Maßnahmenplan für Praxen zur Umsetzung der EU DS-GVO

Informationsveranstaltung für niedergelassene Ärzte und Psychotherapeuten am 24.10.2018 in Mainz

Michael Heusel-Weiss,

Mitarbeiter des Landesbeauftragten für Datenschutz und Informationsfreiheit Rheinland-Pfalz

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

1. Devise: „Bange machen gilt nicht!“

Viele Anforderungen aus der EU Datenschutz-Grundverordnung sollten Inhabern und Mitarbeitern niedergelassener Heilberufspraxen bereits seit langem bekannt sein:

→ aus dem bislang geltenden Datenschutzrecht (BDSG)
→ aus dem Standesrecht (Berufsordnungen)

Einige Beispiele:

1. Devise: „Bange machen gilt nicht!“

- hoher Schutzbedarf patientenbezogener Behandlungsdaten (ärztliche Schweigepflicht)
- Weitergabe von Patientendaten an Dritte nur bei Vorliegen einer Befugnis (entweder durch Gesetz oder Einwilligung)
- Pflicht der Praxisinhaber zur Vornahme angemessener technischer und organisatorischer Vorkehrungen
- Patienten und Mitarbeiter haben Rechte

1. Devise: „Bange machen gilt nicht!“

Aber die DS-GVO bringt auch Neuerungen im Praxisbetrieb. Zum Beispiel:

- Rechenschaftspflicht der Praxisinhaber nach Art. 5 Abs. 2 (Nachweis der Einhaltung der dsr Vorgaben z.B. ggü. der Aufsichtsbehörde)
- aktive Informationspflichten gegenüber den Patienten und Mitarbeitern nach Art. 12 ff.
- Ausweitung der Befugnisse der Datenschutzaufsicht

2. Devise: „Am Anfang war das Wort…“

Der Text der EU Datenschutz-Grundverordnung einschließlich der Erwägungsgründe ist im Internet auf zahlreichen Websites veröffentlicht. Z.B. auf:

www.datenschutz.rlp.de
www.mit-sicherheit-gut-behandelt.de

Es ist für das Erfüllen der Anforderungen aus der DS-GVO unerlässlich, dass den Praxisinhabern der Verordnungstext bekannt ist und sie jederzeit auf ihn zugreifen können.

2. Devise: „Am Anfang war das Wort…“

Dies gilt auch für alle sonstigen Vorgaben zum Datenschutz und zur Einhaltung der berufsrechtlichen Schweigepflicht, die die Tätigkeit der eigenen Praxis betreffen.

Die seitens der zuständigen Datenschutzaufsicht (LfDI Rheinland-Pfalz) und der Heilberufskammern/KV bereit gestellten Informationen, Empfehlungen und Materialien können in diesem Zusammenhang helfen.

Maßnahmenplan für niedergelassene Heilberufspraxen

1. Datenschutz ist Chefsache!

- sinnvoll: personelle Zuordnung von Verantwortlichkeiten
- Pflicht zur Benennung eines DSB regelmäßig nur bei einer Mitarbeiterzahl über 9 (§ 38 Abs. 1 Satz 1 BDSG-neu)
- bei einer Mitarbeiterzahl unter 10:
  idR keine Pflicht zur Benennung eines DSB, aber Empfehlung, einen Ansprechpartner zum DS in der Praxis zu installieren

Maßnahmenplan für niedergelassene Heilberufspraxen

2. Durchführung einer Bestandsaufnahme (IST-Analyse)

Haben Sie sich in der Vergangenheit bereits Gedanken gemacht…

- … welche Daten Sie in Ihrer Praxis bislang zu welchen Zwecken verarbeitet haben?
- … ob Sie hierzu befugt waren (gesetzliche RGL/Einwilligung)?
- … wie lange und sicher die Daten aufbewahrt werden ?
- … welche Dienstleister Zugang zu den Patientendaten haben?

Maßnahmenplan für niedergelassene Heilberufspraxen

2. Durchführung einer Bestandsaufnahme (IST-Analyse)

Wenn 👍: Super, die restlichen Anforderungen aus der DS-GVO insbesondere die Dokumentation, sind dann leichter zu schaffen!

Wenn 👎: Dann wird es jetzt aber höchste Zeit! Leider wird für Sie der Aufwand anfangs etwas höher sein.

