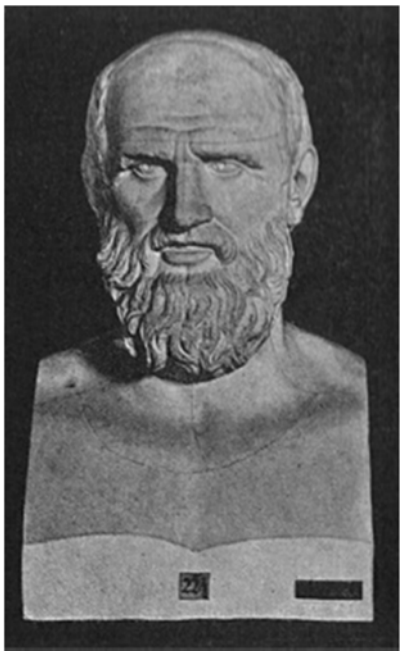
# Datenschutz: nicht nur Sicherheit!

Bild: Das Wortgewand via Pixabay





# Vertraulichkeit bei medizinischer Behandlung



„Was ich bei der Behandlung
sehe oder höre oder auch
außerhalb der Behandlung
im Leben der Menschen,
werde ich, soweit man es nicht
ausplaudern darf, verschweigen
und solches als ein Geheimnis betrachten.“

- Aus dem Hippokratischen Eid

# Vertraulichkeit bei medizinischer Behandlung

Heilberufler-Patienten-Geheimnis:

**§ 203 StGB – Verletzung von Privatgeheimnissen**

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs [...]

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

[...]





# Generell: Gesundheitsdaten sensibel

Art. 9 Datenschutz-Grundverordnung:

- Alle Gesundheitsdaten sind sensibel
- Datenschutzrisiko berücksichtigen


Bild: vjohns1580 via Pixabay

*Artikel 9*

**Verarbeitung besonderer Kategorien personenbezogener Daten**

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

# Überblick

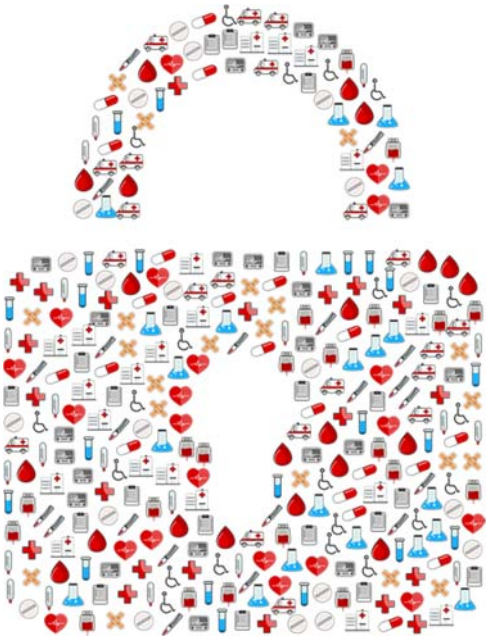


Bild: Gordon Johnson via Pixabay

1. **Datenschutz**
2. **Die Datenschutz-Grundverordnung**
3. **Hilfestellung zur Umsetzung in der Pflege**
4. **Fazit**





# Vereinheitlichung und Modernisierung

- Idee: Eine für alle
  und
  alle für eine
- Ziel:
  echte Harmonisierung
- Rechtssicherung durch Gleichklang der Aufsicht
- Dabei aber 70 Öffnungsklauseln für die Mitgliedstaaten

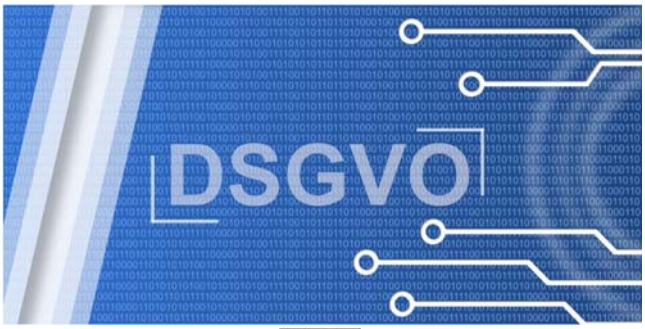



Bild: skylarvision via Pixabay

# Datenschutz-Grundsätze

Art. 5 DSGVO
– immer zu erfüllen bei personenbezogenen Daten

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
b) Zweckbindung
c) Datenminimierung
d) Richtigkeit
e) Speicherbegrenzung
f) Integrität und Vertraulichkeit (Datensicherheit)





