

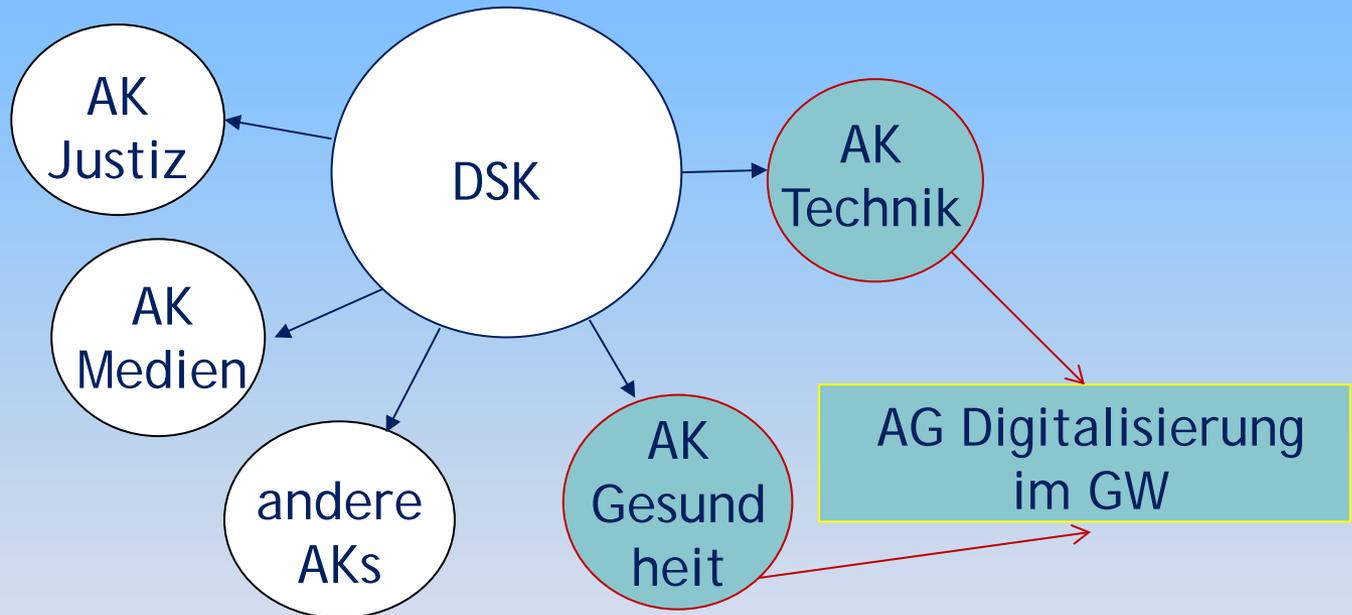
Fachtagung Datenschutz im Gesundheitswesen:
Evaluierung der DS-GVO: Das kann doch weg, oder?

Datenschutz als konstruktiver Wegbegleiter einer digitalen Gesundheitsversorgung



- Arbeitsstrukturen der Datenschutzkonferenz im Gesundheitsbereich
- Aktuelle Themen im Bereich Recht einschließlich DSK-Entscheidungen
- Erfahrungsbericht des LfDI Rheinland-Pfalz

- Arbeitsstrukturen der Datenschutzkonferenz im Gesundheitsbereich



AG Digitalisierung im GW

Vorsitz: BfDI

Mitglieder: 10 Datenschutz-Aufsichtsbehörden

verschiedene Themenfelder, u.a.:

- Nutzung von Cloud-Diensten
- Messenger-Dienste im Krankenhausbereich
- Elektronische Patientenakte
- Gesundheits-Apps
- Datenverarbeitung im Auftrag
- Big Data und Künstliche Intelligenz

AG Digitalisierung im GW

Beispiele aus der Arbeit der AG:

- Inhaltliche Abstimmung zu DVG u.a.
- Whitepaper zum Einsatz von Messenger-Diensten

- Aktuelle Themen im Bereich Recht einschließlich DSK-Entscheidungen

Gesetzgebung zur digitalen Gesundheitsversorgung

- DVG/DiGAV
- Datenschutzrecht steht einer zeitnahen Digitalisierung des Gesundheitswesens nicht entgegen
- allerdings sind Vorgaben des DS-GVO zwingend zu beachten
- diverse dsr Defizite bei DVG/DiGAV aus Sicht der DSK

Gesetzgebung zur digitalen Gesundheitsversorgung

Im Einzelnen:

- zwar Rechtsanspruch der Versicherten auf digitale Gesundheitsanwendungen, aber Vertraulichkeit der Patientendaten ist nicht verlässlich gewahrt (Aufnahme in Liste BfArM erfolgt nur aufgrund von Herstellerangaben!)
- rechtlich fragwürdig: Verarbeitungsbefugnisse der Hersteller (Einwilligung im Bereich SGB V, Umfang der DV, fehlende Geheimhaltungspflicht)

Gesetzgebung zur digitalen Gesundheitsversorgung

Im Einzelnen:

- Rolle der Krankenkassen (Genehmigung des Einsatzes digitaler Gesundheitsanwendungen, Nutzung von Patientendaten zur Entwicklung digitaler Innovationen)

Gesetzgebung zur digitalen Gesundheitsversorgung

- Patienten-Datenschutzgesetz
- Stand: Kabinettsentwurf (01.04.2020)
- bisherige Vorgaben zur elektronischen Gesundheitskarte werden modifiziert, insbesondere Regelungen z.B. zur dsr Verantwortlichkeit in der TI, zur Schaffung einheitlicher Ansprechpartner und Ombudsstellen, zur elektronischen Patientenakte, zur Beteiligung von BSI und BfDI sowie zur Datensouveränität der Patienten

Gesetzgebung zur digitalen Gesundheitsversorgung

Einzelne Defizite aus Sicht des LfDI RP:

- Zuordnung der datenschutzrechtlichen Verantwortlichkeit der gematik unzureichend (mittlerweile bereinigt)
- Interessenkollision der gematik bei Zugriffskomponenten auf E-Verordnung (Anbieter und Zulassungsstelle)
- Unzureichende Einbindung von BSI und BfDI bei Gefährdungslagen

Gesetzgebung zur digitalen Gesundheitsversorgung

Einzelne Defizite aus Sicht des LfDI RP:

- bei ePA nur stufenweise Umsetzung des gesetzlich garantierten Zugriffsrechtenmanagements für Versicherte (in der ersten Stufe nur Einräumung pauschaler Zugriffsrechte möglich - „alles oder nichts“)
- Versicherte ohne geeignetes Endgerät haben dauerhaft nur mittelgranulares Zugriffsrechtenmanagement
- individuelle Freigabemöglichkeit der Versicherten von Daten aus ePA für Forschung (Datenspende) zu unbestimmt

Künstliche Intelligenz/Big Data im Gesundheitsbereich

- KI war Schwerpunktthema des DSK-Vorsitzes 2019 (Rh.-Pf.)
- 97. DSK (April 2019): Hambacher Erklärung zur KI



Künstliche Intelligenz/Big Data im Gesundheitsbereich

Hambacher Erklärung:

- grundsätzliche dsr Anforderungen an KI
- noch ausstehend: Umsetzung der Anforderungen im Bereich Gesundheit
- 98. DSK (November 2019): Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Gewährleistung von Datensicherheit in Gesundheitseinrichtungen

- EntschlieÙung der 98. DSK (November 2019)
- Zielrichtung:
flächendeckende Gewährleistung eines angemessenen Datensicherheitsniveaus in allen Versorgungseinrichtungen ist unabhängig von ihrer Größe geboten
- Forderung DSK:
auch in finanzieller Hinsicht muss sichergestellt werden, dass Einrichtungen unabhängig von ihrer Größe die nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können

Gewährleistung von Datensicherheit in Gesundheitseinrichtungen

- Hintergrund:
mehrere IT-Sicherheitsvorfälle im Jahre 2019 in stationären Einrichtungen (u.a. in RLP)

Gesundheitswebseiten und Gesundheits-Apps

- EntschlieÙung der 98. DSK (November 2019)
- Zielrichtung:
keine unbefugte Weitergabe sensibler Daten der Nutzer von Gesundheitswebseiten und -Apps an Dritte (Tracking-/Analyse-Dienstleister)
- Hintergrund:
diverse Recherchen offenbaren Integration von Tracking- und Analysediensten ohne adäquate Einbindung der Nutzer