Für alle gilt: spätestens seit Mai 2018 muss sich jeder Praxisinhaber um den Datenschutz in der Praxis kümmern und dies dokumentieren!

Maßnahmenplan für niedergelassene Heilberufspraxen

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

Was ist auf jeden Fall zu tun?

- ✓ Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- ✓ Sicherstellung der Betroffenenrechte, insbesondere Erfüllung der Informationspflichten (Art. 13/14 DS-GVO)
- ✓ datenschutzkonforme Einbindung der externen Dienstleister (Art. 28 DS-GVO)
- ✓ Sicherheit der Verarbeitung (Art. 32 DS-GVO)

Maßnahmenplan für niedergelassene Heilberufspraxen

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO)**
  - ✓ Folge der Rechenschaftspflicht der Praxisinhaber, Art. 5 Abs. 2 DS-GVO
  - ✓ dient sowohl der internen DS-Kontrolle durch Praxisinhaber als auch der Prüfung durch DS-Aufsicht
  - ✓ Mustervordrucke stehen im Internet zur Verfügung

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO)**
  - ✓ Verarbeitungstätigkeit: jeder abstrakte Geschäftsprozess in Praxis wie z.B. Diagnostik, Abrechnung, Dokumentation
  - ✓ weitere Angaben: Zweck der Verarbeitung, betroffene Personen und Datenkategorien, Empfänger, Speicher-dauer, t-o Maßnahmen, DÜ an Drittstaat

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **<u>Führen eines Verzeichnisses von Verarbeitungstätigkeiten</u> (Art. 30 DS-GVO)**

  ✓ sinnvoll:
  ergänzende Feststellung der einzelnen Rechtsgrundlagen (Gesetz oder Einwilligung) für die jeweilige Verarbeitungstätigkeit

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **<u>Bereitstellung einer allgemeinen Patienteninformation</u> (Art. 12 ff. DS-GVO)**
  - ✓ Folge des Grundsatzes der Transparenz, Art. 5 Abs. 1 lit. a DS-GVO
  - ✓ ggü. der bisherigen Rechtslage deutliche Ausweitung der Informationspflichten
  - ✓ Abgrenzung zu „Einwilligung“ u. „Datenschutzerklärung“

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **<u>Bereitstellung einer allgemeinen Patienteninformation</u> (Art. 12 ff. DS-GVO)**
  - ✓ Anforderungen an die Patienteninformation: präzise, transparente, verständliche und leicht zugängliche Form sowie klare und einfache Sprache (Art. 12 Abs. 1)
  - ✓ möglich: in Kombination mit Bildsymbolen, Art. 12 Abs. 7

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Bereitstellung einer allgemeinen Patienteninformation (Art. 12 ff. DS-GVO)**
  - ✓ **Inhalt**: Angaben zu Praxis, DSB, Zweck und RGL der Verarbeitung, Empfänger, ggf. DÜ in Drittland (Art. 13 Abs. 1 DS-GVO)
  - ✓ **zudem**: u.a. Speicherdauer, Auskunftsrecht, ggf. Widerrufsmöglichkeit einer Einwilligung, Recht auf Beschwerde bei LfDI (Art. 13 Abs. 2 DS-GVO)

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Bereitstellung einer allgemeinen Patienteninformation (Art. 12 ff. DS-GVO)**

  - ✓ Umsetzung in der Praxis: Beschreibung eines **regelmäßig vorhersehbaren Behandlungsverlaufs** durch Infoblatt
  - ✓ weitere individuelle Informationen je nach Behandlung
  - ✓ **bei Dritterhebung** richten sich Informationspflichten nach Art. 14 DS-GVO

Maßnahmenplan für niedergelassene Heilberufspraxen

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Gewährleistung des Auskunftsanspruchs (Art. 15 DS-GVO)**

  - ✓ praxisinterne Festlegung, in welcher Weise einem Auskunftsbegehren nachgekommen wird
  - ✓ denkbar: personelle Zuordnung der Verantwortlichkeit

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Datenschutzkonforme Einbindung externer Dienstleister (Art. 28 DS-GVO)**

  ✓ Bestehen Dienstleistungsbeziehungen mit Dritten, bei denen (Haupt-) Gegenstand der Leistung das Erheben, Speichern, Übermitteln v. Daten ist?