# Nachweis- und Meldepflichten


Bild: Gerd Altmann via Pixabay

- Der Verantwortliche ist verantwortlich
- Der Auftragsverarbeiter in seinem Bereich
- Ziel: Risikobeherrschung
- Nachweis der Datenschutzkonformität

Bild: Antranias via Pixabay

- „Datenpanne“: z.B. Daten gestohlen oder verloren
- Meldung an Aufsichtsbehörde (innerhalb von 72 Stunden)
- Wenn Risiko für Betroffenen: Benachrichtigung

# Korrekte Datenverarbeitung nötig

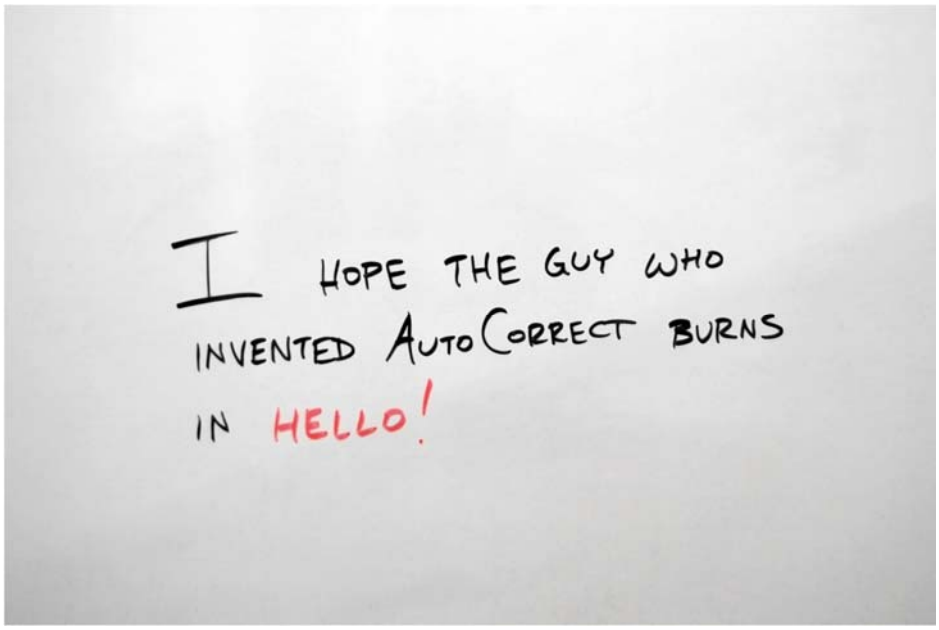



Bild: quinntheislander via Pixabay





# Einwilligung

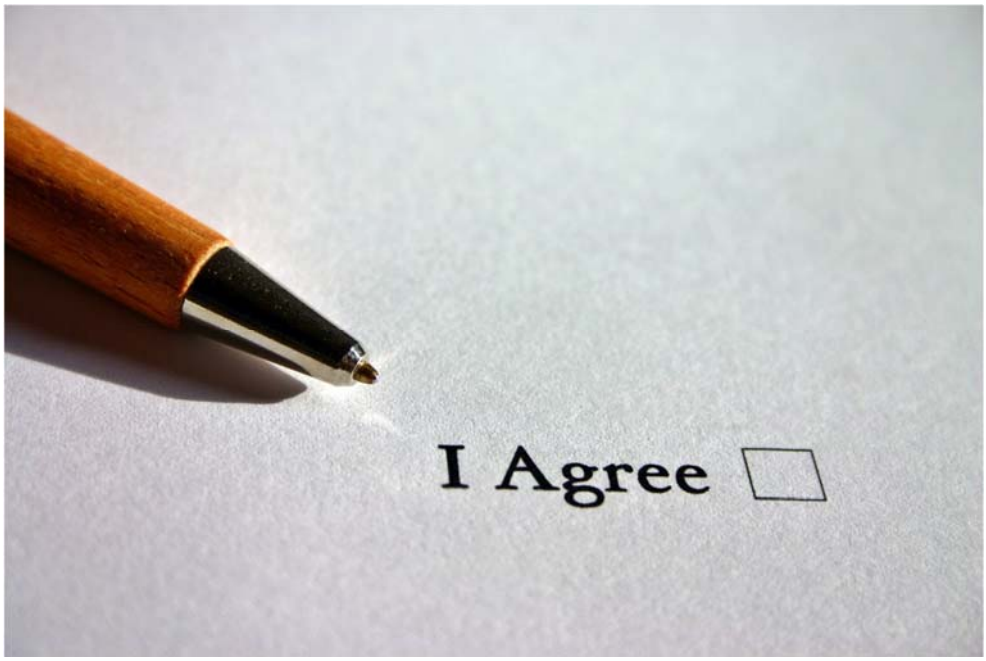



Bild: Catkin via Pixabay

# Widerruf der Einwilligung

Bild: ivanacoi via Pixabay





# Vertrag


Bild: Gerd Altmann via Pixabay

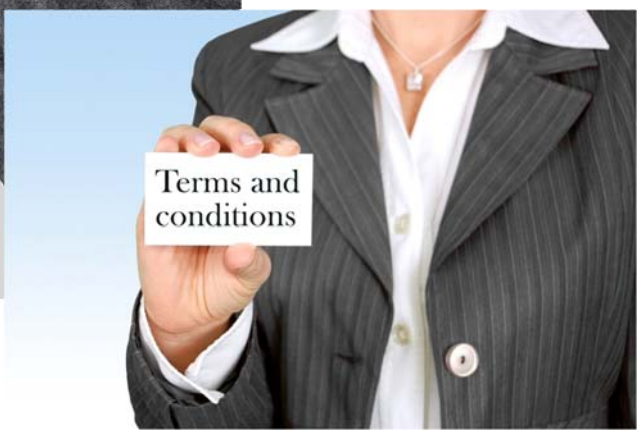



Bild: stux via Pixabay

# Rechte der Betroffenen

**Stärkung der Rechte der betroffenen Personen:**

- Artikel 7: Einwilligung: freiwillig, informiert, widerrufbar
- Artikel 12: Transparente Information [...]
- Artikel 13+14: Informationspflichten
- Artikel 15: Auskunftsrecht der betroffenen Person
- Artikel 16: Recht auf Berichtigung