Gesundheitswebseiten und Gesundheits-Apps

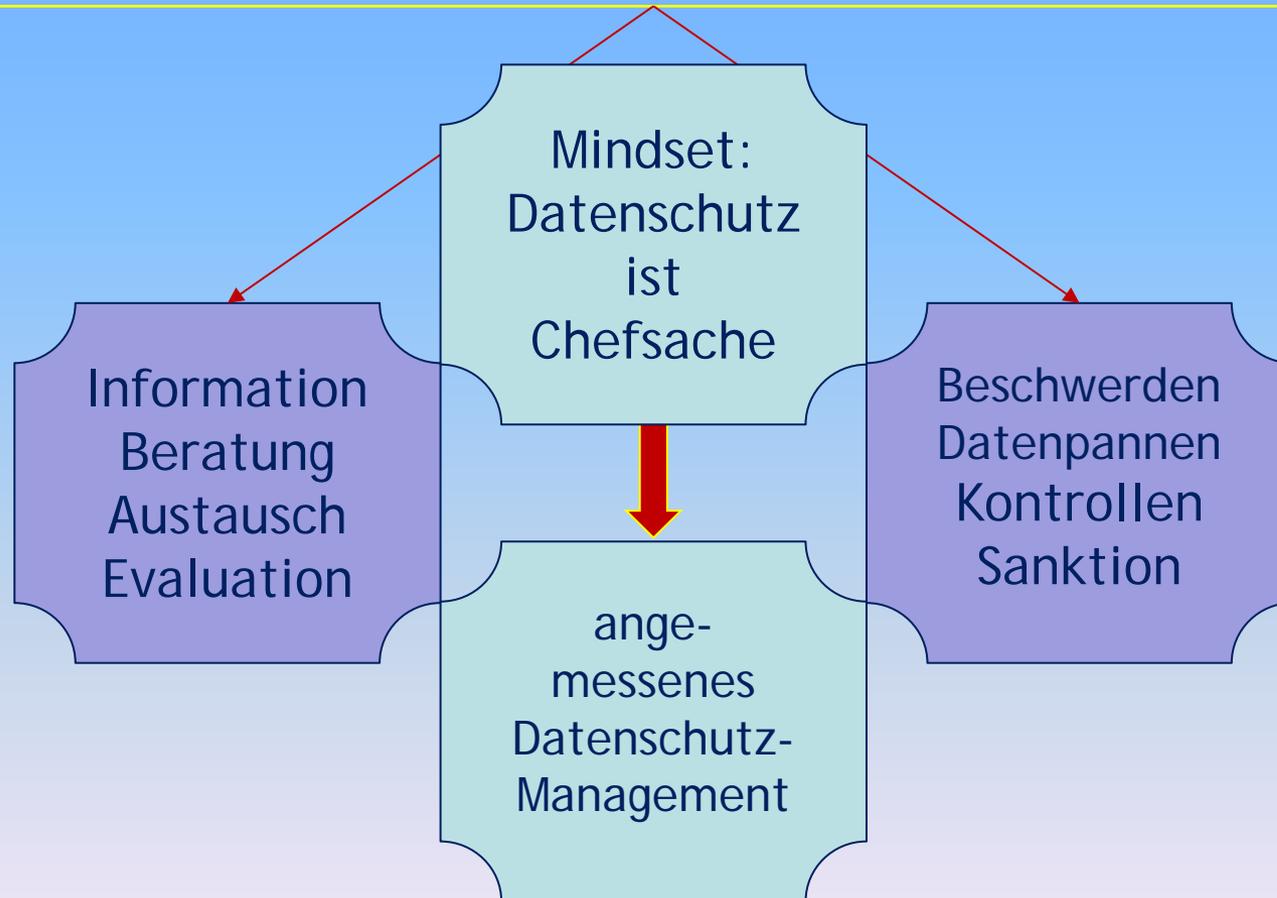
- Inhalte:
 - Betreiber müssen die Vorgaben beachten (Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
 - strenge Transparenzanforderungen an Einwilligung
 - im Rahmen der Regelversorgung ist einwilligungsbasierte Weiterleitung an DL außerhalb des Gesundheitssystems unzulässig, wenn Dienste zum Betrieb entbehrlich sind
 - Appell an Gesetzgeber, tätig zu werden

Umsetzung der Vorgaben der DS-GVO bei Ärzten/Psychotherapeuten

- seit 2014: Initiative „Mit Sicherheit gut behandelt“
- Kooperation des LfDI mit KV RP, Landesärztekammer RP und Landespsychotherapeutenkammer RP
- zahlreiche Informationsveranstaltungen; 2018: 4 zur DS-GVO
- Kernstück: Website www.mit-sicherheit-gut-behandelt.de
- praktische Hilfestellungen zur Umsetzung des Datenschutzrechts und insbesondere zur DS-GVO

