Datenschutzrecht

CAU

Auftragsdatenverarbeitung,
Berufsgeheimnis, Medizindatenschutz,
Sozialdatenschutz
IT-Sicherheit bei KritIS

17. Januar 2018

Harald Zwingelberg

ITS APT

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Ankündigungen

- Alte Klausur als Orientierung hinsichtlich Art und Umfang der Fragen ist jetzt online.

- Gesetzestexte jetzt online oder selbst zusammenstellen:
  - DSGVO (insbesondere Art. 1-35)
  - §§ 203-205 StGB

- Die Vorlesungen von Susan Gonscherowski zu Datenschutz zu Telemedien wird am Montag, den 5. Februar um 16:00 Uhr voraussichtlich im Audimax nachgeholt

Wiederholung

Auftragsdatenverarbeitung, goldende Regeln,

Wiederholung

- Nennen sie die 7 Grundprinzipien des Datenschutzes (goldene Regeln)

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle

Wiederholung
Auftragsdatenverarbeitung - Pflichten

Pflichten / Aufgaben des Verantwortlichen

- Sorgfältige Auswahl und Überwachung nach Art. 28
- Vertragliche Bindung
- Bereitstellung der erforderlichen Informationen für den Auftragsverarbeiter

Pflichten des Auftragsverarbeiters

- Bei Sitz im Drittland – Bestellung eines Vertreters in der Union, Art. 27
- Verzeichnis der Verarbeitungstätigkeiten, Art. 30 (2)
- Vornahme der erforderlichen techn.-org. Maßnahmen (kurz: TOMs)
- Meldung von Sicherheitsverstößen an den Verantwortlichen, Art. 33 (2)
- Unterstützung bei der Datenschutzfolgenabschätzung,
- Benennung eines Datenschutzbeauftragten

Wiederholung
Auftragsdatenverarbeitung - Rechtsfolgen

Rechtsfolgen

- Datentransfer zum und Verarbeitung beim Auftragsverarbeiter ist privilegiert, d.h. sie bedarf keiner gesonderten Rechtsgrundlage neben dem Auftrag.
- Auftragsverarbeiter haftet nur für die Verletzung der speziellen Pflichten eines Auftragnehmers oder bei Verstoß gegen eine Weisung auf Schadensersatz, Art. 82 (2).
  Bei Überschreiben des Auftrags wird Auftragsverarbeiter mit allen Pflichten und Risiken zum Verarbeiter.
- Geldbußen können gegen den Auftragnehmer verhängt werden.
- U.a. ist bußgeldbewährt ein fehlender Vertrag, so dass künftig Auftragnehmer einen solchen aus Eigeninteresse anbieten sollten. Bisher bestenfalls auf gesonderte Nachfrage für Geschäftskunden.

Gesundheitsdatenschutz

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Medizin- und Sozialdatenschutz

1. Geheimnisschutz
2. Gesetzesgrundlagen, Datenerhebung
3. Einwilligung – Schweigepflichtsentbindungserklärung
4. Zweckbindung und Erforderlichkeit
5. Datenübermittlung
6. Betroffenenrechte, insbesondere Akteneinsichtsrechte
7. Datensicherheit
8. Kontrolle

Fragen

- Patientendaten beim Arzt und Versichertendaten bei den Sozialversicherungen unterliegen einem besonderen Schutz. Welche Gründe könnte es dafür geben? Wer hat ein Interesse an diesem Schutz?

- Welche Sozialversicherungsträger (Sozialversicherungen) kennen Sie?

- Welche Gründe kann es geben Daten bei Sozialversicherungsträgern besonders zu schützen?

