Deutscher Anwaltverein
Arbeitsgemeinschaft Medizinrecht

18. Frühjahrstagung

vom 20. bis 21. April 2018 in Nürnberg

Datenschutzrechtliche Fragen im Gesundheitswesen

Elisabeth Kraml,
Bayerisches Landesamt für Datenschutzaufsicht,
Ansbach

Datenschutzrechtliche Fragen im Gesundheitswesen

1. **Rechtsgrundlagen der Verarbeitung selbst in der Telemedizinanwendung**
   - Grundsätzliche Zulässigkeit der Verarbeitung für Behandlungszwecke ergibt sich aus Artt. 6 Abs. 1 Satz 1 lit. b, 9 Abs. 2 lit. h DS-GVO, § 22 Abs. 2 Nr. 1 b BDSG-neu und ggf. Spezialvorschriften => i.d.R. keine Einwilligung nötig
   - Im Einzelfall problematisch kann die Einhaltung von Art. 9 Abs. 3 DS-GVO sein

2. **Einbindung von Dienstleistern**
   - Sonderfall: Gemeinsame Verantwortlichkeit Art. 26 DS-GVO
   - In der Regel oft Auftragsverarbeitung nach Art. 28 DS-GVO; Formulierungshilfe unter https://www.lda.bayern.de/media/muster_adv.pdf
   - § 203 Abs. 3 und 4 StGB erfordert ebenfalls entsprechende Bindung des Dienstleisters
   - Art. 9 Abs. 3 DS-GVO kann in jedem Fall bei deutschem Dienstleister über § 203 Abs. 3 und 4 StGB erfüllt werden, ansonsten str., ob Vertrag nach Art. 28 DS-GVO o.Ä. Verpflichtungen ausreichen
   - Beim Einsatz internationaler Dienstleister sind zusätzlich die Anforderungen an die Übermittlung in ein Drittland zu berücksichtigen (Artt. 44 ff DS-GVO). Als Rechtsinstitut kommen i.d.R. Angemessenheitsbeschlüsse und Standardverträge in Betracht

3. **Technischer Datenschutz**
   Individuell anhand des jeweiligen Verarbeitungsrisikos sind Maßnahmen nach Art. 32 auszuwählen; pauschale Aussagen sind nicht möglich; typische Maßnahmen sind: Ende-zu-Ende Verschlüsselung, 2-Faktor-Authentifizierung, Mandantentrennung, Protokollierung lesender und schreibender Zugriffe.

4. **Datenschutz-Folgenabschätzung**
   - Bei Telemedizin erforderlich
   - Es kann aus den unterschiedlichen Verfahren (Aufsichtsbehörden, ISO) gewählt werden; Auswahl:
     - DSK https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf
     - SDM: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.0.pdf
     - ICO: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
     - CNIL https://www.cnil.fr/en/privacy-impact-assessment-pia (mit OnlineTool)
   - Verbleibt ein Risiko ist die Aufsichtsbehörde zu kontaktieren.

5. **Auswahl weiterer beachtenswerter Anforderungen**
   - Rechenschaftspflicht (Art. 5 Abs. 2, 24 DS-GVO)
   - Informationspflichten (Artt. 13 und 14 DS-GVO)
   - Datenpannen (Artt. 33 ff DS-GVO)
   - Betroffenenrechte (Artt. 15 ff. DS-GVO)

Elisabeth Kraml, Bayerisches Landesamt für Datenschutzaufsicht