gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

35. Sitzung der AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

09. Oktober 2017, 10:30 - 15:00 Uhr

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Tagesordnung

1. Formalia
   - Begrüßung
   - Verabschiedung Tagesordnung
   - Verabschiedung Protokoll der letzten Sitzung vom 25.04.2017
2. Ehrenmitgliedschaft von Prof. Blobel und Prof. Pommerening
3. Aktuelle Ausarbeitungen unserer AG
   - Ergebnis IT-Sicherheitskonzept
   - Ausarbeitung Datenschutz-Folgenabschätzung
   - Art. 32 – Sicherheit der Verarbeitung
   - Workshop DS-GVO
4. Aktuelle Gesetzeslage
   - Änderungen im Sozialdatenschutz
   - Änderung § 203 StGB
5. TOMs unter der DS-GVO: Wie sehen zukünftig Checklisten aus?
6. Privacy by Design/Default
7. Fernwartung und Datenschutz
   - Evtl. Thema für eine Ausarbeitung unserer AG?
8. Leitung der AG
9. Treffen der AG 2018
   - conhIT 2018
   - Herbst/Winter - Wann? Wo?
     GMDS Jahrestagung: 02.-06. September 2018, Osnabrück
10. Verschiedenes
    - Künftige Aktivitäten der AG
    - Internetauftritt der AG
    - Mailingliste

Tagesordnungspunkt 2

- 1955 konstituierte sich GMDS: Gründung des Ausschusses für „Dokumentation in der Medizin“ in der DGD
  - 1957: Beginn mit der Einrichtung von Arbeitskreisen und Arbeitsgruppen
  - 1966: Umbenennung in „Deutsche Gesellschaft für Medizinische Dokumentation und Statistik in der DGD e. V.“ (GMD)
  - 1970: GMDS, um eine Verwechslung mit der „Gesellschaft für Mathematik und Datenverarbeitung“ (GMD) zu vermeiden
- 1970: Hessen verabschiedet das weltweit erste Datenschutzgesetz
- 1974: USA führen Privacy Act ein
- 1976: GMDS benennt sich in „Deutsche Gesellschaft für Medizinische Dokumentation, *Informatik* und Statistik e. V.“ (GMDS) um
- 1977: Bundesdatenschutzgesetz verabschiedet
- 1981: Alle Bundesländer (BRD) haben ein Landesdatenschutzgesetz
- 1983: Volkszählungsurteil etabliert das „Recht auf informationelle Selbstbestimmung“
- 1991: „Ulmer Urteil“ bzgl. der Grundsätze, die den Beruf des Datenschutzbeauftragten ausmachen

Tagesordnungspunkt 2

DER SPIEGEL 48/1993

Datenschutz

In Brüssel verwässert

Besorgt registrieren deutsche Datenschützer eine Wende der Bonner Politik in Brüssel. In der Vergangenheit hatte sich die Bundesregierung darum bemüht, das deutsche Recht soweit wie möglich auch auf europäische Ebene zu übertragen. Seit neuestem, kritisiert Berlins Datenschutzbeauftragter Hansjürgen Garstka, schlage sich Bonn aber immer öfter auf die Seite Dänemarks, Großbritanniens und Irlands, die von der "informationellen Selbstbestimmung" (Bundesverfassungsgericht) wenig halten. Dank dem Zusammenwirken der "Viererbande" (Garstka) sei der in Teilen selbst für die Bundesrepublik vorbildliche erste Entwurf einer europäischen Datenschutz-Richtlinie inzwischen "verwässert" worden. Zudem falle die überarbeitete Fassung in zwei Punkten nun auch hinter deutsches Recht zurück: Gestrichen wurden Regelungen über die gemeinsame Datenerhebung (etwa: Nach welchen Daten darf der Arbeitgeber den Arbeitnehmer fragen?); auch für öffentliche Sicherheit, Finanzen und Justiz soll die gemeinsame Datenschutz-Richtlinie nicht gelten, obwohl der Maastrichter Vertrag genau diese Bereiche zu Aufgaben der Europäischen Union gemacht hat.