Gründe für Schweigepflicht und Sozialgeheimnis

Ärztliche Schweigepflicht

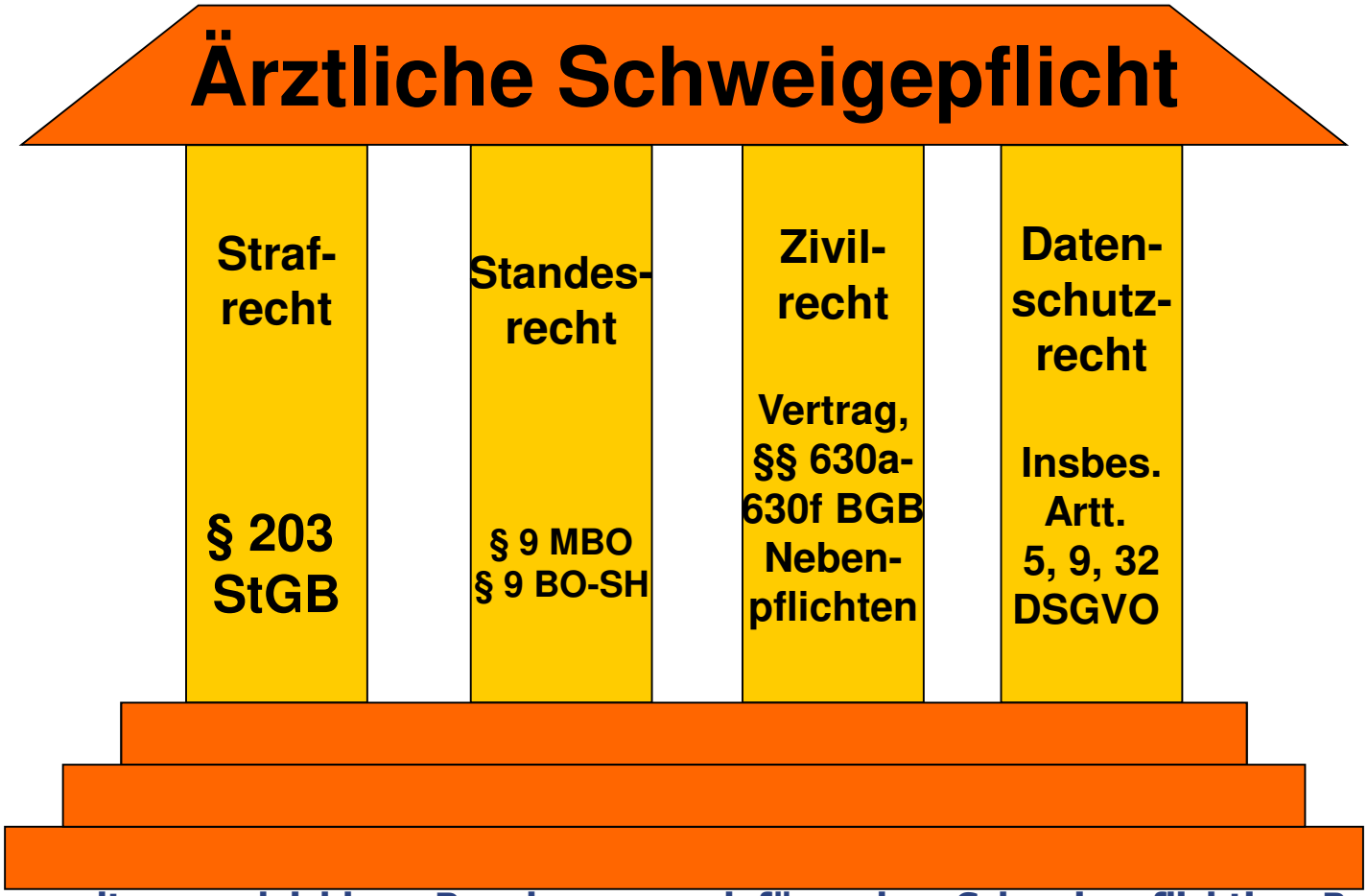
- Persönlichkeitsrecht des Patienten
- staatliches Interesse an gesunden Bürgern und Vertrauen in die Vertraulichkeit der Arzt-Patientenbeziehung
- Eigeninteresse der Ärzte – Vertrauen der Patienten (therapeutisch und wirtschaftlich – siehe Erläuterungen zum Hippokratischen Eid)
- besonders schutzbedürftige Daten

Sozialgeheimnis

- Persönlichkeitsrecht des Betroffenen
- staatliches Interesse an der Vermeidung sozialer Notlagen
- Angehörige einer Sozialversicherung (ob zwangsweise oder freiwillig) sollen nicht mehr staatlichen Eingriffen ausgesetzt sein als andere
- besonders schutzbedürftige Daten (insbes. Gesundheit, Vermögen, soziale Verhältnisse)

Beachte: Auch Datenschutzrechtlich unterliegen Gesundheitsdaten als eine Art von besonders sensitiven Daten nach § 9 DSGVO besonderen datenschutzrechtlichen Anforderungen . Im Sozialrecht finden sich diese im SGB X.