  ✓ Sind die Anforderungen des Art. 28 DS-GVO erfüllt? (ggf. Anpassung der Verträge)

Maßnahmenplan für niedergelassene Heilberufspraxen

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Sicherheit der Verarbeitung (Art. 32 DS-GVO)**

  - ✓ Praxisinhaber ist verpflichtet, geeignete t-o Maßnahmen zu treffen, um ein dem Risiko in der Praxis angemessenes Schutzniveau zu gewährleisten
  - ✓ **Voraussetzung**: Ermittlung der konkreten Risiken bei der Verarbeitung der Patientendaten, vgl. Art. 32 Abs. 2
  - ✓ **Folge**: geeignete t-o Vorkehrungen sind zu treffen

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Sicherheit der Verarbeitung (Art. 32 DS-GVO)**

  ✓ Katalog der Schutzmaßnahmen: Art. 32 Abs. 1 lit. a - d

  ✓ in den Heilberufspraxen:
  betroffen sind nicht nur der Einsatz v. IT/Telemedizin, sondern z.B. auch Fragen der Praxisgestaltung, der Einsatz von Vordrucken oder die Kommunikation mit Externen (Fax/E-Mail)

Maßnahmenplan für niedergelassene Heilberufspraxen

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **zusätzlich Datenschutz-Folgenabschätzung ? (Art. 35 DS-GVO)**
  - ✓ **strukturierte** umfassende Risikoeinschätzung der DV
  - ✓ **Inhalt**: Katalog des Art. 35 Abs. 7 DS-GVO, u.a. Beschreibung der geplanten Verarbeitungsvorgänge, Bewertung der Notwendigkeit der DV und Risikoeinschätzung, Auflistung der geplanten Abhilfemaßnahmen
  - ✓ Art. 36 Abs. 1 DS-GVO: ggf. Konsultation der DS-Aufsicht

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **zusätzlich Datenschutz-Folgenabschätzung ? (Art. 35 DS-GVO)**
  - ✓ obligatorisch, wenn **umfangreiche** Verarbeitung von Gesundheitsdaten(Art. 35 Abs. 3 lit. b DS-GVO)
    ➲ z.B. Krankenhäuser, Großpraxen
  - ✓ obligatorisch, wenn hohes Verarbeitungsrisiko vorliegt
  - ✓ beachte: immer Pflicht zur Benennung des DSB, wenn DSFA durchgeführt werden muss (§ 38 Abs. 1 S. 2 BDSG)

3. Maßnahmen zur Umsetzung der Vorgaben (SOLL-Analyse)

- **Sonstiges**

  - ✓ Ist der Webauftritt der Praxis ds-konform?
  - ✓ Sind die Mitarbeiter ausreichend sensibilisiert?
  - ✓ Ist die Praxis auf die Erfüllung der Meldepflichten (Art. 33 f. DS-GVO) im Falle einer Datenpanne vorbereitet (Festlegung des Workflows, interne Zuständigkeit)?

Maßnahmenplan für niedergelassene Heilberufspraxen

4. Weiterführende Informationen und Hilfestellungen

- Auf Homepages der Koop.partner sowie der gemeinsamen Seite www.mit-sicherheit-gut-behandelt.de
- KBV und BÄK haben Hinweise und Empfehlungen zur ärztlichen Schweigepflicht und Datenschutz einschließlich eines Datenschutz-Checks veröffentlicht
- LÄK RP, BezÄKn, LPK, KV RP und LfDI RP stehen im Rahmen ihrer Möglichkeiten für Anfragen zur Verfügung

4. Weiterführende Informationen und Hilfestellungen

- DSK hat diverse Kurzpapiere zu einzelnen Inhalten der DS-GVO einschließlich Maßnahmenplan erarbeitet
- Auf europäischer Ebene werden Arbeitspapiere zu Themenfeldern der DS-GVO erstellt, die EU-weit abgestimmt sind (über www.datenschutz.rlp.de erschließbar)

Fazit: „Alles halb so schlimm!“

Und nicht vergessen:

- ☺ Bange machen gilt nicht!
- ☺ Am Anfang war das Wort…
- ☺ Datenschutz ist Chefsache!

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Noch Fragen?

Michael Heusel-Weiss

Referent

beim Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz

+49 (6131) 208-2549
m.heusel-weiss@datenschutz.rlp.de
Postfach 30 40 - 55020 Mainz