Tagesordnungspunkt 2

- 1955 konstituierte sich GMDS
- 1970: Hessen verabschiedet das weltweit erste Datenschutzgesetz
- 1974: USA führen Privacy Act ein
- 1977: Bundesdatenschutzgesetz verabschiedet
- 1981: Alle Bundesländer (BRD) haben ein Landesdatenschutzgesetz
- 1983: Volkszählungsurteil etabliert das „Recht auf informationelle Selbstbestimmung“
- 1991: „Ulmer Urteil“ bzgl. der Grundsätze, die den Beruf des Datenschutzbeauftragten ausmachen
- 1993: 38. Jahrestagung der GMDS
  - Gründung der Datenschutz-AG

Tagesordnungspunkt 2

TOP 5. Festlegung von Arbeitsschwerpunkten

Als Arbeitsschwerpunkte werden benannt:

A. Erstellung eines Datenschutzkonzepts für Klinikinformationssysteme

- Formulierung der Datenschutzanforderungen
- Definition einer modellhaften Zugriffsmatrix
- Sicherheitskriterien: Definition von zu beachtenden Gefährdungen und nötigen Sicherheitsstufen aus den Anforderungen des Datenschutzes
- Empfehlungen zur technischen Absicherung des Datenschutzes in Krankenhäusern
- Definition, evtl. Bereitstellung der kryptographischen Infrastruktur
- Konzept zur Trennung von Forschung und Patientenversorgung, insbesondere in Universitätskliniken

B. Umsetzung des Datenschutzkonzeptes

- Durchführung von Modellprojekten, Referenzinstallationen
- Fachliche Beratung zu Datenschutz-Technologien und organisatorischen Fragen

Nicht explizit behandelt werden sollen die Themen Viren, vertrauenswürdige Software-Erstellung, Erstellung fehlerfreier Software, Krankenversicherten-Karte.

TOP 6. Themen für die nächste Sitzung

Tagesordnungspunkt 2

- 1955 konstituierte sich GMDS
- 1970: Hessen verabschiedet das weltweit erste Datenschutzgesetz
- 1974: USA führen Privacy Act ein
- 1977: Bundesdatenschutzgesetz verabschiedet
- 1981: Alle Bundesländer (BRD) haben ein Landesdatenschutzgesetz
- 1983: Volkszählungsurteil etabliert das „Recht auf informationelle Selbstbestimmung“
- 1991: „Ulmer Urteil“ bzgl. der Grundsätze, die den Beruf des Datenschutzbeauftragten ausmachen
- 1993: 38. Jahrestagung der GMDS
  - Gründung der Datenschutz-AG
- 1994: Grundsatzerklärung der AG
  Allgemeine Grundsätze für den Datenschutz in Krankenhausinformationssystemen (bis heute unverändert gültig)
- 1995: Verabschiedung der europäischen Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- 1996: Gründung Arbeitskreis „Gesundheits- und Sozialwesen“ der GDD
- 1997: Datenschutz verhindert Forschung

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Tagesordnungspunkt 2

Die Auswirkungen der Europäischen Datenschutzrichtlinie auf die Forschung in Deutschland

Rechtsanwalt Dr. Thomas Mayen, Fachanwalt fürVerwaltungsrecht, Bonn

Das Europäische Parlament und der Rat der Europäischen Union haben am 24. 7. 1995 die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erlassen. Die Richtlinie ist von den Mitgliedstaaten innerhalb von drei Jahren nach ihrer Annahme in innerstaatliches Recht umzusetzen. Der nachstehende Beitrag untersucht die möglichen Auswirkungen der neuen Richtlinie speziell auf die Forschung in Deutschland. Anders als die deutschen Datenschutzgesetze sieht die Richtlinie keine speziellen Forschungsklauseln vor, sondern nur punktuelle Sonderregelungen. Speziell für sog. sensible Daten enthält die Richtlinie in Art. 8 eine sehr strikte Regelung, ohne hiervon für die Forschung - anders als für andere Bereiche - Ausnahmen vorzusehen. Ergeben sich hierdurch neue zusätzliche Forschungsbehinderungen?

IV. Schlußbemerkung

Schon die bestehenden Datenschutzgesetze in Deutschland enthalten wichtige und weitreichende Beschränkungen zu Lasten der wissenschaftlichen Forschung. Diese Beschränkungen erschweren nicht nur die Arbeit der wissenschaftlichen Forschung, sondern machen wegen der Unbestimmtheit und Rechtsunsicherheit der einzelnen Klauseln eine Zusammenarbeit zwischen Forschung und Datenschutzbehörden im Einzelfall notwendig. Diese Anforderungen werden durch die neue Europäische Datenschutzrichtlinie nicht vermindert, sondern in einigen Punkten eher noch verschärft. Dies gilt für die Anforderungen an die Zulässigkeit der Datenerhebung, den Schutz sensitiver Daten, die Anforderungen an die Anonymisierung. An anderen Stellen werden Unbestimmtheiten und hiermit verbundene Rechtsunsicherheiten vergrößert, die sich in der Praxis häufig ebenfalls als Forschungsbehinderung auswirken bzw. diese ermöglichen. Positiv hervorzuheben ist