Grundlagen der ärztlichen Schweigepflicht*



*** im Kern gelten vergleichbare Regelungen auch für andere Schweigepflichtige: Beamte bezüglich Amtsgeheimnissen, Rechtsanwälte, Steuerberater, Geistliche, … Unterschiede bestehen bezüglich der anwendbaren Rechtsgrundlagen.**

Umfang und Adressatenkreis der ärztlichen Schweigepflicht

§ 203 StGB: Verletzung von Privatgeheimnissen

- Adressatenkreis: u.a. Ärzte, Zahnärzte, Tierärzte, Heilberufe mit staatl. Prüfung, Psychologen, Rechtsanwälte, Notare, Steuerberater, Ehe- Familien Jugendberater, Mitglieder von Beratungsstellen, Sozialarbeiter, Mitarbeiter privater Krankenkassen bzw. Unfall- oder Lebensversicherungen,
  Umfang: Bereits die Tatsache, dass jemand Patient ist
- „unbefugte" Offenbarung eines fremden Geheimnisses
  - Keine Mitteilung an Familienmitglieder der Patienten
  - Schweigepflicht gilt idR über den Tod des Patienten hinaus
  - Rechtfertigung der Geheimnisoffenbarung durch
    - Einwilligung
    - Mutmaßliche Einwilligung (z.B. bei Bewusstlosen)
    - Gesetzliche Offenbarungspflichten (z.B. § 138 StGB)
    - Rechtfertigender Notstand (z.B. § 34 StGB)

Grenzen der Schweigepflicht: Beispiele

- Bankräuber beim Arzt: Pflicht zur Anzeige nur bei bestimmten geplanten (künftigen) Straftaten (vgl. § 138 StGB). Im Übrigen: Schweigepflicht
- Misshandeltes Kind beim Arzt: § 34 StGB – Recht zur Benachrichtigung der zuständigen Stelle, z.B. des Jugendamtes, aber keine Mitteilungspflicht
- Alkoholiker fährt regelmäßig Auto: Mitteilung an Register? § 34 StGB
- Einschaltung externer Inkassounternehmen bei der Behandlungsabrechnung als Auftragsverarbeiter denkbar (siehe unten)
- HIV-Patient beim Arzt: Pflicht zur Mitteilung der HIV-Infektion an den/die Sexualpartner(in)? § 34 StGB bei Anhaltspunkten für eine *konkrete* Ansteckungsgefahr (z.B. erklärte Absicht des Patient zu ungeschütztem Geschlechtsverkehr mit einer bestimmten Person) (so ein sehr umstrittenes - und nach allg. Meinung falsches - Urteil des OLG Frankfurt)
- Arzthaftungsprozess: Mitteilung von Patientendaten zur rechtlichen Verteidigung? Nach § 34 StGB zulässig, aber nur im erforderlichen Umfang
- Polizei fahndet nach einem Bankräuber und befragt den Arzt, bei dem dieser in Behandlung war: Schweigepflicht

Rechtliche Bedeutung der Schweigepflicht

- Verfassungsrechtliche Ausgangslage: Dem Bürger ist alles erlaubt, was nicht verboten ist (Art. 2 Abs. 1 GG: Recht auf freie Entfaltung der Persönlichkeit, insb. allgemeine Handlungsfreiheit).
- Im Datenschutz gilt aber auch für Private: Alles ist verboten, was nicht erlaubt ist (vgl. § 4 Abs. 1 BDSG, § 11 I LDSG bzw. neu Art. 6 (1) und Art. 5 (1) (a) DSGVO). – Jeder Umgang mit personenbezogenen Daten bedarf einer rechtlichen Grundlage. [Stichwort: Rechtmäßigkeit]

- In Bereichen, die einem besonderen Geheimnisschutz unterstellt sind (neben der ärztlichen Schweigepflicht und dem Sozialgeheimnis etwa auch das Steuergeheimnis) werden an die rechtlichen Grundlagen besondere Anforderungen gestellt: Daten dürfen nur dann erhoben, verarbeitet und übermittelt werden, wenn ***bereichsspezifische*** Regelungen dies erlauben.
  Also bei besonderem Verbot braucht es auch eine solche Ausnahme.