- Artikel 17: Recht auf Löschung („Recht auf Vergessenwerden“)
- Artikel 18: Recht auf Einschränkung der Verarbeitung
- Artikel 19: Mitteilungspflicht im Zusammenhang mit Art. 17/18
- Artikel 20: Recht auf Datenübertragbarkeit
- Artikel 21: Widerspruchsrecht
- Artikel 22: Automatisierte Entscheidungen im Einzelfall / Profiling





# Betroffenenrechte Artt. 12 bis 22

Artt. 13+14 Information[1]


Art. 15 Auskunft[1]

Art. 16 Berichtigung[2]

Art. 17 Löschung[3]


Art. 20 Datenüber-tragbarkeit[4]

Artt. 21/22 Wider-spruch/Profiling[1]

# Betroffenenrecht Beschwerde bei den Datenschutz-Aufsichtsbehörden


Bild: Gerd Altmann via Pixabay

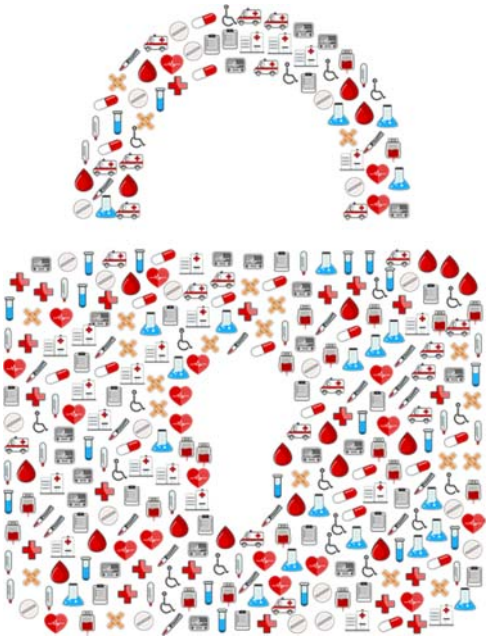




# Neu: Datenschutz „by Design“ & „by Default“

- Anforderung nach Art. 25 DSGVO
- Pflicht für:
  - Datenverarbeiter (primär: Verantwortlicher)
  - Indirekt: Dienstleister und Hersteller von IT-Systemen
    - Aber: oft noch nicht die Regel
    - Nachfragen & einfordern
- Ziel: eingebauter Datenschutz von Anfang an
  a) datenminimierend
  b) mit möglichst datenschutzfreundlichen Voreinstellungen