Tagesordnungspunkt 2

- 1955 konstituierte sich GMDS
- 1970: Hessen verabschiedet das weltweit erste Datenschutzgesetz
- 1974: USA führen Privacy Act ein
- 1977: Bundesdatenschutzgesetz verabschiedet
- 1981: Alle Bundesländer (BRD) haben ein Landesdatenschutzgesetz
- 1983: Volkszählungsurteil etabliert das „Recht auf informationelle Selbstbestimmung“
- 1991: „Ulmer Urteil“ bzgl. der Grundsätze, die den Beruf des Datenschutzbeauftragten ausmachen
- 1993: 38. Jahrestagung der GMDS
  - Gründung der Datenschutz-AG
- 1994: Grundsatzerklärung der AG
  Allgemeine Grundsätze für den Datenschutz in Krankenhausinformationssystemen
  (bis heute unverändert gültig)
- 1995: Verabschiedung der europäischen Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- 1996: Gründung Arbeitskreis „Gesundheits- und Sozialwesen“ der GDD
- 1997: Datenschutz verhindert Forschung
- 1998: GMDS-AG
  - „Sicherheitsempfehlungen zu Modem-Verbindungen im Krankenhaus“
- 1999: GMDS-AG
  - „Formulierungshilfen für einen Fernwartungsvertrag aus der Sicht des Datenschutzes“
- 2001: GMDS- AG
  - „Sicherheitsempfehlungen zum Internet-Anschluß von Krankenhäusern und Gesundheitsnetzen“,
  - „Sicherheitsempfehlungen zum Betrieb von Servern und lokalen Netzen in Krankenhäusern“,
  - „Bemerkungen zur Nutzung von E-Mail im Gesundheitswesen“

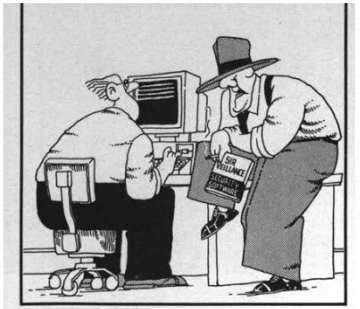
Tagesordnungspunkt 2

Anekdote am Rande: ein Informatik-Student wurde 1999 von seinem Professor dazu verdonnert, etwas über das etwas obskure Thema „Datenschutz“ zu referieren

Sicherheit

auf der

Daten-Autobahn?



»Das Sicherheitsprogramm reagiert in drei Fällen: bei einem falschen Paßwort, bei einem inkorrekten Dateiwunsch und manchmal auch schon bei dem dumpfen Gefühl, daß Sie vielleicht auch nur so ein mieser Sausack sind, der gesicherte Daten klauen will.«

Eine Quelle:

	Landeshaus 24105 Kiel Tel.: 0431/988-0	Landeshaus 24105 Kiel Tel.: 0431/988-0
Thüringen	Innenministerium des Landes Thüringen Steigerstr. 24 99096 Erfurt Tel.: 0361/37900	Thüringer Landesverwaltungsamt Carl-August-Allee 2a 99423 Weimar Postfach 2 49 99403 Weimar Tel.: 03643/585

7.3 Zugriff auf Patientendaten im Krankenhaus

(Erarbeitet von der GMDS-Arbeitsgruppe, *Datenschutz in Gesundheitsinformationssystemen*, Stand 21.4.1999)

Tagesordnungspunkt 2:
Ehrenmitgliedschaft von Prof. Blobel und Prof. Pommerening

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Nicht nur für ein gelungenes Referat:

Danke für die AG!

Tagesordnungspunkt 3:
Aktuelle Ausarbeitungen unserer AG

- Sicherheitskonzept
  - Finalisierung erfolgte am 22.09.2017
  - Veröffentlichung erfolgt nach Freigabe durch Verbände
    - Freigabe GMDS, ZTG liegt vor
    - Freigabe bvitg ist noch offen
- Ausarbeitung Datenschutz-Folgenabschätzung
  - Zusammenarbeit: DKG, bvitg unsere AG
  - Zwei Papiere erstellt
    - Praxishilfe/Interpretationshilfe
    - Beispiele für DSFA (KIS, Krebsregister, Personaldaten)
  - Papiere zur Kommentierung an AK Gesundheitswesen/Soziales der Aufsichtsbehörden gemailt
- Umgang mit Art.32 DS-GVO, d.h. Sicherheit der Verarbeitung
  - Gemeinsam mit bvitg, DKG Veröffentlichung geplant
    - „Das Krankenhaus“: Zielgruppe Krankenhaus-Verwaltung
    - MDI: Zielgruppe IT-Leiter/innen
  - Interpretationshilfe zu Art. 32 bei Bedarf
    - Meinung unserer AG?
- Workshop DS-GVO 26./27.10.2017
  - > 40 Anmeldungen bei 40 zur Verfügung stehenden Plätzen