Sozialgeheimnis

- § 35 Abs. 1 Satz 1 SGB I – Sozialgeheimnis:
- Berechtigter: „Jeder" (über den Sozialdaten erhoben werden) Leistungsempfänger, Vermieter, Arbeitgeber,...
- Adressat: alle Leistungsträger (nicht Leistungserbringer wie z.B. Ärzte)

  => Institutionenbezogenes Spezialrecht für Leistungsträger
- Klarstellung: Auch innerhalb eines Leistungsträgers dürfen Daten nur Befugten zugänglich sein, § 35 I SGB I

- Gegenstand: Sozialdaten nach § 67 Abs. 1 SGB X

  „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener)"
- Normbefehl:
  - Verbot „unbefugter" Datenverarbeitung
  - § 35 II SGB I: nur nach den Voraussetzungen der §§ 67 ff. SGB X

Erhebung von Sozialdaten, § 67a SGB X

- Grundsatz: Sozialdaten dürfen erhoben werden, wenn sie zur Aufgabenerfüllung erforderlich sind
  - Keine Datenerhebung auf Vorrat
  - Nur entscheidungserhebliche Tatsachen
  - Daten müssen auch tatsächlich Verwendung finden
  - Kontoauszüge: Vorlagepflicht für Auszüge der vergangenen 3 Monate, Schwärzung bei bes. Arten pers.bez. Daten statthaft. § 67a I 2, iVm § 67 XII SGB X
  - Kopien für die Akte nur, soweit klärungsbedürftige Buchung vorhanden. Nach Klärung Löschung
  - Praxis weicht davon wohl noch ab mit Hinweis auf andernfalls fehlende Nachvollziehbarkeit der Entscheidungen.

Zu Kontoauszügen siehe: BSG, Urteil vom 19. 9. 2008 - B 14 AS 45/ 07 R

Erhebung von Sozialdaten, § 67a SGB X

- Es gilt der Grundsatz der Datenerhebung beim Betroffenen

- Transparenz: Betroffener muss bei Erhebung über den Zweck der Erhebung und Verarbeitung, die verantwortliche Stelle und die relevanten Rechtsvorschriften informiert werden.

- Hinweis auf Rechtsfolgen: Soweit eine Auskunftspflicht besteht oder bei Nichtauskunft Nachteile drohen, ist darauf hinzuweisen.
  (Auskunftspflicht z.B. in § 60 SGB I, Folgen § 66 SGB I)

Einwilligung in eine medizinische Untersuchung

Medizinrechtliche Einwilligung

- Einwilligung in den Eingriff, andernfalls ist Behandlung eine Körperverletzung
- Informed consent = Aufklärung und freie Einwilligung
- Aufklärung über
  - 1. Diagnose und Diagnosesicherheit
  - 2. Verlaufsprognose
  - 3. Wesen der Maßnahme, Mitwirkungspflichten
  - 4. Erfolgsquote, Nutzen
  - 5. Komplikationen und Komplikationswahrscheinlichkeit
  - 6. Handlungsalternativen
  - 7. Wirtschaftliche Aufklärung

- Schwerpunkt: Einwilligung in körperlichen Eingriff
- Aber auch: Einwilligung in Informationsgewinnung und übermittlung (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen)

Datenschutzrechtliche Einwilligung:

- Informierte Einwilligung, Art. 13 DSGVO
- Anforderungen nach Art. 7 DSGVO, insb.:
  - freie Entscheidung, Art. 7 (4)
  - Aufklärung über den Zweck der Datenerhebung oder -verarbeitung Art. 13 (1) (c)
  - Keine Formpflicht aber Nachweisobliegenheit, Art. 7 (1)
  - ggf. besondere Hervorhebung der datenschutzrechtlichen Einwilligungserklärung Art. 7 (2)
  - ausdrücklicher Hinweis auf die Verwendung von Gesundheitsdaten, Art. 8 (2) (a) DSGVO
- Schwerpunkt: Schutz des Rechts auf informationelle Selbstbestimmung
- beachte z.B. § 9 Abs. 3 MBO: Hinweis auf die Daten, die aufgrund einer vermuteten Einwilligung übermittelt werden dürfen

Einwilligung - Beispielsfälle

- Heimlicher HIV-Test – unzulässig, da keine zu erwartende Routineuntersuchung
- Forschung: Forschung mit anonymisierten Daten ist zulässig, Untersuchungen an personenbezogenen Proben ohne Einwilligung sind i.d.R. unzulässig (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen).
- Fotos von Patienten als Gedächtnisstütze für den Arzt: keine übliche Maßnahme und nicht erforderlich für Patientenakte aber mit Einwilligung der Patienten möglich. Keinesfalls darf fotografiert werden ohne vorherige Aufklärung und Einwilligung.
- Betriebsarzt: Proband muss über die Untersuchung im Vorwege aufgeklärt werden, insbesondere wenn Untersuchung nicht üblich oder erkennbare Voraussetzung für die angestrebte Tätigkeit ist.

Zweckbindung und Erforderlichkeit

- Der Zweck der Erhebung und Verarbeitung muss hinreichend bestimmt sein. Rahmen ist in der Regel das konkrete Behandlungsverhältnis
- Der Umfang der Erhebung und Verarbeitung der Daten muss erforderlich sein. (Die Erforderlichkeit wird häufig durch die gesetzgeberische Wertung sichergestellt. Gesondert geprüft werden muss sie nur dort, wo sie ausdrücklich erwähnt wird, z.B. § 28 Abs. 6 Nr. 1 BDSG.)
- Arzthaftungsprozess: Es dürfen nur Patientendaten dem RA offengelegt werden, deren Kenntnis für den Prozess erforderlich ist, Art. 9 (2) (f) DSGVO. Schwierige Bestimmung der Erforderlichkeit, weil Vor- oder Miterkrankungen u.a. für die Bestimmung der Schadenshöhe relevant sind und diese Bewertung oft nur im Dialog mit dem RA erfolgen kann.
- Forschung, Archive, Statistik: Art. 9 (2) (j) DSGVO i.V.m. nationalen Gesetzen wie § 27 BDSG-neu, §§ 13, 26 LDSG-SH-Entwurf 2018

Typische Übermittlungsbefugnisse

- Abrechnung mit der Kassenärztlichen Vereinigung
- Bei Privatliquidation ist bisher Einwilligung für Übermittlung an eine Einzugsstelle notwendig – Transparenzpflicht bleibt aber!
  neu: kein Hindernis im StGB mehr durch § 203 III 2 StGB-2017
- §§ 284 ff, 294 ff SGB V (Vertragsarztrecht)
  - Wirtschaftlichkeitsprüfungen
  - Qualitätsprüfungen z.B. Sonografie (Stichproben)
- Meldepflichten: InfektionsschutzG, KrebsregisterG
- Bei vor-, mit und nachbehandelnden Ärzten wird konkludente Einwilligung unterstellt - d.h. Widerspruch ist möglich, § 9 MBO
- Praxisinterne Übermittlung, gegenseitige Einsicht in Patientenakten:
  (+) Gemeinschaftspraxis (Partner, Gesellschaft), MVZ,
  (-) Praxisgemeinschaft (gemeinsam genutzte Räume und Mitarbeiter), angegliederte Kosmetikerin beim Dermatologen
- Klinken: Meldeschein Hotel zur Einsicht der Polizei, wie bei Hotel

Übermittlung von Sozialdaten, §§ 67d ff SGB X

- Übermittlung Grundsatz: Es bedarf einer **gesonderten Übermittlungsbefugnis**, die von der übermittelnden Stelle zu prüfen ist. Soweit eine andere Stelle anfragt, trägt diese die Verantwortung für die Richtigkeit der Anfrage, §_67d II SGB X