- Erfahrungsbericht des LfDI Rheinland-Pfalz

generelle Strategie des LfDI RP im Bereich Gesundheit



Beratungsaufkommen/Schwerpunkte

- unmittelbar nach Wirksamwerden der DS-GVO sehr hoher Beratungsbedarf von ambulanten und stationären Einrichtungen
- damaliger Schwerpunkt: Datenschutz-Management
- derzeit immer noch deutlicher Beratungsbedarf
- im Fokus: Auskunftsrecht, E-Mail-Kommunikation, toM, Abgrenzung Einwilligung (als DV-Befugnis) und bloße Information nach Art. 13 DS-GVO, aber auch berufsrechtliche Fragen (Praxisübergabe, Archivierung)

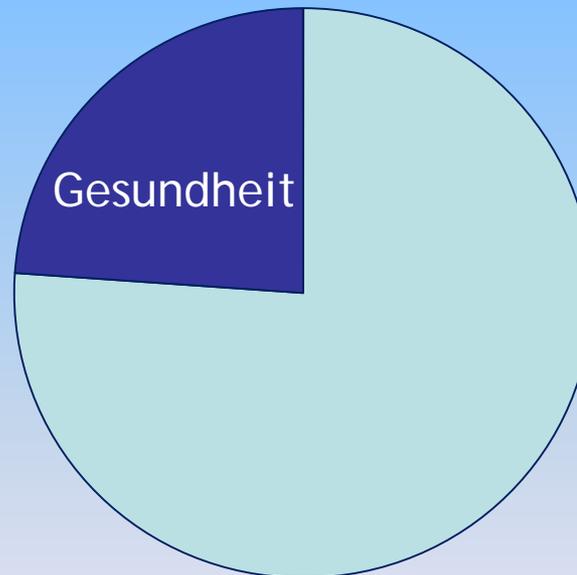
Beratungsaufkommen/Schwerpunkte

- Initiative „Mit Sicherheit gut behandelt“ in RP
- Rolle von anderen Akteuren (Verbände, Heilberufskammern und KV) bei Beratung definieren
- wichtig: Vernetzung, Austausch, Perspektivwechsel

Meldungen nach Art. 33 DS-GVO

Datenpannen-Meldungen an LfDI RP 2019

Gesundheit: 86



Gesamtzahl: 360

Meldungen nach Art. 33 DS-GVO

Position LfDI RP:

Schwelle der Meldepflicht des Art. 33 Abs. 1 DS-GVO ist immer erreicht, wenn Verstöße Patientendaten betreffen.

Grund:

- ➔ Gesundheitsdaten sind besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO
- ➔ Ein DS-Verstoß führt dann automatisch ein Risiko für die Rechte und Freiheiten natürlicher Personen mit sich



Verstöße im Gesundheitsbereich sind immer meldepflichtig!

Meldungen nach Art. 33 DS-GVO

Häufigste Ursachen der gemeldeten Verstöße:

- Fehler bei Kuvertierung (Versand mehrerer Dokumente)
- Unzureichende Adressierung von Faxen und Briefen
- Unverschlüsselter E-Mail-Versand
- Verlust von Datenträgern
- Defizite bei Entsorgung von Datenträgern/Akten

Meldungen nach Art. 33 DS-GVO

Schlussfolgerungen aus Meldungen

- Beachtung von Art. 32 DS-GVO zwingend (toM)
- nach eingetretenem Verstoß: Fehleranalyse und ggf. Ergänzung/Anpassung der bisherigen toM
- Empfehlung LfDI: einrichtungsinterne Analyse der in einem bestimmten Zeitraum aufgetretenen Verstöße durch DS-Management durchführen und angemessene Verbesserungen veranlassen

Meldungen nach Art. 33 DS-GVO

Schlussfolgerungen aus Meldungen

- Ende 2019 bundesweite Presserecherche bzgl. Meldungen nach Art. 33 DS-GVO im Gesundheitsbereich
- LfDI fordert alle Akteure im Gesundheitswesen zu sorgfältigerem Umgang mit Patientendaten auf
- <https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/falschversand-von-patientenbezogenen-unterlagen-ist-bundesweit-weit-verbreitet>

Sanktionspraxis

- 2019 Bußgeld in Höhe von 105.000 Euro ggü. Universitätsmedizin Mainz
 - ➔ DV im Zusammenhang mit Patientenverwechslung, Weitergabe an Dritte, strukturelle und gravierende Defizite im Datenschutz-Management
- ansonsten diverse Bußgeldbescheide sowie Verwarnungen
- Ziel: höhere Sensibilität bei DV im Gesundheitsbereich

Vielen Dank!

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

www.datenschutz.rlp.de