# Überblick





1. Datenschutz
2. Die Datenschutz-Grundverordnung
3. Hilfestellung zur Umsetzung in der Pflege
4. Fazit





# Hilfe: https://uldsh.de/dsgvo-aerzte

**Die Datenschutz-Grundverordnung tritt in Kraft – das müssen selbstständige Heilberufler beachten**

https://uldsh.de/dsgvo-aerzte, Stand: 25. Mai 2018

Am 25. Mai 2018 tritt die im Jahr 2016 verabschiedete EU-Datenschutz-Grundverordnung (DSGVO) vollständig in Kraft. Sie wird dann die wesentlichen in Deutschland und den anderen EU-Mitgliedstaaten anzuwendenden Vorschriften über den Datenschutz enthalten. Ergänzend finden sich für Heilberufler einzelne Konkretisierungen im neuen Teil 2 des Bundesdatenschutzgesetzes (BDSG), das am gleichen Tag in Kraft tritt.

**Wer ist Verantwortlicher?**

Der Betreiber oder die Betreiberin der Praxis, Apotheke etc. ist die oder der **Verantwortliche** im Sinne des Gesetzes. Sie oder er hat sicherzustellen, dass die Vorschriften über den Datenschutz eingehalten werden. Dazu gehört die Pflicht, bestimmte Dokumentationen zu führen, mit denen die Einhaltung der Vorgaben nachgewiesen werden kann.

In diesem Text sollen die wichtigsten Anforderungen der DSGVO und des BDSG für selbstständige Heilberufler kurz vorgestellt werden. Dabei wird auch auf bereits vorhandene Informationsquellen verwiesen, insbesondere auf die „Kurzpapiere" die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu einer Reihe von wichtigen Themen und Begriffen des neuen Rechts gemeinsam entwickelt und veröffentlicht hat.

**Rechtsgrundlagen für die Verarbeitung personenbezogener Daten der Patienten: Vertrag oder Einwilligung**

Die DSGVO erlaubt die Verarbeitung von personenbezogenen Daten nur, wenn dafür eine **Rechtsgrundlage** zur Verfügung steht.

Im Fall einer Arztpraxis, Apotheke etc. ist die Rechtsgrundlage **in der Regel der Vertrag**, der mit dem Patienten geschlossen wird. Die zur Begründung, Durchführung und Beendigung des Vertrags notwendigen Daten dürfen verarbeitet werden.

- 1 -

# Grundlegendes

- Verantwortlicher: Betreiber der Einrichtung

- Rechtsgrundlagen:
  - Privat-rechtliche Trägerschaft: DSGVO + BDSG
    (etwas anders: öffentlich-rechtlich/kirchlich)
    - Vertrag mit Kunden über die Pflege mit den erforderlichen Daten [Art. 6 (1) b DSGVO]
    - Für Zusatz-Dienste: Einwilligung (nachweisen!) [Art. 6 (1) a DSGVO]
  - In der Rolle „Leistungserbringer für Pflege-/Krankenkassen“: besondere Vorschriften im Sozialgesetzbuch [Art. 6 (1) c DSGVO]
  - Notfallsituationen: Art. 6 (1) d DSGVO [i.V.m. Art. 9 (2) c DSGVO]





# Einwilligung

- Freiwillig, informiert, widerrufbar
- Nachweisbar

- Ausreichende Informationen geben,
  z.B. bei Weitergabe der Kundendaten an Dritte (Schweigepflichtentbindungserklärung) Angaben über Identität und Kontaktdaten der Empfänger sowie Zweck + Umfang der Datenweitergabe

- Auch: Folgen der Verweigerung oder des Widerrufs der Einwilligung

# Informationspflichten I

Insbesondere:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (sofern benannt)
- Zwecke und Rechtsgrundlage der Verarbeitung
- Ggf. Empfänger(kategorien) der personenbezogenen Daten
- Informationen über die Betroffenenrechte
- Information über Beschwerderecht bei einer Datenschutzaufsichtsbehörde