- diverse Übermittlungsbefugnisse in §§ 68-77 SGB X und anderen Sonderregelungen, z.B. für den Datenabgleich gegen Sozialleistungsmissbrauch und Schwarzarbeit

- Bei erhobenen medizinischen Daten Weitergabe nur, wenn sie dem Arzt selbst gestattet gewesen wäre, § 76 I SGB X

Betroffenenrechte im Medizinbereich

medizinrechtliche Ansprüche

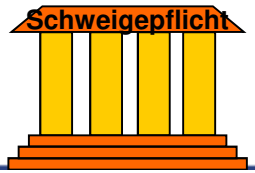
- Medizinrechtlicher Auskunftsanspruch aus Art. 2 I i.V.m. Art. 1 I GG
  - Patientenautonomie als Ausprägung des Rechts auf freie Entfaltung der Persönlichkeit
- Einsicht in Patientenakte:
  - § 630g BGB als Teil des Behandlungsvertrags
  - § 10 II Berufsordnung Ärzte
- Alle objektive Befunde unterliegen dem Einsichtsrecht. Arzt darf aber persönliche Notizen schwärzen.

datenschutzrechtliche Ansprüche

- Art. 13, 14 DSGVO Benachrichtigung
- Art. 15 DSGVO Auskunft
- Art. 17 DSGVO Löschung
- Art. 18 DSGVO Sperrung

- Zusätzlich: Schadensersatzanspruch

Für den Sozialdatenschutz finden sich entsprechende Regelungen in den §§ 84 ff. SGB X



Datensicherheit im Gesundheitsbereich

- Gesundheitsdaten sind besondere Arten von Daten und unterliegen je nach datenverarbeitender Stelle besonderer Berufsgeheimnisse.
- Es sind die **geeigneten** Maßnahmen zu treffen mit Rücksicht u.a. auf das **Risiko für die Betroffenen**.
- Umfang hängt von Quantität und Qualität der Daten ab, insbesondere welche Einschnitte Betroffene bei einem Datenverlust erleiden würden.
- Arzt hat dabei sicherzustellen:
  - Vertraulichkeit — Keine Einsicht durch Dritte
  - Verfügbarkeit — Dokumentation, Folgebehandlungen
  - Integrität — Aufbewahrungsfirsten

Auftragsverarbeitung

- Bis 2017 war Auftragsverarbeitung für Berufsgeheimnisträger nur in Ausnahmefällen (Ländergesetze) möglich oder auf Grund einer Einwilligung.
- Seit 2017: § 203 Abs. 3 StGB:

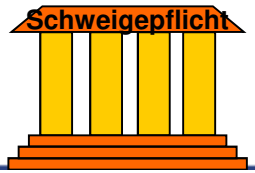
  Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.
- Damit entfällt die Strafbarkeit
- Das ist für sich allein aber keine Erlaubnis.
- Als Rechtsgrundlage kommt dann eine Auftragsverarbeitung nach der DSGVO in Betracht.

Auftragsverarbeitung

- Besondere Anforderungen an die Auftragsverarbeitung im Gesundheitsbereich:
  - Zwingende Bekanntgabe der Identitäten der Auftragsverarbeiter, Zwecke, Umfang der Verarbeitung vor Beginn der Behandlung
  - Besonders sorgfältige Auswahl aller Auftragsverarbeiter.
  - Klare Verpflichtung auf die Verschwiegenheit zwingend – Auftragnehmer muss alle eingesetzten Mitarbeiter verpflichten.
  - Soweit möglich müssen Betroffene einzelnen Verarbeitungen widersprechen können – Praktisch nicht möglich beim Haupt-IT-Dienstleister eine Klinik, denkbar aber durchaus bei der Auswahl eines externen Medizin- oder Dentallabors.
  - Eine Auftragsverarbeitung in Drittstaaten wird oft mangels hinreichender Garantien zur Gewährleistung Datensicherheit nicht möglich sein – insbesondere gegen staatliche Zugriffe. Insoweit muss m.E. das Berufsgeheimnis gewahrt bleiben.