Tagesordnungspunkt 4:
Aktuelle Gesetzeslage

- Änderungen im Sozialdatenschutz

Tagesordnungspunkt 4:
Aktuelle Gesetzeslage

- Änderungen im Sozialdatenschutz
- Omnibusverfahren
- Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften
  (BGBl 2017, S. 2541*, Inkrafttreten zum 25.05.2018)
- Öffentliche Anhörung 29.05.2017**

* http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2541.pdf
** Unterlagen der Anhörung: http://www.bundestag.de/ausschuesse18/a11/anhoerungen/119-sitzung-bundesversorgungsgesetz/507328

Tagesordnungspunkt 4:
Aktuelle Gesetzeslage: § 35 SGB I

- Abs. 1
  - Legaldefinition Sozialdaten entsprechend DS-GVO angepasst
- Abs. 2
  - Sozialdatenschutz ist abschließend in Sozialgesetzbüchern geregelt
  - Lex specialis gegenüber anderen deutschen Normen
  - EU-Recht bleibt vorrangiges Recht, wenn dieses unmittelbar anzuwenden ist
- Abs. 2a (Neu)
  - Gesetzliche Geheimhaltungspflichten sowie Berufs- oder besondere Amtsgeheimnisse (also insb. § 203 StGB) bleiben unberührt
  - ➔ SGB keine Erlaubnisnorm im Sinne § 203 SGB
- Abs. 4
  - Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich
- Abs. 6, 7
  - Regelungen § 35 Abs. 1-5 SGB I gilt auch für Auftragsverarbeiter

Tagesordnungspunkt 4:
Aktuelle Gesetzeslage: SGB X

- § 67 Begriffsbestimmungen
  - Entsprechend DS-GVO überarbeitet
  - Begriffe wie „übermitteln“, „anonymisieren“ nicht länger definiert
  - ➔ Anonyme Nutzung z. T. in SGB erlaubt, aber jetzt unklar, was als „anonym“ i.S.d. SGB anzusehen ist
- § 67a
  - Abs. 1: Zulässigkeit der Verarbeitung = Kenntnis der Daten ist zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem SGB erforderlich
  - Abs. 2: Ersterhebung von Sozialdaten beibehalten; Dritterhebung nur unter den in §67a Abs. 2 SGB X genannten Voraussetzungen
- § 67b (Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten)
  - Im Prinzip unverändert
  - Einwilligung: schriftlich oder elektronisch
- § 67c (Zweckbindung sowie Speicherung, Veränderung und Nutzung von Sozialdaten zu anderen Zwecken)
  - Im Prinzip unverändert

Tagesordnungspunkt 4:
Aktuelle Gesetzeslage: SGB X

- §§ 67d bis 78: diverse Übermittlungsbefugnisse
  - § 67d: Übermittlungsgrundsätze
  - § 69: Übermittlung für die Erfüllung sozialer Aufgaben
  - § 70: Übermittlung für die Durchführung des Arbeitsschutzes
  - § 75: Übermittlung von Sozialdaten für die Forschung und Planung
  - §76: Einschränkung Übermittlungsbefugnisse bei besonders schutzwürdigen Sozialdaten (in § 203 Abs. 1, 3 StGB genannte Personen;
    → Hinweis: Abs. 3 fällt demnächst ersatzlos weg, in Kommentierung wurde Ministerium zwar darauf hingewiesen, aber die „Zeitnot“)
- §80: Auftragsverarbeitung
  - An DS-GVO angepasst, aber Anzeigepflicht bleibt erhalten
  - Auftragsverarbeitung unter Vorgaben von Abs. 3 erlaubt
    (Vermeidung Störungen im Betriebsablauf oder Auftragsverarbeiter ist erheblich kostengünstiger)
  - Beschränkung von Abs. 3 gilt nicht für die Beauftragung bzgl. Prüfung oder Wartung automatisierter Verfahren
  - Auftragsverarbeitung künftig weltweit möglich
    - ➢ Allerdings Beschränkung auf Angemessenheitsbeschluss gemäß Art. 45 DS-GVO

Tagesordnungspunkt 4:
Aktuelle Gesetzeslage: SGB X

- §§ 81a – c
  - Gerichtlicher Rechtsschutz
- §§ 82, 82a
  - Beschränkung der aus Artt. 13,14 DS-GVO resultierenden Informationspflichten
- § 83
  - Beschränkung der aus Art. 15DS-GVO resultierenden Auskunftsrecht
- § 83a
  - Beschränkung der aus Artt. 33, 34 DS-GVO resultierenden Informationspflichten bzgl. Verletzung des Schutzes von Sozialdaten
- § 84
  - Beschränkung der aus Artt. 16, 17, 18, 19, 21 resultierenden Rechte bzgl. Löschung, Berichtigung, Widerspruch, Sperrung
- §§ 85, 85a
  - Sanktionen: Strafvorschriften/Bußgelder analog BDSG-neu
  - §85a Abs. 3: „Gegen Behörden und sonstige öffentliche Stellen werden keine Geldbußen verhängt“