- In verständlicher Sprache – Ziel: Transparenz


https://uldsh.de/tb37, Tz. 6.1.4





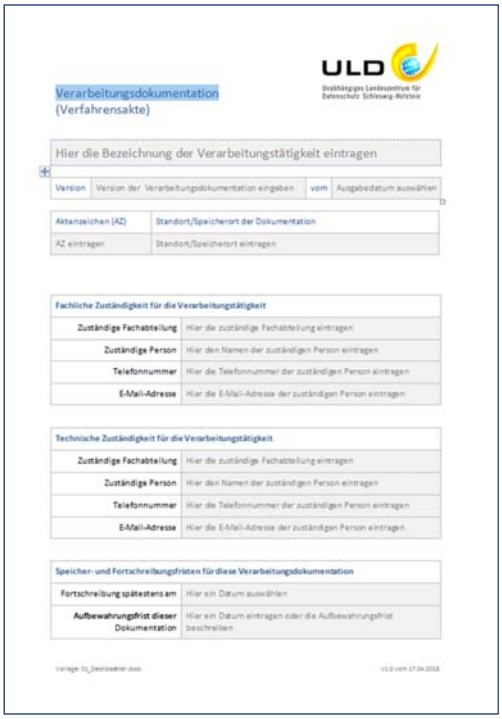
# Informationspflichten II

- Im zeitlichen Zusammenhang mit der Erhebung
- Per Flyer oder Handzettel zu Beginn (bei der Aufnahme)
- Detaillierte Informationen z.B. auf Webseite
- Nachweis der Erfüllung der Informationspflicht:
  Vermerk in der Dokumentation zur Übergabe des Handzettels würde reichen

- Nicht ausreichend: nur als Aushang in der Einrichtung

# Verzeichnis von Verarbeitungstätigkeiten

Muster unter
https://uldsh.de/doku



Verarbeitungsdokumentation
(Verfahrensakte)

Hier die Bezeichnung der Verarbeitungstätigkeit eintragen

| Version | Version der Verarbeitungsdokumentation eingeben | vom | Ausgabedatum auswählen |
|---|---|---|---|

| Aktenzeichen (AZ) | Standort/Speicherort der Dokumentation |
|---|---|
| AZ eintragen | Standort/Speicherort eintragen |

| Fachliche Zuständigkeit für die Verarbeitungstätigkeit | |
|---|---|
| Zuständige Fachabteilung | Hier die zuständige Fachabteilung eintragen |
| Zuständige Person | Hier den Namen der zuständigen Person eintragen |
| Telefonnummer | Hier die Telefonnummer der zuständigen Person eintragen |
| E-Mail-Adresse | Hier die E-Mail-Adresse der zuständigen Person eintragen |

| Technische Zuständigkeit für die Verarbeitungstätigkeit | |
|---|---|
| Zuständige Fachabteilung | Hier die zuständige Fachabteilung eintragen |
| Zuständige Person | Hier den Namen der zuständigen Person eintragen |
| Telefonnummer | Hier die Telefonnummer der zuständigen Person eintragen |
| E-Mail-Adresse | Hier die E-Mail-Adresse der zuständigen Person eintragen |

| Speicher- und Fortschreibungsfristen für diese Verarbeitungsdokumentation | |
|---|---|
| Fortschreibung spätestens am | Hier ein Datum auswählen |
| Aufbewahrungsfrist dieser Dokumentation | Hier ein Datum eintragen oder die Aufbewahrungsfrist beschreiben |

S[CH]ER Aktion Datenschutz in meiner Arztpraxis
www.datenschutzzentrum.de/medizin/





# Betrieblicher Datenschutzbeauftragter

- Nach § 38 BDSG zu benennen, wenn
  - in der Regel mind. 10*) Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind
  - eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) durchzuführen ist
    (z.B. bei Gesundheitsdaten in großem Umfang oder bei besonderen Risiken, bspw. bei Gendaten)
- Intern oder extern, keine Interessenkollisionen
- Kontaktdaten an zuständige Aufsichtsbehörde melden

*) künftig in BDSG: Änderung auf 20 Personen

S[CH]ER Aktion Datenschutz in meiner Arztpraxis
www.datenschutzzentrum.de/medizin/

# Weitere Pflichten

- Beschränkung der DV auf das erforderliche Maß
- Fristgerechte Löschung (übliche Mindestfrist 10-jährige Aufbewahrung; teilweise längere Aufbewahrung gesetzlich vorgesehen oder aus medizinisch-fachlicher Sicht erforderlich – für die eigene Verarbeitung prüfen und umsetzen)
- Technisch-organisatorische Maßnahmen, z.B. gegen unberechtigten Zugriff
- Prozesse für Betroffenenrechte, z.B. Auskunft
- Abschluss von Verträgen mit Dienstleistern (Auftragsverarbeitung)
- Meldung von Datenschutzvorfällen an die Aufsichtsbehörde und ggf. Benachrichtigung der betroffenen Personen

S[CH]ER Aktion Datenschutz in meiner Arztpraxis
www.datenschutzzentrum.de/medizin/





Selbst-Check
für Arzt-/Zahnarztpraxen

Unbefugte
(Augen, Ohren und Hände)
dürfen keinen Zugang zu Patientendaten haben!