Kontrolle im Gesundheitsbereich

- Die Kontrolle erfolgt intern (bDSB) – i.d.R. bei Kliniken oder extern.
- Externe Kontrolle je nach rechtlicher „Säule“
  - DSGVO: Datenschutzbehörden
  - Berufsrecht: Kammern (Ärztekammer, Anwaltskammer, Notarkammer, etc.)
  - Strafrecht: Staatsanwaltschaft. Wenn ein solcher Fall beiden Aufsichtsbehörden landet, wird er an die zuständige StA abgegeben. Da § 203 StGB ein Antragsdelikt ist, muss ein Geschädigter Strafantrag stellen, § 205 StGB.
  - BGB: Patient verfolgt seine Ansprüche selbst auf dem Zivilrechtsweg.



Gesundheitsdatenschutz

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

IT-Sicherheit bei KirtIS
Faktor Mensch

- Viele Sicherheitsvorfälle werden nicht mehr durch schlechte oder unsichere Technik verursacht, sondern durch Fehler der Mitarbeiter.
- Krankenhäuser zählen zu den kritischen Infrastrukturen (KritIS), die eines besonderen Schutzes bedürfen (ähnlich: Energie- und Wasserversorgung, Polizei, Telekommunikationsnetze,...)
- Schulung ist wichtig – muss aber passgenau sein, um auch ernst genommen zu werden.
- Idee: Pentesting, das Fehler der Mitarbeiter aufdeckt zwecks Vorbereitung einer zielgerichteten Schulung.

- Frage: Was ist bei so einem Vorhaben zu berücksichtigen?