Tagesordnungspunkt 4:
Aktuelle Gesetzeslage

- Änderungen im Sozialdatenschutz
- §203 StGB

Anpassung § 203 StGB*
Timeline

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Änderung im Bundestag am 01.09.2017 beschlossen
- Bundesrat beschloss am 22.09.2017 keinen Ausschuss einzuberufen

➔ Gesetz faktisch „durch“, fehlt
  - Unterschrift Präsident
  - Veröffentlichung im Bundesgesetzblatt

- Änderung in §203 StGB
  - § 203 Abs. 1,2 unverändert
  - → § 203 Abs. 3: Neu
  - → § 203 Abs. 4: Neu
  - § 203 Abs. 5 (ehemals Abs. 4)
  - § 203 Abs. 6 (ehemals Abs. 5)
- Begleitend: Änderung §§ 53a, 97 StPO

* Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen http://dip21.bundestag.de/dip21.web/searchDocuments/documentData_detail_vo.do bzw. https://www.bmjv.de/SharedDocs/

Neu: § 203 Abs. 3

(3) **Kein Offenbaren** im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen **berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen** zugänglich machen. 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.

- ➔ Schweigepflicht wird auf externe **Dienstleister** erweitert
- ➔ Beinhaltet Auftragsverarbeiter und Unter-Auftragsverarbeiter
- ➔ **Keine Einschränkung bzgl. Tätigkeiten** durch externe Dienstleister
- ➔ Einzige Einschränkung: Dienstleister darf jedoch nur **erforderliches** Wissen offenbart werden

Schweigepflicht geändert, Strafbarkeit entsprechend Täterkreis erweitert (§203 Abs. 4)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den **Absätzen 1 und 2 genannte Person** nicht dafür Sorge getragen hat, dass eine **sonstige mitwirkende Person**, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, **zur Geheimhaltung verpflichtet wurde**; dies gilt **nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person** sind,
2. als **im Absatz 3 genannte mitwirkende Person** sich einer **weiteren mitwirkenden Person**, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, **bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde**; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

Schweigepflicht geändert, Strafbarkeit entsprechend Täterkreis erweitert (§203 Abs. 4)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- In Wartungsverträgen & Co künftig auf „Verpflichtung zur Einhaltung der Schweigepflicht des eingesetzten Personals“ durch Dienstleister achten
  - Cave: Dienstleister muss für Verpflichtung bei ggf. vorhandenen Unterauftragnehmer achten (§203 Abs. 3 Ziff. 2 StGB-neu)
- Keine „Pflicht zur Verpflichtung“, wenn Mitwirkende selbst Geheimnisträger i. S. d. §203 StGB
- Erweiterung gilt nur für „Dienstleister“ bzw. „mitwirkende Personen“
  - Für eigenständige Verarbeitung (z.B. Übermittlung in externe Patientenakte) wird auch künftig Schweigepflichtentbindung benötigt
- Hinweis:
  - in Vertrag zur Auftragsverarbeitung berücksichtigen, ggf. Ergänzungsvereinbarung treffen
  - Bei Beauftragung von Unterauftragnehmern muss Auftragnehmer für Verpflichtung „Sorge tragen“ ➔ Berücksichtigung in Unterauftragsverträgen

Änderung § 53a StPO:
Berufshelfer → „mitwirkende Personen“

§ 53a Zeugnisverweigerungsrecht der **mitwirkenden Personen**

(1) Den Berufsgeheimnisträgern nach § 53 Absatz 1 Satz 1 Nummer 1 bis 4 stehen die Personen gleich, die im Rahmen

1. eines **Vertragsverhältnisses**,
2. einer **berufsvorbereitenden Tätigkeit** oder
3. einer **sonstigen Hilfstätigkeit**

an deren beruflicher Tätigkeit mitwirken. Über die Ausübung des Rechts dieser Personen, das Zeugnis zu verweigern, entscheiden die Berufsgeheimnisträger, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann.

(2) Die Entbindung von der Verpflichtung zur Verschwiegenheit (§ 53 Absatz 2 Satz 1) gilt auch für die nach Absatz 1 mitwirkenden Personen.

* Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen
http://www.bundesrat.de/SharedDocs/TO/960/to-node.html;jsessionid=8204B3AE818C046EEAC112A04878E700.2_cid339

Änderung § 97 Abs. 2 StPO: Satz 2 aufgehoben

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

(2) Diese Beschränkungen gelten nur, wenn die Gegenstände im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten sind, es sei denn, es handelt sich um eine elektronische Gesundheitskarte im Sinne des § 291a des Fünften Buches Sozialgesetzbuch. ~~Der Beschlagnahme unterliegen auch nicht Gegenstände, auf die sich das Zeugnisverweigerungsrecht der Ärzte, Zahnärzte, Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen erstreckt, wenn sie im Gewahrsam einer Krankenanstalt oder eines Dienstleisters, der für die Genannten personenbezogene Daten erhebt, verarbeitet oder nutzt, sind, sowie Gegenstände, auf die sich das Zeugnisverweigerungsrecht der in § 53 Abs. 1 Satz 1 Nr. 3a und 3b genannten Personen erstreckt, wenn sie im Gewahrsam der in dieser Vorschrift bezeichneten Beratungsstelle sind.~~ Die Beschränkungen der Beschlagnahme gelten nicht, wenn bestimmte Tatsachen den Verdacht begründen, dass die zeugnisverweigerungsberechtigte Person an der Tat oder an einer Datenhehlerei, Begünstigung, Strafvereitelung oder Hehlerei beteiligt ist, oder wenn es sich um Gegenstände handelt, die durch eine Straftat hervorgebracht oder zur Begehung einer Straftat gebraucht oder bestimmt sind oder die aus einer Straftat herrühren.

Änderung § 97 Abs. 3,4 StPO: An §53a StPO angepasst

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

(3) Die Absätze 1 und 2 sind entsprechend anzuwenden, soweit ~~die Hilfspersonen (§ 53a) der in § 53 Abs. 1 Satz 1 Nr. 1 bis 3b Genannten~~ **die Personen, die nach § 53a Absatz 1 Satz 1 an der beruflichen Tätigkeit der in § 53 Absatz 1 Satz 1 Nummer 1 bis 3b genannten Personen** mitwirken, das Zeugnis verweigern dürfen.

(4) […] Dieser Beschlagnahmeschutz erstreckt sich auch auf Gegenstände, die von den in § 53 Abs. 1 Satz 1 Nr. 4 genannten Personen ~~ihren Hilfspersonen (§ 53a)~~ **den an ihrer Berufstätigkeit nach § 53a Absatz 1 Satz 1 mitwirkenden Personen** anvertraut sind. Satz 1 gilt entsprechend, soweit die ~~Hilfspersonen (§ 53a) der in § 53 Abs. 1 Satz 1 Nr. 4 genannten Personen~~ Personen, **die nach § 53a Absatz 1 Satz 1 an der beruflichen Tätigkeit der in § 53 Absatz 1 Satz 1 Nummer 4 genannten Personen mitwirken** das Zeugnis verweigern dürften.

Schweigepflicht geändert, Schweigerecht und Beschlagnahmeverbot entsprechend angepasst

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Schweigerecht für „mitwirkende Personen“ entsprechend Änderungen § 203 StGB angepasst
- Beschlagnahmeverbot entsprechend §203 StGB und §53a StPO gestaltet
- Schweigepflicht, Schweigerecht, Beschlagnahmeverbot gilt für Dienstleister
- Schweigepflicht, Schweigerecht, Beschlagnahmeverbot gilt ggf. nicht für Speicherung in externen Patientenakten (pEPA, ePA, usw.)
  - Bei externer Patientenakte i.d.R. keine „Mitwirkenden“ im Sinne des § 203 StGB vorhanden

  ➔ Dann auch kein Schweigerecht entsprechend § 53a StPO

  ➔ Dann auch kein Beschlagnahmeverbot gemäß § 97 StPO

Tagesordnungspunkt 5:
TOMs unter der DS-GVO: Wie sehen zukünftig Checklisten aus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Separate Folien

Tagesordnungspunkt 6:
Privacy by Design/Default

- Separate Folien

Tagesordnungspunkt 7:
Fernwartung und Datenschutz

- Separate Folien

Tagesordnungspunkt 8:
Leitung der AG

- Dr. Schwanke steht aus beruflichen Gründen nicht mehr als stellvertretende Leitung zur Verfügung
- Daher Neuwahl beim nächsten Treffen
- Wahl als Nachfolger
  - Herr Thorsten Schütz
    - Leiter IT und Betriebsorganisation Klinikum Itzehoe
    - Beisitzer im Vorstand Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter KH-IT e. V.
    - Mitglied im Branchenarbeitskreis „Medizinische Versorgung“ von UP KRITIS
  - Weitere Kandidaten?