Dieser Selbst-Check für Arzt-/Zahnarztpraxen berücksichtigt die ab dem 25. Mai 2018 zu beachtende Europäische Datenschutz-Grundverordnung (DSGVO)!

➡ Wird eine Frage mit NEIN beantwortet, besteht u. U. Handlungsbedarf!

# Hilfreich: Selbst-Check

| Praxisverwaltung | | |
|---|---|---|
| Fehlendes Wissen, fehlende technische und organisatorische Maßnahmen, aber auch mangelnde Sensibilität im Umgang mit Patientendaten und der tägliche Arbeitsstress können das Patientengeheimnis gefährden. | *ja* | *nein* |
| Sind Mitarbeiterinnen und Mitarbeiter über ihre Befugnisse und gesetzlichen Pflichten bei der Wahrung der Schweigepflicht ausreichend informiert? | ☐ | ☐ |
| Sind schriftliche Patientenunterlagen, wie z. B. Karteikarten und Patientenakten, vor dem Zugriff und der Einsicht durch Unbefugte geschützt? | ☐ | ☐ |
| Sind abschließbare Aktenschränke vorhanden? Werden diese bei Dienstschluss verschlossen? | ☐ | ☐ |
| Ist die Aufbewahrung von „alten Akten“ sicher organisiert (kein „offener Keller“)? | ☐ | ☐ |
| Sind die Praxisräume, in denen sich Patientendaten/Abrechnungsdaten befinden, ausreichend gegen Einbruch geschützt? | ☐ | ☐ |
| Ist sichergestellt, dass das Reinigungspersonal keinen Zugang zu Patientendaten hat? | ☐ | ☐ |
| Werden in der Praxis ausschließlich Shredder für die Aktenvernichtung entsprechend der DIN 66399-1/2 der Partikelgröße P-5 (vormals Sicherheitsstufe 4) verwendet? Weitergehende Informationen erhalten Sie beim ULD. | ☐ | ☐ |

# Privatgeräte im Einsatz? – Problem!

Bild: Clker-Free-Vector-Images via Pixabay

- BYOD – „Bring your own device“: problematisch
  - Verantwortung mit Rechenschaftspflicht
  - Mischung privat/dienstlich
  - Sicherheit? Datenpannen?
  - Kontrollmöglichkeiten?

Bild: Gerd Altmann via Pixabay

- Lösung:
  - Dienstgeräte mit nötiger Funktionalität
  - Weitergehende Digitalisierung mit Sicherheitsgarantien





# Digitalisierung in der Pflege: Dokumentation

Bild: rawpixel via Pixabay

Bild: Mohamed Hassan via Pixabay

- Behandlungsdokumentation per Tablet
- Dienstliche Hard- und Software
- Geschützte Speicherung (z.B. eigene Cloud, verschlüsselt)
- Verschlüsselter Datentransfer
- Passende Zugriffsberechtigungen
- Konfiguration ohne Datenabfluss an Unberechtigte
- Abgesicherte Kopplung mit Sensorikfunktionalität möglich

# Technikeinsatz auch während der Behandlung

- Zur Unterstützung der Behandlung
- Zur Kontrolle?

*Behandelnder* ← *Arbeitgeber*

↕ ↖

*Behandelter* ← *Familie*

- Im Hintergrund, weil „Smart Home“?
- Protokollierung, Audio, Video ...