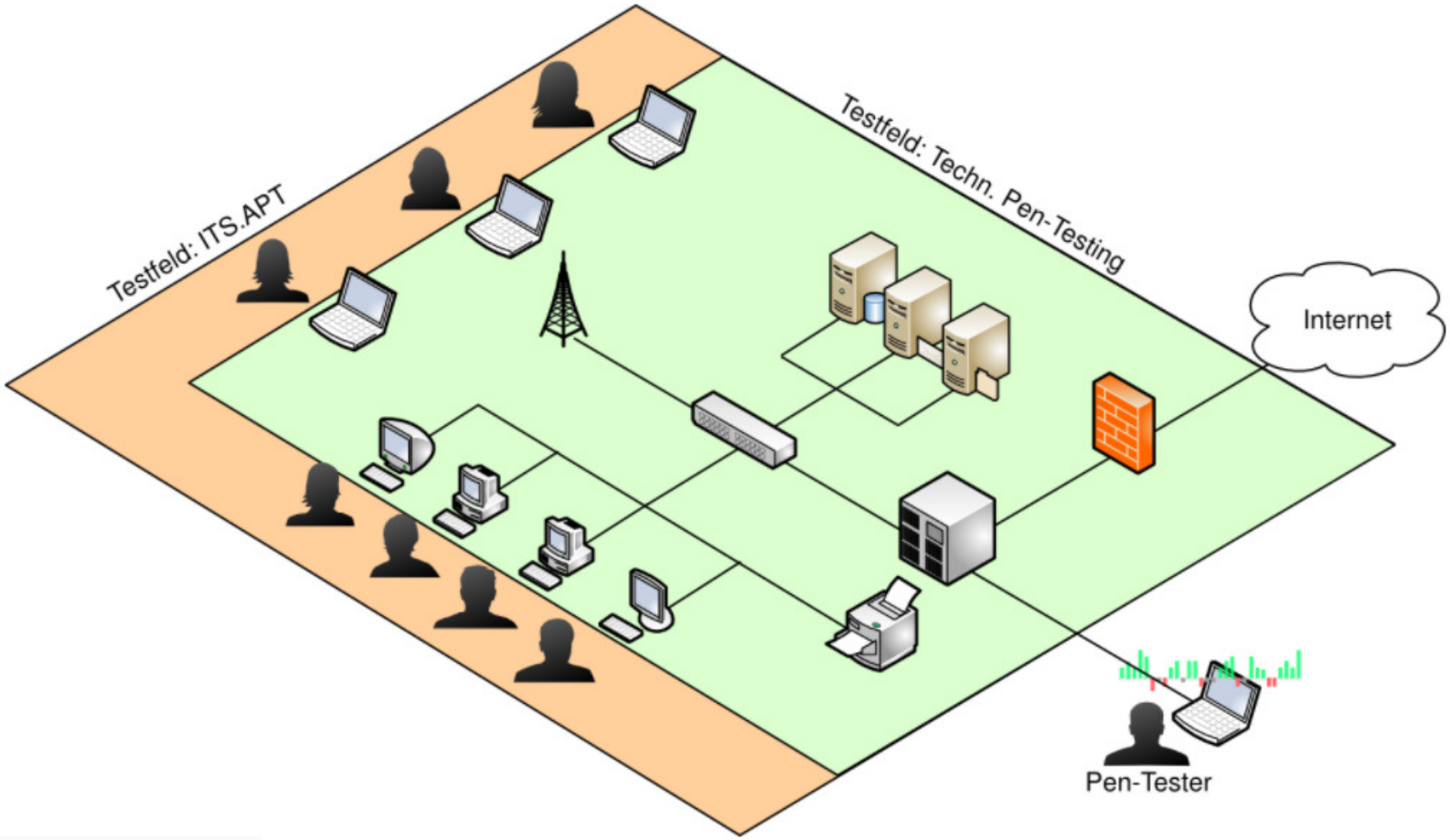
ITS APT

IT-Sicherheit bei KirtIS
Faktor Mensch

- Frage: Was ist bei Pentesting mit Zielrichtung Mitarbeiter zu berücksichtigen?
  - Mitarbeiterdatenschutz: Das Pentesting erhebt Beschäftigtendaten.
  - Schutz vor arbeitsrechtlichen Maßnahmen nötig
  - Schutz vor strafrechtlichen Folgen – so scheidet z.B. aus, Beschäftigte aufzufordern, „mal eben eine Akte zu senden", da dies § 203 StGB zumindest als Versuch verwirklichen könnte.
  - Patientendatenschutz: kein Zugriff auf Patientendaten für Pentester
  - Patientensicherheit: Kein Test am laufenden System mit Patientendaten. Lösung: ITS.APT hat Test zunächst in Verwaltung durchgeführt.
  - Reaktionen der Betroffenen antizipieren (Stecker ziehen)
  - Geeignete Artefakte entwickeln und an Einsatzort anpassen
  - Helpdesk frühzeitig einbeziehen
  - Geeignetes Testfeld auswählen.

Sonderfrage Rechtsgrundlage (übernächste Folie)

IT-Sicherheit bei KirtIS
Faktor Mensch



ITS APT

IT-Sicherheit bei KirtIS
Faktor Mensch

- Sonderfrage Rechtsgrundlage
  - Eine Einwilligung aller Mitarbeiter scheidet aus – a) praktisch und b) weil dann alle informiert sind.
  - Gesetzliche Grundlage wäre wünschenswert und wurde angeregt.
  - Es bleibt eine Betriebs- oder Personalvereinbarung als RGL
    - Art. 88 DSGVO erlaubt Mitgliedstaaten Kollektivvereinbarungen als RGL zuzulassen.
    - § 26 IV BDSG-neu setzt das um
    - § 15 LDSG-SH-Entwurf (ggf. zu eng gefasst)
    - Betriebs- und Personalräte sollten sich die erforderlichen Garantien bei der Datensicherheit geben lass. Die Vereinbarung muss sicherstellen, dass auf Basis des Tests keine arbeitsrechtlichen Maßnahmen ergriffen werden.
    - Artefakte müssen der Art nach beschrieben sein. PR/BR sollte die konkreten Entwürfe auch vorab zur Kenntnis und Stellungnahme erhalten.
  - Personal- und Betriebsräte sollten mit Blick auf die Wichtigkeit wohlwollend prüfen aber auch auf klaren Schutz der Mitarbeiter bestehen.

Weitere Informationen (finale Projektergebnisse ab Sommer 2018):
https://itsec.cs.uni-bonn.de/itsapt/

https://itsec.cs.uni-bonn.de/itsapt/

ITS APT

Fragen? Andernfalls:
Viel Erfolg bei der Klausur

Kontakt:
Harald Zwingelberg
hzwingelberg@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1284

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein