Die Datenschutz-Grundverordnung und ihre Umsetzung im Praxisalltag

Marit Hansen

Landesbeauftragte für Datenschutz
Schleswig-Holstein

Kiel, 15.09.2018

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

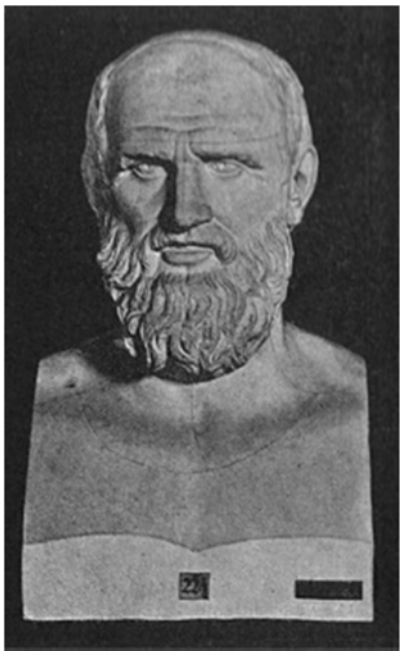
Überblick

1. **Datenschutz: bekannt**
2. **Die Datenschutz-Grundverordnung**
3. **Hilfestellung zur Umsetzung in Ihrer Praxis**
4. **Zusammenfassung**

Nicht nur Sicherheit!

Bild: Das Wortgewand via Pixabay

Vertraulichkeit zwischen Arzt und Patient



„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 zwischen Arzt und Patient

Arzt-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

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.

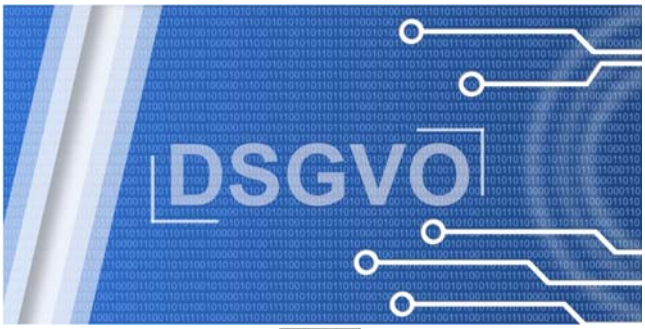
(2) Absatz 1 gilt nicht in folgenden Fällen:

Überblick

1. Datenschutz: bekannt
2. Die Datenschutz-Grundverordnung
3. Hilfestellung zur Umsetzung in Ihrer Praxis
4. Zusammenfassung

Vereinheitlichung und Modernisierung

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



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: geralt 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