Tagesordnungspunkt 9: Treffen der AG 2018

- Frühjahrstreffen
  - conhIT 2018
  - 17. bis 19. April 2018
  - Messe Berlin
- Herbsttreffen
  - Möglichkeit 1:
    - GMDS Jahrestagung: 02.-06. September 2018, Osnabrück
    - Kosten: Tageskarte GMDS-Mitglieder ~150 Euro, Nicht-Mitglieder ~ 210 Euro
  - Möglichkeit 2:
    - Unabhängig von Jahrestagung
    - Vorschlag Termin
      - 39. KW (24.-28.09.2018)
      - 40. KW (01.-05.10.2018)
      - 41. KW (08.-12.10.2018)
    - Vorschlag Ort
      - Berlin
      - Düsseldorf
      - ???

Tagesordnungspunkt 10: Verschiedenes

- Künftige Aktivitäten der AG
  - Art. 32 und Sicherheit der Verarbeitung
  - Fernwartung
  - Privacy by Design/Default
  - TOM
  - Löschen
  - …?

Tagesordnungspunkt 10:
Verschiedenes: Löschen und DS-GVO

- Art. 17 DS-GVO: betroffene Person kann von Verantwortlichen Löschung verlangen; Einschränkungen
  - Ausübung des Rechts auf freie Meinungsäußerung und Information
  - Erfüllung einer rechtlichen Verpflichtung
  - Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt
  - Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde
  - Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
  - Für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke
  - Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
  - ➔ Keine Einschränkung der Verarbeitung statt Löschung
  - ➔ Aber: Nur auf Aufforderung der betroffenen Person

Tagesordnungspunkt 10:
Verschiedenes: Löschen und DS-GVO

- Art. 5 Abs. 1 lit. b DS-GVO

  Personenbezogene Daten müssen

  – „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden […]“
  – Nach Zweckerreichung keine weitere Verarbeitung
  – „Speichern“ ist Verarbeitung i.S.d. DS-GVO

- Art. 5 Abs. 1 lit. e DS-GVO

  Personenbezogene Daten müssen

  – „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist […]“
  – Ohne Identifikationsmöglichkeit = Anonyme Daten = keine personenbezogene Daten

➔ Art. 5 fordert Löschen der Daten

Tagesordnungspunkt 10:
Verschiedenes: Löschen und DS-GVO

Problem hierbei:

- Patientendaten sind nicht in einem Informationssystem gespeichert, sondern in mehreren, z.B.
  - Krankenhaus-Informationssystem (KIS)
  - Labor-Informationssystem (LIS)
  - Onkologisches Informationssystem (OIS)
  - Picture Archiving and Communication System (PACS)
  - Radiologie-Informations-System (RIS)
- Patientendaten benötigen oftmals den Kontext aus anderen Informationssystemen. Z. B.
  - Rechtfertigende Indikation zur Röntgenuntersuchung (§ 23 RöV) basiert auf Informationen des KIS
  - Werden Daten aus KIS gelöscht, ist ggf. Richtigkeit der rechtfertigenden Indikation nicht länger überprüfbar
- Bei Weitergabe an Externe: diese müssen über Löschung informiert werden (Art. 19 DS-GVO)
  - Weiß man zum Löschzeitpunkt noch, an welche externen Personen man die Daten weitergab?

Tagesordnungspunkt 10:
Verschiedenes: Löschen und DS-GVO

- Gesetzliche Speicherdauern nicht einheitlich geregelt, z. B.
  - Patientenakte: 10 Jahre nach Abschluss Behandlung, soweit keine anderen Vorschriften (§630 f Abs. 3 BGB)
  - Berufsgenossenschaftliche Verletzungsverfahren: 15 Jahre (Ziff. 3.6.8 VAV i. V. m. § 33 SGB VII)
  - Nosokomiale Infektionen: 10 Jahre (§ 23 Abs. 4 IfSG)
  - Röntgenbehandlung: 30 Jahre (§ 28 Abs. 3 RöV)
  - Röntgenbilder, Aufzeichnungen: 10 Jahre (§ 28 Abs. 3 RöV)
  - Angaben zur rechtfertigenden Indikation: 10 Jahre (§ 85 Abs. 3 StrlSchV)
  - Angaben zur Blut-Spenderdokumentation, Rückverfolgbarkeit: 30 Jahre (§11 Abs. 1 S. 2 TFG)
  - Immunisierungsprotokolle: 20 Jahre (§8 Abs. 3 i. V. m. § 11 Abs. 1 TFG)
  - …

Tagesordnungspunkt 10:
Verschiedenes: Löschen und DS-GVO

- Heterogene Zeiten erschweren Löschung von Patientendaten, da diese oftmals nur im Kontext interpretierbar sind
- Häufig unterbreiteter Vorschlag: aus Haftungsgründen 30 Jahre aufbewahren
- Haftungsfristen
  - Regelmäßige Verjährungsfrist: 3 Jahre (§ 195 BGB)
    Beginn der Zeitrechnung: Person erlangte Kenntnis oder hätte Kenntnis ohne grobe Fahrlässigkeit erlangen müssen
  - Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, verjähren ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grob fahrlässige Unkenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an (§ 199 BGB)
  - Nach 30 Jahren: alles verjährt (§ 197 BGB)
- Aber: Aufbewahrung nur mit legitimen Grund ➔ Risiko für Haftungsfall muss nachgewiesen werden, d.h. Risikoabwägung bzgl. Aufbewahrung erforderlich

Tagesordnungspunkt 10:
Verschiedenes: Löschen und DS-GVO

- EU DS-GVO: Art. 83 Abs. 5 lit a bzw. Art. 83 Abs. 5 lit. b
  - Bußgeld bis zu 20.000.000 Euro

→ Evtl. Neubewertung des Risikos erforderlich

→ Evtl. auf Grund Vorsichtsprinzip (§ 252 Abs. 1 Nr. 4 HGB i. V. m. § 253 Abs. 1 S.4 HGB) in Bilanzierung zu berücksichtigen?

- Lukas Mempel erarbeitet Vorlage zur Erarbeitung des Themas

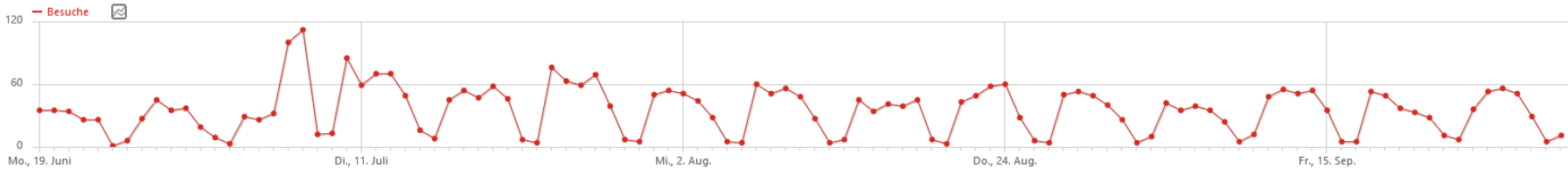
Tagesordnungspunkt 10:
Verschiedenes

- Künftige Aktivitäten der AG
  - TOM
  - Löschen
  - Privacy by Design/Default
  - Fernwartung
  - Art. 32 und Sicherheit der Verarbeitung
  - …?
- Internetauftritt der AG
  - Alle AGs sollen auf GMDS-Homepage umziehen
  - Homepage unsere AG: https://gmds.de/aktivitaeten/medizinische-informatik/arbeitsgruppenseiten/datenschutz-und-it-sicherheit-im-gesundheitswesen-dig/
  - Es kann nur eine Teilmenge an Daten mitgenommen werden
  - Übertragung muss „von Hand“ erfolgen
  - Geplant: Ende Umzug bis Ende 2017
  - ➔ Mit Abfall Besuchszahlen muss gerechnet werden

Tagesordnungspunkt 10:
Verschiedenes

- Internetauftritt: Portal zur DS-GVO : http://ds-gvo.gesundheitsdatenschutz.org/
- Aktiv seit Mitte Juni 2017, durchschnittlich ~60 Besuche pro Tag

Graph der letzten Besuche



- Besucher überwiegend aus Deutschland

Tagesordnungspunkt 10:
Verschiedenes

- Künftige Aktivitäten der AG
  - Art. 32 und Sicherheit der Verarbeitung
  - Fernwartung
  - Privacy by Design/Default
  - TOM
  - Löschen
  - …?
- Internetauftritt der AG
  - Alle AGs sollen auf GMDS-Homepage umziehen
  - Homepage unsere AG: https://gmds.de/aktivitaeten/medizinische-informatik/arbeitsgruppenseiten/datenschutz-und-it-sicherheit-im-gesundheitswesen-dig/
  - Es kann nur eine Teilmenge an Daten mitgenommen werden
  - Übertragung muss „von Hand“ erfolgen
  - Geplant: Ende Umzug bis Ende 2017
  - ➔ Mit Abfall Besuchszahlen muss gerechnet werden
- Mailingliste
  - Mailingliste wird ebenfalls umziehen (voraussichtlich 42. KW)
  - Keine offene Mailingliste mehr, d. h. nur AG-Mitglieder sind in Mailingliste enthalten
  - Aktuelle AG-Mitglieder werden bzgl. Umzug angemailt („OptIn“)