Bild: WikiImages via Pixabay

Bild: Gerd Altmann via Pixabay





# Überblick

Bild: Gordon Johnson via Pixabay

1. **Datenschutz**
2. **Die Datenschutz-Grundverordnung**
3. **Hilfestellung zur Umsetzung in der Pflege**
4. **Fazit**

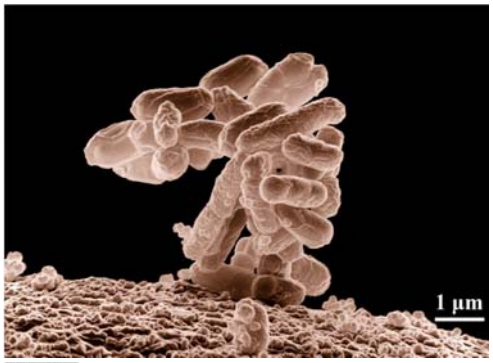



Bild: WikiImages via Pixabay

# Datenschutz ist wie Hygiene

- Man kann die Bedrohungen oft nicht sehen. Oder zu spät.
- Späte Effekte möglich.
- Es betrifft einen selbst und andere. Jeder ist mitverantwortlich.

⇨ Das richtige Verhalten sollte eingeübt und selbstverständlich sein.

Bild: Jacqueline Macou via Pixabay





# Fazit

Bild: kalhh via Pixabay

- Datenschutzrisiken in den Griff bekommen
  - Technisch-organisatorisch
  - Sensibilisierung der Beschäftigten
  - Prozesse definieren und einüben
- Auch bei Dienstleistern / Herstellern einfordern
- Hilfen nutzen


# Ihre Fragen?

Marit Hansen
https://www.datenschutzzentrum.de/

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



# Weitere Informationen

www.datenschutzzentrum.de/meldungen/

Meldungen an das ULD

» Meldungen an das ULD

Sie können auf verschiedenen Wegen mit uns in Kontakt treten:

**Für spezielle Meldungen bieten wir Ihnen gesonderte Kontaktformulare an:**

- Meldung von **Kontaktdaten der Datenschutzbeauftragten** (gemäß Artikel 37 Absatz 7 DSGVO, §58 Absatz 5 LDSG 2018)
- **Beschwerde von betroffenen Personen** (gemäß. Artikel 77 DSGVO sowie § 36 LDSG 2018)
- **Datenpannen** (Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO oder § 41 LDSG)
  - Formular als ODT-Datei
  - Formular als RTF-Datei

**Allgemeine Anfragen:**

**E-Mail:**
mail@datenschutzzentrum.de
Hinweise zur verschlüsselten Kommunikation mittels PGP/GnuPG


www.datenschutzzentrum.de/dsgvo/

# Weitere Informationen

- https://www.datenschutzzentrum.de/dsgvo/
- Kurzpapiere zu vielen Themen der DSGVO
  - Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO
  - Aufsichtsbefugnisse/Sanktionen
  - Verarbeitung personenbezogener Daten für Werbung
  - Datenübermittlung in Drittländer
  - Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
  - Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
  - Marktortprinzip – Regelungen für außereuropäische Unternehmen
  - Maßnahmenplan „DS-GVO“ für Unternehmen
  - Zertifizierung nach Art. 42 DS-GVO
  - Informationspflichten bei Dritt- und Direkterhebung
  - Recht auf Löschung / „Recht auf Vergessenwerden“
  - Datenschutzbeauftragter
  - Auftragsverarbeitung nach Art. 28 DS-GVO
  - Beschäftigtendatenschutz
  - Videoüberwachung
  - Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO
  - Besondere Kategorien personenbezogener Daten
  - Risiko für die Rechte und Freiheiten natürlicher Personen
  - Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO
- DSGVO + BDSG: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf

DSK DATENSCHUTZKONFERENZ





# Startpunkt: Wissen über die eigene Datenverarbeitung

1. Ab 25.05.2018 gelten die DSGVO und das BDSG-neu sowie LDSG-neu.
2. Beachten Sie insbesondere folgende Fragestellungen:

a) Werden die Grundsätze der Datenverarbeitung eingehalten und wird die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) erfüllt?

b) Können die Rechte betroffener Personen nach internen Mechanismen fristgemäß (Art. 12 Abs. 3 DSGVO) erfüllt werden?

c) Wurden Verträge zur Auftragsverarbeitung, Betriebsvereinbarungen sowie Einwilligungserklärungen auf ihre Konformität mit den Anforderungen der DSGVO geprüft und ggf. angepasst?

d) Werden die Anforderungen von Sicherheit und Datenschutz technisch und organisatorisch umgesetzt (Art. 32 und Art. 25 DSGVO)?

e) Gibt es interne Prozesse zur fristgemäßen Erfüllung der Meldepflichten bei Datenschutzverstößen (Art. 33 und Art. 34 DSGVO)?