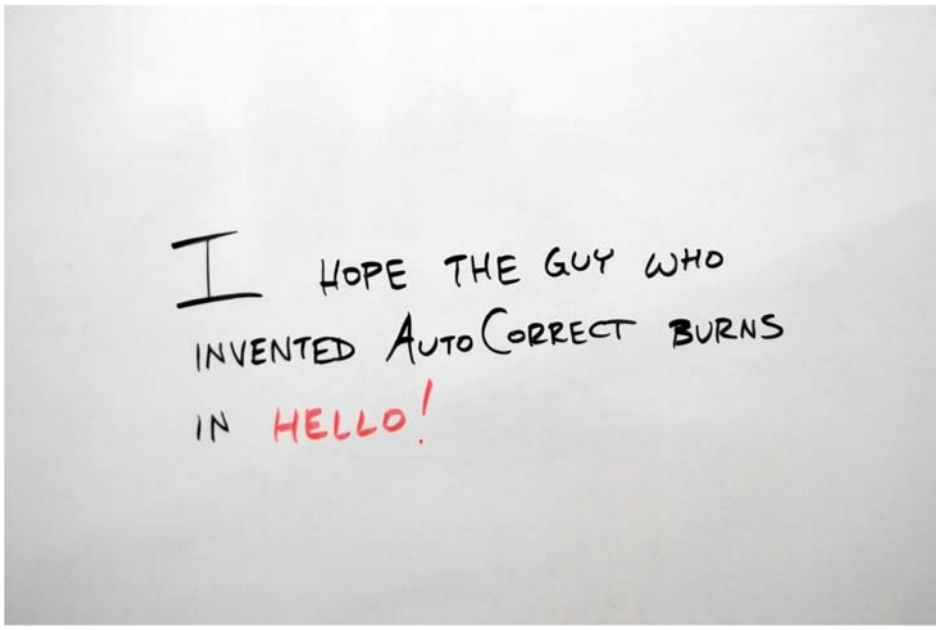


Bild: quinntheislander via Pixabay

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

Einwilligung

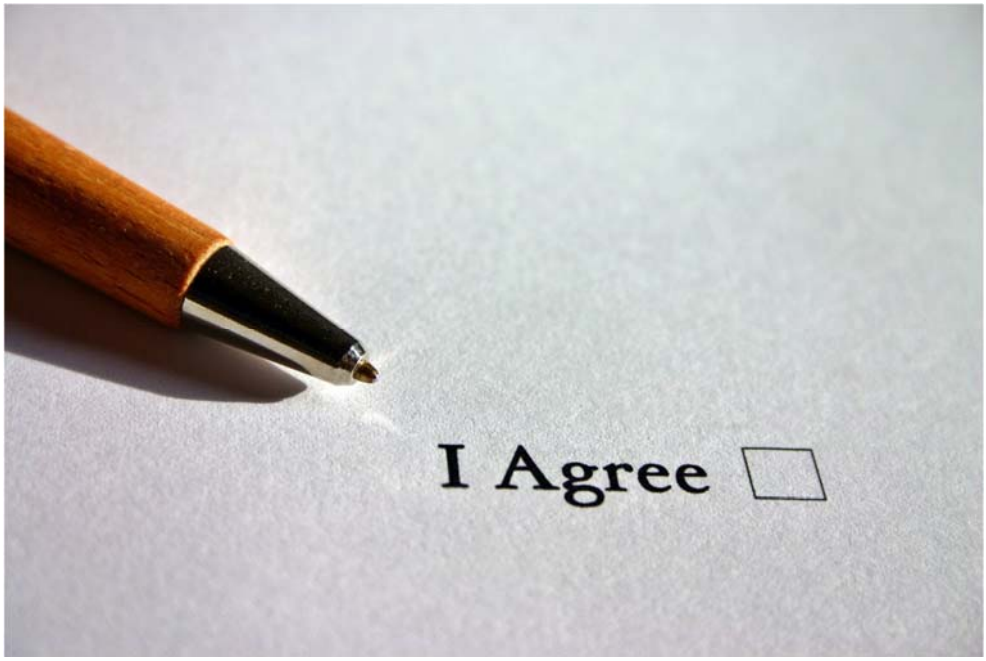


Bild: Catkin via Pixabay

Widerruf der Einwilligung

Bild: ivanacoi via Pixabay

Vertrag

Bild: geralt via Pixabay

Bild: stux via Pixabay

Bild: rawpixel via Pixabay

Betroffenenrecht Information

Bild: geralt via Pixabay

Bild: rawpixel via Pixabay

Betroffenenrecht Auskunft

Bild: geralt via Pixabay

Bild: rawpixel via Pixabay

Betroffenenrecht Berichtigung

Bild: stevepb via Pixabay


Bild: rawpixel via Pixabay

Betroffenenrecht Löschen

Bild: Hans via Pixabay


Bild: rawpixel via Pixabay

Betroffenenrecht Übertragbarkeit

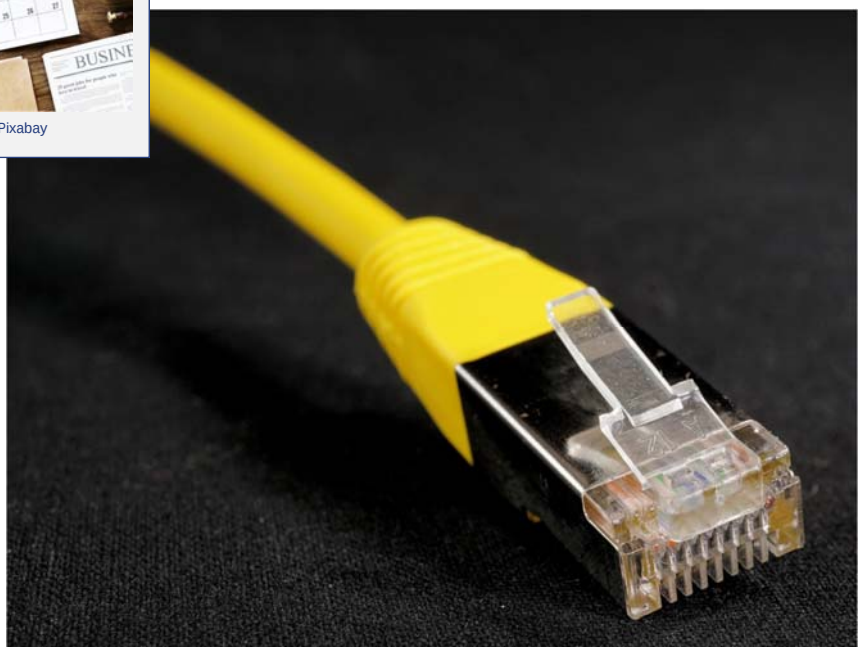


Bild: webandi via Pixabay

Profiling/Einzelentscheidung: Information über Logik, Eingreifmöglichkeit

Bild: rawpixel via Pixabay

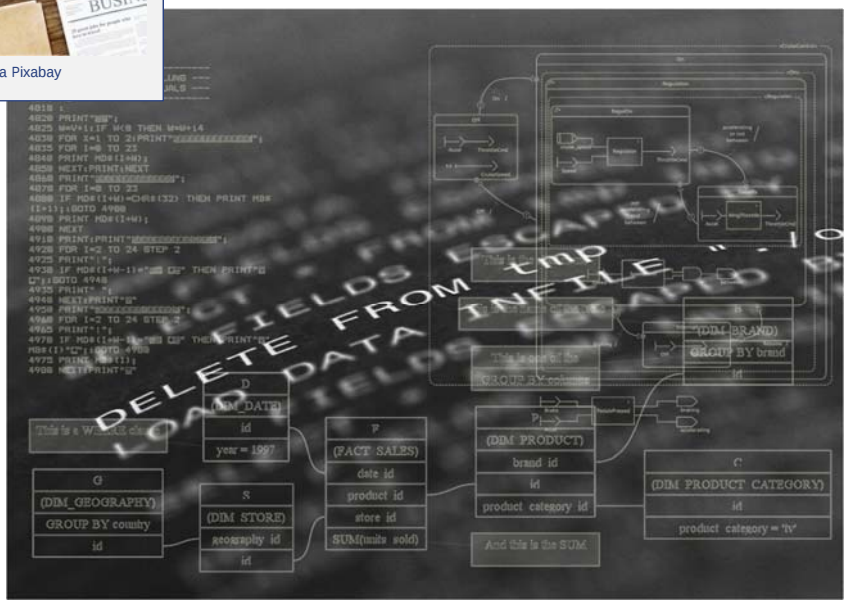


Bild: geralt via Pixabay

Betroffenenrecht Beschwerde bei den Datenschutz-Aufsichtsbehörden

Bild: geralt via Pixabay

Datenschutz „by Design“ & „by Default“

- Art. 25 DSGVO – mehr als „eingebaute Sicherheit“ (Art. 32 DSGVO)
- Richtet sich an:
  - Datenverarbeiter (primär: Verantwortlicher)
  - Indirekt: Dienstleister und Hersteller von IT-Systemen
- Ziel: Gestaltung von Systemen + Diensten
  von Anfang an über den gesamten Lebenszyklus
  a) datenminimierend
  b) mit möglichst datenschutzfreundlichen Voreinstellungen
- Wichtig für jede Beschaffung + Nachweispflicht

Chancen

Bild: congerdesign via Pixabay

- Selbstüberprüfung der eigenen Prozesse
  - Beurteilung des Risikos
  - Sortieren + aufräumen
  - Verbesserungspotenziale
- Eingebauter Datenschutz
  - Anbieten und nachfragen
  - Marktbewegung
  - Zertifizierung möglich
- Vertrauenswürdigkeit:
  Kundschaft kann Spreu vom Weizen trennen

Überblick

1. Datenschutz: bekannt
2. Die Datenschutz-Grundverordnung
3. Hilfestellung zur Umsetzung in Ihrer Praxis
4. Zusammenfassung

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 Praxis

- Rechtsgrundlagen:
  - Vertrag mit Patienten zur Durchführung der Behandlung; erforderlich: Name, Anschrift, Versicherungsnummer, ärztliche Dokumentation
  - Für zusätzliche Dienste (z.B. Recall-Service): Einwilligung (nachweisen!)
  - Einbindung privater Verrechnungsstellen: Einwilligung jedenfalls dann nötig, wenn die Honorarforderungen abgetreten werden könnten

Einwilligung

- Freiwillig, informiert, widerrufbar
- Nicht notwendigerweise schriftlich, aber nachweisbar

- Ausreichende Informationen geben,
  z.B. bei Weitergabe der Patientendaten 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

- Im zeitlichen Zusammenhang mit der Erhebung

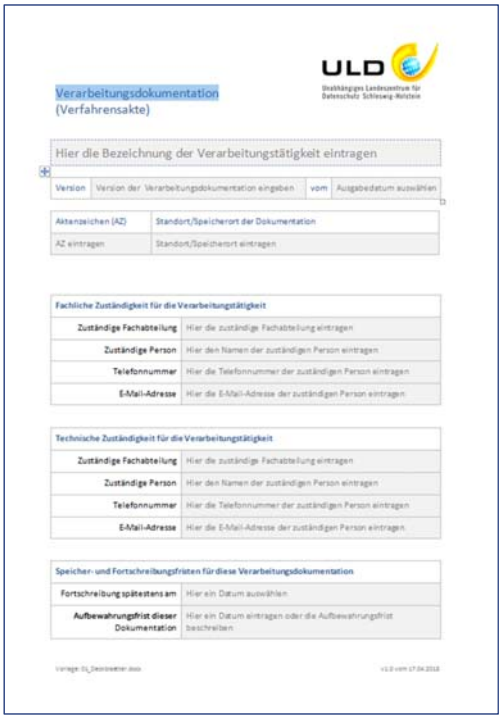
Informationspflichten II

- Per Flyer oder Handzettel bei der Aufnahme
- Detaillierte Informationen z.B. auf Webseite
- Nachweis der Erfüllung der Informationspflicht:
  Vermerk im Praxissystem der Übergabe des Handzettels würde reichen

- Nicht ausreichend: nur als Aushang in der Praxis

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 Maßstab oder bei besonderen Risiken, bspw. bei Gendaten)
- Intern oder extern
- Kontaktdaten dem ULD melden

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

Weitere Pflichten

- Beschränkung der DV auf das erforderliche Maß
- Fristgerechte Löschung (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 das ULD 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.	☐	☐

Schon in der Vor-DSGVO-Zeit veröffentlicht, nun angepasst

Zahnärzteblatt 11/2016 bis 06/2017:

ZAHNÄRZTEKAMMER

Datenschutz-Selbstcheck – Teil I

„Empfang und Wartebereich"

Patientendaten sind im Empfangs- und Wartebereich einer Arzt- bzw. Zahnarztpraxis vor neugierigen Ohren, Augen und Händen zu schützen. Der Gesetzgeber schützt das Patientengeheimnis: Eine unbefugte Offenbarung von Patientendaten steht unter Strafe. Werden Arzt- bzw. Zahnarztpraxen dieser Verantwortung gerecht? Was ist zu beachten? Der neue „Selbst-Check für Arztpraxen" stellt Fragen und gibt Antworten.

ZAHNÄRZTEKAMMER

Datenschutz-Selbstcheck – Teil VIII

Outsourcing und Videoüberwachung in der Praxis

Bei der Beauftragung eines externen Dienstleisters (Auftragnehmer) zum Beispiel mit der Administration der IT oder der Aktenvernichtung kann oftmals ein Zugriff auf Patientendaten durch den Auftragnehmer nicht vollständig ausgeschlossen werden. Wenn aber ein Zugriff auf Patientendaten nicht ausgeschlossen werden kann, benötigt der Arzt bzw. Zahnarzt eine ausreichende Befugnis, um sich nicht strafbar zu machen.

Noch mehr Hilfen

ZAHNÄRZTEKAMMER

Das müssen selbstständige Zahnärzte beachten:

Die Datenschutz-Grundverordnung tritt in Kraft

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 die Heilberufe einzelne Konkretisierungen im neuen Teil des Bundesdatenschutzgesetzes (BDSG), das am gleichen Tag in Kraft tritt.

Zahnärzteblatt
05/2018

Überblick

1. **Datenschutz: bekannt**
2. **Die Datenschutz-Grundverordnung**
3. **Hilfestellung zur Umsetzung in Ihrer Praxis**
4. **Zusammenfassung**

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)?

Fazit

Bild: karosieben via Pixabay

- Datenschutzrisiken in den Griff bekommen
- Auch bei Dienstleistern/Herstellern einfordern
- Hilfen nutzen
  - ULD: Herr Koop steht für Ihre Fragen zur Verfügung
  - (Zahn-)Ärztekammern

Machen!

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