PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

16. Frühjahrstagung AG Medizinrecht

Thema:
Datenschutzrechtliche Fragen von IT im Gesundheitswesen, u.a. E-Health-Gesetz

Referent:
Dr. Ole Ziegler
Fachanwalt für Medizinrecht
Fachanwalt für Handels- und Gesellschaftsrecht
Mediator

Hamburg, den 15.04.2016

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Übersicht

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

A. Aktuelle Anwendungsfelder

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Cyber-Attacken auf Krankenhäuser/IT-Sicherheit im Krankenhaus

- Angriff auf das Lukaskrankenhaus Neuss (DÄBl 2016, A 364 ff.; Ärztezeitung vom 12.02.2016)
- „Diagnose: Computergrippe“ (Kurz, FAZ vom 16.11.2015, Seite 14)
- „It´s way to easy to hack the hospital“ (Monte Reel/Jordan Robertson, Bloomberg Businessweek, 16.11.2015, Seite 42 ff.)
- Mayo-Clinic-Gruppe beauftragte den Hacker Billy Rios mit der Überprüfung der Sicherheitssysteme ihrer Krankenhäuser. Rios kam zu folgendem erschütterndem Ergebnis: „The only barrier is the good will of a stranger“
- „This device can save your life – or steal your identity“ (Bloomberg.com/features/2015-hospital-hack, zuletzt abgerufen am 01.04.2016)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Zugriff auf Kliniknetzwerke (Krankenhaus-Informationssysteme) und angeschlossene medizinische Geräte
- Computerviren/Trojaner zur Ausspähung
- Erpressung, d.h. durch Versperren des Zugangs zu eigenen (medizinischen) Daten durch sog. Ransomware (vgl. BSI, Ransomware, Bedrohungslage, Prävention & Reaktion, 2016)
- Manipulation der Dosierung von Infusionen
- Identitätsmissbrauch
- Derzeitiges Problem: Generische, nicht zu ändernde Passwörter; unkontrollierte Vernetzung
- „Internet der Dinge“, Entwicklung von „Security by design“
- Angesprochen sind Krankenhausbetreiber und Hersteller von medizinischen Geräten

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Krankenhausinformationssysteme

- Daten in der **Cloud**; Auftragsdatenverarbeitung
- Behandlungsdokumentation: **Ersetzendes Scannen**

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Smart Home; Ambient Assisted Living (AAL)

- Sensorbox, Quelle: Fraunhofer IPA

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Sensoren im Raum und am Körper sowie Videoüberwachung
- Sowohl im Krankenhaus, Pflegeheim als auch in der häuslichen Umgebung (Ambient Assisted Living = umgebungsunterstütztes Wohnen)
- Smart Home 2030, Studie des Gottlieb Duttweiler Institute, Schweiz, 2015
- Zukünftig ergänzt um lernfähige Sensoren, die Bewegungsmuster erfassen, um ein Sturzverhalten „im Ansatz“ zu erkennen (Projekt Cicely im Bereich der SAPV)
- Aufzeichnung von Bildern und selbständige Auswertung der Daten durch Mikroprozessoren

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

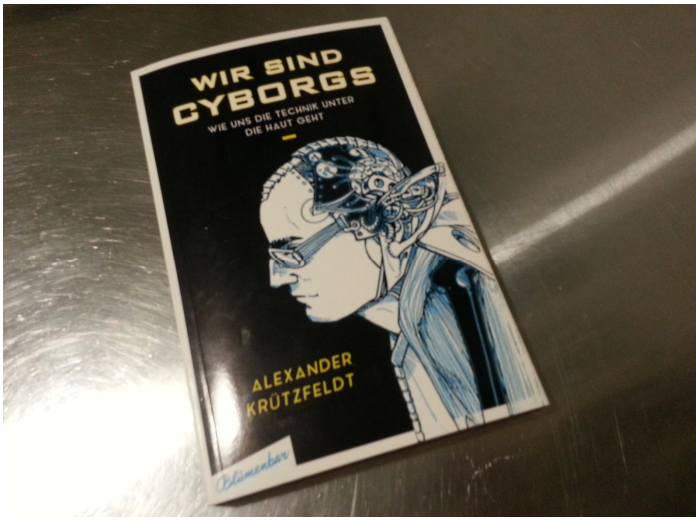
- ggf. Alarmierung des Pflegepersonals oder Dritter mittels mobiler Endgeräte
- Daten befinden sich solange im Arbeitsspeicher des Bildverarbeitungsrechners, bis sie ausgewertet wurden

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

IT-gestützte Eingriffe in das Gehirn

- Schnittstelle von Neuro- und Computerwissenschaften: Gehirn-/Maschine-Schnittstellen
- Invasiv in das Gehirn eingebrachte Stimulationselektronen, z.B. Closed Loop zur Behandlung von Traumata
- Einwirkung auf das Gedächtnis und den Schlaf: Therapeutisch induziertes „Verlernen“ von Traumata (vgl. FAZ v. 25.03.2015)
- Steuerung von Muskelgruppen durch das Gehirn, z.B. bestimmte Armbewegungen bei paraplegischen Patienten („The nerve bypass“, Süddeutsche Zeitung vom 14.04.2016)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB



PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

„Virtuelle Arztpraxis“/Geräte zur Gesundheitsversorgung

- Spezifische Apps in Smartphones
- Einbindung internetfähiger Endgeräte
- Spezielle Geräte, z.B. Fitnessarmbänder (sog. Wearables)
- Siehe Beispiele im Microsoft Trendbook 2013

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

„E-Hygiene“

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Sensor warnt vor Asthmaanfall

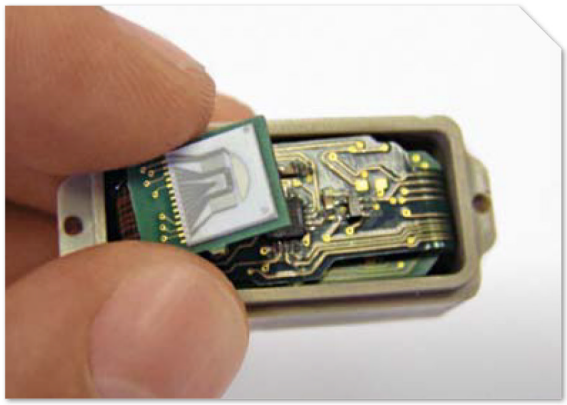
Quelle: http://www.siemens.com
Initiator: Siemens AG, Deutschland

Ingenieure der Firma Siemens haben einen **intelligenten Sensor** entwickelt, der einen bevorstehenden Asthmaanfall eines Patienten schon Stunden im Voraus erkennt. Hierzu detektiert der portable Gas-Sensor, der kaum größer als ein Handy ist, den Signalstoff Stickstoffmonoxid in der Atemluft des Patienten. Dieser Signalstoff ist das sichere Anzeichen dafür, dass sich eine Entzündung der Atemwege anbahnt, die zum Asthmaanfall führen kann. Wird dies erkannt, kann durch die Einnahme von entzündungshemmenden Medikamenten diesem bevorstehenden Anfall sicher entgegengewirkt werden.

Trendexplorer PPT Export
Send a Trend

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Implantat-Chip überwacht Tumorwachstum



Quelle: http://portal.mytum.de
Initiator: Technische Universität München (TUM), Deutschland

Medizintechniker der Technischen Universität München haben einen **implantierbaren Chip entwickelt,** der das Wachstum von Tumoren im Körper überwacht. Hierzu misst der Sensor die Konzentration an gelöstem Sauerstoff im Gewebe in Tumornähe. Sinkt der Sauerstoffgehalt in dieser Region ab, wächst der Tumor oder wird aggressiv. Die Daten werden per Funk an den behandelnden Arzt geschickt, der die Therapiemethode festlegt. Diese Überwachung ist sinnvoll, wenn eine sofortige operative Entfernung des Tumors große Risiken birgt oder bei älteren Menschen die Lebensqualität mindern würde.

Trendexplorer PPT Export
Send a Trend Weitere Bilder

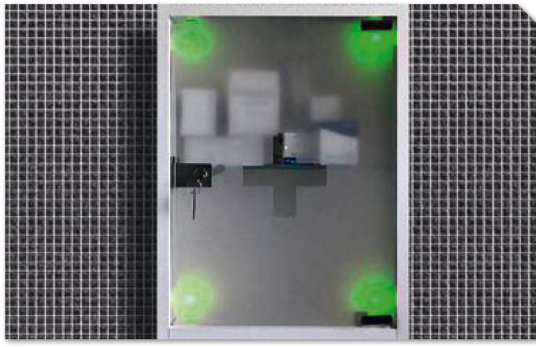
PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Arzneischrank gibt automatisch Dosis an

Quelle: http://www.ias.uni-stuttgart.de
Initiator: Universität Stuttgart, Deutschland

Forscher der Universität Stuttgart haben einen **Arzneischrank entwickelt,** der automatisch den Inhalt verwaltet und die Einnahme von Medikamenten sowie mögliche Unverträglichkeiten des Nutzers überwacht. Der Schrank enthält einen Mikrocontroller, auf dem die Patientendaten und Rezepte gesammelt werden. Über optische Signale und die Sprachausgabe erfährt der Nutzer, wann er welche Medikamente einnehmen muss und ob er sie verträgt. Davon könnten insbesondere ältere Menschen profitieren sowie alle, die mehrere Tabletten parallel einnehmen müssen.

Trendexplorer PPT Export
Send a Trend Video



PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Sensor dokumentiert Knieheilung

Quelle: http://www.fraunhofer.de
Initiator: Fraunhofer-Institut für Produktionstechnik und Automatisierung, Deutschland

Ein Forscherteam des Fraunhofer-Instituts für Produktionstechnik und Automatisierung in Stuttgart hat ein **Sensorsystem zur Überwachung der Kniegesundung** nach einem Unfall entwickelt. Hierzu ist ein Winkelmesssystem in die Kniebandage des Patienten integriert, das den Bewegungswinkel des Knies erfasst und speichert. Eine dazugehörige Software wertet diese Messungen aus, sodass der Heilungsprozess individuell erfasst und dokumentiert wird. So ermöglicht es das System, die Therapie individuell auf den jeweiligen Patienten abzustimmen und einen optimalen Verlauf der Heilung sicherzustellen.

Trendexplorer PPT Export
Send a Trend

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Telematikinfrastruktur** als Voraussetzung für eine elektronische Kommunikation von Leistungserbringern, KV, Patient (insbesondere **E-Health-Gesetz**)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

B. Rechtliche Rahmenbedingungen

- **Datenschutz-Grundverordnung (DS-GVO)**
  - Verschiedene Fassungen: Vorschlag der EU-Kommission vom 25.01.2012; Verhandlungsposition des EU-Parlaments vom 12.03.2014; Einigung der Justiz- und Innenminister im Ministerrat am 04.12.2014; Verhandlungsposition des Ministerrats vom 11.06.2015; **Ergebnis der Trilogparteien vom 15.12.2015**
  - **06.04.2016**: EU-Rat veröffentlicht **offizielle deutsche Textfassung** (http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE)
  - Derzeit technische Überarbeitung der Arbeitsfassung der Trilogparteien; Freigabe im Mai/Juni 2016 erwartet (Krüger-Brand, Deutsches Ärzteblatt 2016, A 218)
  - Inkrafttreten in Deutschland: 2 Jahre nach Inkrafttreten der DS-GVO, Art. 99 Abs. 2; voraussichtlich also Mitte 2018

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Bis zur Arbeitsfassung der Trilogparteien enthielt der Entwurf einer Datenschutzgrundverordnung mit Art. 81 eine Regelung für den **Umgang mit Gesundheitsdaten**, wonach die Mitgliedstaaten berechtigt waren, Sicherungsvorkehrungen „in den Grenzen der Verordnung“ bzw. „in Übereinstimmung mit der Verordnung“ nationalstaatlich zu regeln
  - Art. 81 ist nunmehr ersatzlos entfallen
  - Daher stellt sich die Frage, inwieweit für den Gesetzgeber gleichwohl Typisierungs- und Konkretisierungsmöglichkeiten im Gesundheitsbereich bestehen
  - DSG-VO verfolgt das Konzept der sogenannten Vollharmonisierung; dies bedeutet, dass die DSG-VO ein Mindestniveau vorgibt, nationale Normen fallen weg, soweit die DSG-VO keine Öffnungsklausel enthält

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Legaldefinition von Gesundheitsdaten in Art. 4 Nr. 15 DSG-VO
- Z.B. Gesundheitsdaten, Art. 9 Abs. 2 DSG-VO: „Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen einführen oder aufrechterhalten, soweit die Verarbeitung von (…) Gesundheitsdaten betroffen ist“ (gleichsinnig Albrecht, CR 2016, 88, 96 f.; Buchner, DuD 2016, 155, 160)
- Z.B. Vorschriften des Kapitel IX (aber: Art. 81 DSG-VO-E ist entfallen)
- Z.B. Art. 6 Abs. 2 DSG-VO und Art. 6 Abs. 3 b DSG-VO
- Bereichsspezifische Regelungen, z. B. im SGB V, bleiben daher erhalten

- Trotz dieser Spielräume einheitliche Auslegung der DSG-VO?
  - Instrument: Stellungnahmen und Orientierungshilfen des Europäischen Datenschutz-Ausschusses, Art. 68 DSG-VO
- EuGH (Urt. v. 08.04.2014 – C 293/12 und C 594/12):

  - die wesentlichen Regelungen müssen in den zentralen Vorgaben selbst angelegt sein (kritisch: Kingreen/Kühling, JZ 2015, 213, 220: „Verrechtlichungsfalle“)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- EuGH – Urt. v. 06.10.2015 (C-362/14) in Sachen **Schrems/Digital Rights Ireland** (NJW 2015, 3151):
  - Entscheidung der Kommission aus dem Jahr 2000, USA sei ein **„safe harbor“,** ist ungültig, da Kommission damals nicht feststellte, dass die USA tatsächlich ein „angemessenes Schutzniveau“ im Sinne von Art. 25 Abs. 6 der RL 95/46 gewährleistet (dazu Borges, NJW 2015, 3617 m.w.N.; Fuchs, BB 2015, 3074; Kühling/Heberlein, NJW 2016, 7)
  - Angesichts dessen stellen die USA ein „Drittland“ im Sinne von Art. 44 ff. DSG-VO (Kapitel V der DSG-VO) dar
  - Auswirkungen auf folgende beispielhafte Fallkonstellationen
    - Wartung von Krankenhausinformationssystemen durch in USA ansässige Unternehmen oder jedenfalls dort erfolgende Support-Leistungen (das ist auch eine Übermittlung lediglich zur „Ansicht“; vgl. Gemeinsame Stellungnahme zum Save Harbor-Urteil v. bvitg und GDD und GMDS, Seite 13)
    - Datenaustausch zwischen Herstellern und/oder Ärzten im Rahmen klinischer Prüfungen bzw. multinationaler Studien

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Unterschiedliche Reaktionen von Gesundheitsanbietern auf das Safe-Harbor-Urteil
  - „No-Cloud-Policy“ (Aber: Cloud ist nicht gleich Cloud)
  - IT ausschließlich im eigenen Haus
  - Bevorzugung europäischer Dienstleister
- Reaktionen in der Legislative
  - Judicial redress act in den USA (vgl. Art. 45 DSG-VO und Erwägungsgrund 81 zur DSG-VO)
  - Legislativpaket der EU-Kommission zum sog. „EU-US-Privacy Shield“ (Pressemitteilung IP/16/433 vom 29.02.2016, dazu: Grau/Granetzny, NZA 2016, 405)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Beschluss der 91. Konferenz der deutschen Datenschutzbehörden vom 06.04./07.04.2016: „Der bislang vorgelegte Entwurf (…) genügt nicht, um von einem angemessenen Datenschutzniveau (…) sprechen zu können."
- Art. 29-Arbeitsgruppe von EU-Datenschutzbehörden fordert Nachbesserungen an privacy shield (FAZ vom 14.04.2016, S. 16)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-RL)**
  - Einigung des Rats der EU und des Europaparlaments vom 29.06.2015
  - 18.12.2015: Zustimmung der Mitgliedstaaten zur Einigung
  - Annahme in EU-Ministerrat und Europaparlament bis Mitte 2016 erwartet
  - Informationsaustausch zwischen Betreibern einer sogenannten kritischen Infrastruktur und staatlichen Stellen
  - Zusammenhang mit deutschem IT-Sicherheitsgesetz vom 24.07.2015

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Nationales Verfassungsrecht: Grundgesetz**
  - Recht auf informationelle Selbstbestimmung (BVerfGE 65,1)
  - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfG NJW 2008, 822)
- **Bundes- und Landesdatenschutzgesetze**
  - Gesundheitsdaten, § 3 Abs. 9 BDSG
  - Sozialdaten, § 67 Abs. 1 SGB X
  - BSG – Urt. v. 10.12.2008 – B 6 KA 37/07 R: Scharf verstandener Gesetzesvorbehalt im Bereich der Sozialverwaltung sowie des SGB V, daher Notwendigkeit vorhabenbezogener, bereichsspezifischer Regelungen, anderenfalls existiert keine Rechtsgrundlage für Erhebung, Speicherung und Übertragung von Daten im GKV-Bereich
  - So auch BSG – Urt. v. 02.11.2010 – B 1 KR 12/10 R, Rdnr. 45: Vorrang bereichsspezifischer Regelungen im SGB V gegenüber dem BDSG

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Landeskrankenhausgesetze**, z.B. § 12 Abs. 2 Hess. KHG
- **Telemediengesetz, Telekommunikationsgesetz**
  - „Telekommunikationsdienst", § 3 Ziff. 24 TKG, sofern technischer Vorgang die inhaltlichen Aspekte überwiegt
  - „Elektronischer Informations- und Kommunikationsdienst", § 1 Abs. 1 TMG, sofern die Inhaltsleistung die Signalübertragung überwiegt
  - nur Telekommunikationsdienste im Sinne von TKG sind gemäß § 6 Abs. 1 TKG meldepflichtig

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015 (BGBl I 2015, Nr. 31 vom 24.07.2015)**
  - Schon **2013**: **Leitfaden** des Bundesamts für Sicherheit (BSI) „Schutz kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“
    - Als Beispiele von KI werden genannt (S. 6 des Leitfadens):
      - Krankenhausinformationssysteme;
      - Spezialanwendungen in Labor, Radiologie, Intensivstation;
      - elektronische Patientenakte;
      - Vernetzung
    - Als IT-Sicherheitsvorfälle werden insbesondere Ausfälle der IT; Schadsoftware, namentlich Auswirkungen auf Medizingeräte genannt (Seite 7 des Leitfadens)
  - Inkrafttreten des IT-Sicherheitsgesetzes: 25.07.2015
  - Weitere Novellierung wird notwendig nach Inkrafttreten der NIS-Richtlinie der EU

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Adressatenkreis: Betreiber einer „kritischen Infrastruktur“, § 2 Abs. 10 BSI-G
- Vom Anwendungsbereich ausgenommen sind sog. **Kleinstunternehmer**, § 8 c Abs. 1 BSI-G: Weniger als 10 Mitarbeiter sowie ein weniger als 2 Mio. Euro betragender Jahresumsatz (vgl. Empfehlung der Kommission ABl L 124 v. 20.05.2003, Seite 36)
- „Kritische Infrastruktur“ in diesem Sinne sind auch die Bereiche der „medizinischen Versorgung“ und der „Versorgung mit Arzneimitteln und Medizinprodukten“ (vgl. Begr BT-Drucksache 18/4096, S. 31: „Branchen: medizinische Versorgung, Labore“)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Referentenentwurf** einer Rechtsverordnung des Bundesinnenministeriums vom 09.02.2016 (**BSI-KritisVO**)
  - Zwei „Körbe“. In „**Korb“ II** findet sich der Sektor „Gesundheit“.
  - Derzeit Konsultation der Bundesländer; Inkrafttreten des Korbes I bis Mitte 2016
  - Bis Ende 2016 Konkretisierung der kritischen Infrastrukturen im Sektor Gesundheit (vgl. Referentenentwurf einer BSI-KritisVO vom 09.02.2016 sowie Könen, DuD 2016, 12, 13 f.). Inkrafttreten von Korb II wohl im 1. Quartal 2017.
  - Kriterium z.B.: Marktanteil an der Versorgung einer bestimmten Region mit einer bestimmten Leistung (vgl. BSI: Fragen und Antworten, www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/IT-SiGesetz/faq_node.html)
  - BSI erwartet, dass nicht mehr als 2.000 Betreiber Kritischer Infrastrukturen in den regulierten sieben Sektoren existieren (BT-Drucksache 18/4096, 21)
  - Bedeutend anzusehende Versorgungsgrade, § 10 Abs. 1 Satz 2 BSI-G
  - Vgl. lebens- und verteidigungswichtige Einrichtungen im Sinne von §§ 9 a-11 der Sicherheitsüberprüfungsfeststellungsverordnung, SFÜV (Gerling, RDV 2015, 167, 169)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Das Inkrafttreten der Rechtsverordnung des Bundesinnenministeriums setzt diverse Umsetzungs- bzw. Übergangsfristen in Gang
- Maßnahmen sind spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung zu treffen, § 8 a Abs. 1 Satz 1 BSI-G
- **Branchenspezifische Standards** können für verbindlich erklärt werden, wenn diese besser geeignet sind, § 8 a Abs. 2 BSI-G
  - Das BSI-G sieht „nur“ einen Mindeststandard vor, so dass zum einen die Möglichkeit besteht, branchenspezifische Standards vorzuschlagen
  - Zum anderen Ausstrahlungswirkung auch auf andere Branchen bzw. Einrichtungen, die keine „kritische Infrastruktur“ sind: Ausbildung eines „De facto-Standards“.
  - Problem: Was gilt, wenn mehrere inhaltlich voneinander abweichende Standardvorschläge für dieselbe Branche existieren? (Hornung, NJW 2015, 3336)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Rechtsfolgen**
  - Den Adressaten werden „**beachtliche wirtschaftliche Belastungen**“ entstehen (BT-Drucksache 18/4096, 3 ff.)
    - DKG (Baum), Das Krankenhaus 2016, 173: ca. 600 Mio. Euro Belastung pro Jahr für eine sachgerechte Ausstattung der IT-Bereiche von Krankenhäusern, das entspreche 10 % des Investitionsmittelbedarfs der Krankenhäuser
  - **Meldepflicht** gegenüber dem BSI bzgl. „ erheblicher“ IT-Sicherheitsvorfälle, § 8 b Abs. 4 Satz 1 BSI-G
    - Erwartet werden sieben Meldungen an das BSI je Betreiber pro Jahr bei 660 € Kosten pro Meldung (vgl. BT-Drucksache 18/4096, Seiten 4 f. und 38 ff.)
    - Welche Angaben zu melden sind, folgt aus § 8 b Abs. 4 Satz 2 BSI-G:
      - „Erhebliche“ Vorfälle (nach Gitter/Meißner/Spauschus, DuD 2016, 7, 9, zu verneinen bei „alltäglichen Ereignissen wie Spam oder Schadsoftware, die standardmäßig von den eingesetzten Sicherungssystemen abgefangen werden“)
      - Problematik der Klassifikation von Vorfällen (Grobauer/Kossakowski/Schreck, DuD 2016, 17, passim)
    - Vgl. Katalog des § 42 a BDSG oder auch § 83 a SGB X
    - Problem: Meldungen können personenbezogene Daten beinhalten, ohne dass § 8 b BSI-G eine Ermächtigungsgrundlage für die Übermittlung solcher Daten enthält (Hornung, NJW 2015, 3337 f.)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

Meldeformular

nach § 8b Absatz 4 BSIG

0. Allgemeine Informationen zum Meldenden

0.1	Name des meldenden Unternehmens bzw. der meldenden GÜAS	Trinkwasser-Mustergewinnungswerk
0.2	Betroffene Anlage (Kritische Infrastruktur gemäß BSI-KritisV) (Name und Ort)	Trinkwasser-Mustergewinnungswerk, Musterstadt
0.3	Name des Ansprechpartners für technischen Rückfragen	Frau Erika Mustermann
0.4	Kontaktdaten des Ansprechpartners (E-Mail, Telefonnummer)	e.mustermann@twgw.muster, Tel.: 0000 – 99 99-9099
	Die nachfolgenden Informationen sind bereits erfasst unter der Registrierungsnr.: (dann kein Ausfüllen der Felder 0.5-0.10 notwendig)	
0.5	Name des Hauptansprechpartners (Kontaktstelle gemäß § 8b (3) BSIG)	Herr Max Mustermann
0.6	E-Mail	it-sig@twgw.muster
0.7	Telefon (Festnetz)	0000 – 99 99 9090
0.8	Telefon (Mobil)	0000 – 99 99 999
0.9	Fax	0000 – 99 99 9091
0.10	Notfallkommunikationssysteme (z.B. Satellitentelefon)	

1. Allgemeine Informationen zum Vorfall

1.1	Meldungsart (Mehrfachnennungen möglich)	☐ Freiwillige Mitteilung ohne gesetzliche Verpflichtung ☒ Erstmeldung gemäß gesetzlicher Verpflichtung BSIG §8b (4) ☐ Folgemeldung zu IT-Störungsnummer: ☐ Abschlussmeldung zu IT-Störungsnummer:
1.2	Wie ist Ihre aktuelle Lageeinschätzung?	☐ Rot (Ausfall der kritischen Versorgungsdienstleistung auf lokaler, regionaler, nationaler Ebene erwartet bzw. eingetreten) ☒ Orange (Beeinträchtigung der kritischen Versorgungsdienstleistung bis hin zum Notbetrieb erwartet bzw. eingetreten) ☐ Gelb (Verstärkte Auffälligkeiten in der Kritischen Informationsinfrastruktur, aber keine Beeinträchtigung der Versorgungsdienstleistung eingetreten, oder es werden nur geringe Beeinträchtigungen erwartet) ☐ Grau (Keine Auffälligkeiten in der Kritischen Informationsinfrastruktur)
1.3	Zeitpunkt des letzten in die Meldung eingeflossenen Sachstands: (Datum, Uhrzeit)	01.04.2016, 13:37 Uhr
1.4	Betroffener Sektor bzw. betroffene Branche	

Energie
☐ Elektrizität
☐ Gas
☐ Mineralöl

Ernährung
☐ Ernährungswirtschaft
☐ Lebensmittelhandel

Finanz- und Versicherungswesen
☐ Banken
☐ Börsen
☐ Versicherungen
☐ Finanzdienstleister

Wasser
☒ Öffentliche Wasserversorgung
☐ Öffentliche Abwasserbeseitigung

Informationstechnik und Telekommunikation
☐ Informationstechnik
☐ Telekommunikation

Gesundheit
☐ Medizinische Versorgung
☐ Arzneimittel und Impfstoffe
☐ Labore

Transport und Verkehr
☐ Luftfahrt
☐ Seeschifffahrt
☐ Binnenschifffahrt
☐ Schienenverkehr
☐ Straßenverkehr
☐ Logistik

29.04.2016

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

1.5	Welche kritischen Dienstleistungen gem. BSI-KritisV sind betroffen?	Trinkwasserversorgung
	Welche Anlagentypen gem. BSI-KritisV sind betroffen bzw. könnten betroffen sein? (Nummer und Anlagenbezeichnung)	Gewinnungsanlage

2. Beschreibung der IT-Störung

2.1	Welche Grundwerte der Informations-sicherheit wurden verletzt? (Mehrfachnennungen möglich)	☒ Verfügbarkeit ☒ Integrität ☐ Authentizität ☐ Vertraulichkeit
2.2	Auf welchem/r IT-System / IT-Prozess / IT-Komponente ist was aufgetreten? (Kurzbeschreibung)	Fehlfunktion und Abstürze der PC-gestützten Pumpensteuerung
2.3	Wie ist es aufgetreten?	Konfigurationsdateien des Programms zur Pumpsteuerung wurden von Locky verschlüsselt
2.4	Welche (erfolgreichen) Gegen-maßnahmen wurden eingeleitet?	Locky wurde vom PC entfernt, Neuinstallation beauftragt
2.5	Datum und Zeit, an dem die IT-Störung eingetreten ist	31.03.2016 20:00 Uhr
2.6	Datum und Zeit, an dem die IT-Störung entdeckt wurde	01.04.2016 08:00 Uhr
2.7	Die IT-Störung hält noch an	☒ Ja ☐ Nein – Dauer (dd:hh:mm):
2.8	Wie ist die IT-Störung aufgefallen? (Mehrfachnennungen möglich)	
	☒ Systemausfall ☒ Fehlverhalten von Systemen ☐ Auswertung von Logfiles ☐ Systemwartung ☐ Technisches (Netz-)Monitoring ☐ Testbetrieb ☐ Hinweise von Dritten ☐ Veröffentlichung von gestohlenen Informationen durch Dritte ☐ Audit, Prüfung, Zertifizierung ☐ Hinweise des BSI ☐ Sonstiges:	

3. Vermutete oder tatsächliche Ursachen

3.1	Physikalischer Schaden (Mehrfachnennungen möglich)	☐ Zerstörung von Geräten ☐ Diebstahl von Geräten ☐ Manipulation von Geräten ☐ Verlust von Geräten ☐ Sonstiges:
3.2	Technisches Versagen (Mehrfachnennungen möglich)	☐ Versagen der Hardware ☐ Überlastung ☐ Software fehlerhaft ☐ Fehlverhalten von Systemen ☐ Sonstiges:
3.3	Organisatorische Ursache (Mehrfachnennungen möglich)	☐ Fehlbedienung ☐ Unautorisierte Nutzung von Ressourcen ☐ Social Engineering ☐ Sonstiges:
3.4	Versagen der genutzten Infrastruktur (Mehrfachnennungen möglich)	☐ Stromausfall ☐ Netzwerkausfall ☐ Kühlungsausfall ☐ Sonstiges:

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Informationstechnik

IT-Lagezentrum BSI

5. Informationen zum Ausfall bzw. zur Beeinträchtigung der kritischen Dienstleistungen

5.1	Hat die IT-Störung zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) geführt? Wenn nein: Welche Umstände oder Gegenmaß-nahmen führen dazu, dass es nicht zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur kommt? (Bsp.: Unabhängige Parallelversorgung, Angreifer wurde vorher aufgehalten, etc.)	☐ Ja, zu einem Ausfall ☒ Ja, zu einer Beeinträchtigung ☐ Nein (dann kein Ausfüllen der Felder 5.6 bis 5.8 notwendig)
5.2	Inwiefern ist die Funktionsfähigkeit der Kritischen Infrastruktur (also die Verfügbarkeit der kritischen Dienstleistungen) beeinträchtigt bzw. könnte sie beeinträchtigt werden? (u.a. welche Systeme und Komponenten sind betroffen bzw. könnten betroffen sein?)	Die Wasserpumpe „Mustermündung" arbeitet unregelmäßig und liefert nur noch einen Bruchteil der im Normalbetrieb gewonnenen Wassermenge.
5.3	Wie viele Personen könnten Ihres Wissens von der Beeinträchtigung / dem Ausfall der Funktions-fähigkeit der Kritischen Infrastruktur betroffen sein?	☐ < 250.000 Einwohner (bzw. < 50% der in der BSI-KritisV für Ihre Anlage angegebenen Schwelle) ☒ 250.000 bis 500.000 (bzw. 50% bis 100%) ☐ 500.000 bis 1.000.000 (bzw. 100% bis 200%) ☐ 1.000.000 bis 5.000.000 (bzw. 200% bis 1000%) ☐ > 5.000.000 Einwohner (bzw. > 1000%) ☐ Es kann keine Aussage gemacht werden
5.4	Wie ist die (potentielle) geographische Verbreitung der Beeinträchtigung / des Ausfalls der Funktions-fähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)? (Stadt, Region, Landkreis, Bundesland, Bundesgebiet)	Musterstadt und umliegender Kreis
5.5	Ist der Vorfall (potentiell) grenzüberschreitend? Wenn ja: Welche Staaten sind / wären ebenfalls betroffen?	☐ Ja ☒ Nein
5.6	Von wann bis wann bestand die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)?	Von ca. (TT.MM.JJJJ hh:mm): Bis ca. (TT.MM.JJJJ hh:mm): ☒ Auswirkung dauert an
5.7	Wann wurde die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) festgestellt?	Am (ca.) (TT.MM.JJJJ hh:mm): 01.04.2016 08:00
5.8	Welche Maßnahmen wurden ergriffen, um die Beeinträchtigung/den Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistung) zu mindern oder zu beheben?	Suche nach Original-Konfigurationsdateien

6. Sonstiges

6.1*	Weiterführende Informationen	
6.2*	Weiterführende Bewertungen	
6.3*	Weiteres	

* Freiwillige Angabe

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

3.5	Technischer Angriff (Mehrfachnennungen möglich)		
	Ausnutzung von Schwachstellen ☐ Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server) ☐ Code Execution ☐ Protokollschwachstelle ☐ Privilege Escalation ☐ Injection-Angriff ☐ Cross-Site-Scripting ☐ Cross-Site-Request-Forgery ☐ Schwache Algorithmen/Schlüssel ☐ Sonstiges:	**Hacking und Manipulationen** ☐ Webanwendungsbasierte Angriffe, z.B. Drive-by-Exploits ☐ Angriffe auf Webanwendungen, z.B. SQL-Injection, Buffer Overflow ☐ Angriffe auf Anwendungen bzw. Dienste wie DNS, SMTP, FTP ☐ Systematisches Ausprobieren von Passwörtern ☐ Sonstiges:	**Schadprogramme (Malware)** ☒ Malware-Infektion, z.B. durch Trojaner, Rootkits zum Zwecke der Kontroll-Übernahme, der Datenmanipulation oder des Datenabflusses ☒ Ransomware z.B. Sperren von IT-Systemen zu Erpressungszwecken ☐ Adware, Scareware z.B. zu Betrugszwecken ☐ Multifunktionale Malware z.B. Viren, Würmer, Riskware ☐ Sonstiges:
	Gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe) ☒ Initialer Angriff per E-Mail ☒ Initialer Angriff über Webseiten (Watering hole attack) ☒ Initialer Angriff über manipulierte Hardware (z.B. USB-Stick) ☐ Sonstiges:	**Missbrauch (Innentäter)** ☐ Weitergabe interner Informationen ☐ Unberechtigtes Erlangen von besonderen Zugriffsrechten, z.B. von Administrations-rechten ☐ Missbräuchliche Nutzung von Berechti-gungen (insb. von Zugriffsrechten), z.B. durch Externe über Fernwartungszugänge ☐ Sonstiges:	**Identitätsmissbrauch** ☐ Verschleierung einer Identität ☐ Diebstahl von Zugangsdaten, z.B. Identitätsdiebstahl, Phishing, Spear-Phishing, Pharming, Skimming ☐ Diebstahl oder Fälschung von Zertifikaten ☐ Unrechtmäßige Registrierung von Internetdomänen (Cybersquatting) ☐ Sonstiges:
	Verhinderung von Diensten ☐ Überflutung, z.B. (D)DoS ☐ Gezielter Systemabsturz, z.B. Paketfragmentierung ☐ Sonstiges:		Sonstiges:
3.6*	Sonstiges (z. B. CVE, Name der Schadsoftware, weitergehende Informationen, ...)	Locky	

4. Allgemeine Informationen zum informationstechnischen Angriff

☐	Es handelt sich nicht um einen informationstechnischen Angriff (dann kein Ausfüllen der Felder 4.1-4.5 notwendig)	
4.1	Angriffsart	☐ Gezielter Angriff ☐ Ungerichteter Angriff ☒ Unbekannt
4.2	Bei mehrfachen Angriffen bitte vermutete Anzahl angeben	
4.3*	Vermutete Motivation (Mehrfachnennungen möglich)	☒ Unbekannt ☒ Finanziell ☐ Persönlich ☐ Politisch ☒ Kriminell ☐ Terroristischer Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BKA) ☐ Nachrichtendienstlicher Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BfV) ☐ Sonstiges:
4.4	Welche Daten sind im Rahmen der bisherigen Analyse der IT-Störung angefallen und können dem BSI zur Verfügung gestellt werden? (Mehrfachnennungen möglich)	☐ Malware-Samples ☐ Hashsummen ☐ Dateinamen ☐ Signaturen ☐ Logfiles ☐ IP-Adressen ☐ URLs ☒ Sonstiges: Keine / unbekannt / Administratoren untersuchen noch
4.5	Strafverfolgung Wenn eine Strafanzeige gestellt wurde und Sie eine Weiterleitung an das BKA wünschen, ergänzen Sie bitte die entsprechenden Detailangaben.	☒ Unbekannt / keine Angabe ☐ Es wurde keine Strafanzeige gestellt ☐ Strafanzeige wurde gestellt Aktenzeichen: Polizeidienststelle: Bundesland: ☐ Weiterleitung der Meldung an BKA durch BSI ist erwünscht ☐ Täter wurde ermittelt

- **Organisatorische und technische Schutzmaßnahmen**, § 8 a Abs. 1 Satz 1 BSI-G
  - Die Schutzmaßnahmen sollen den Stand der Technik einhalten, d. h. eine Abweichung ist nur in begründeten Ausnahmefällen zulässig.
  - Einrichtung eines Informations-Sicherheitsmanagement-Systems (ISMS), z.B. gem. ISO 27001 bzw. ISO 27799 bzw. DIN EN 80001-1 (Anwendung Risikomanagement für IT-Netzwerke)
  - Die organisatorischen und technischen Maßnahmen sind spätestens zwei Jahre nach Inkrafttreten der BSI-KritisVO zu treffen, § 8 a Abs. 1 S. 1 BSI-G

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Mindestens alle zwei Jahre müssen ausreichende Schutzmaßnahmen „auf geeignete Weise“ nachgewiesen werden, § 8 a Abs. 3 Satz 1 BSI-G
  - Z.B. Sicherheits-Audits, die vom Betreiber einer kritischen Infrastruktur zu beauftragen sind
  - Das Bundesamt für Sicherheit in der Informationstechnologie kann zur Konkretisierung der Nachweismöglichkeiten Vorgaben machen, § 8 a Abs. 4 BSI-G (BT-Drucksache 18/4096, 48, kündigt einen Leitfaden hierzu an)

- Bußgeldbewehrte Pflichten, § 14 BSI-G
  - Gem. § 14 Abs. 2 BSI-G: Bußgeld bis zu 50.000 Euro
  - Bei Unterbleiben der Beseitigung festgestellter Mängel: Bußgeld von bis zu 100.000 Euro
- Sanktionen gem. Art. 83 ff. DSG-VO
- Ordnungswidrigkeiten, §§ 30, 130 OWiG

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Ggf. **Haftung des Betreibers** einer „kritischen Infrastruktur“
  - Haftung möglich, sofern Beeinträchtigung der Funktionsfähigkeit infolge von IT-Sicherheitsvorfällen
  - Frage: Sind Meldepflichten Schutzgesetze im Sinne von § 823 Abs. 2 BGB? (verneinend Hornung, NJW 2015, 3339; aber: Pflichten gem. § 83 a SGB X sind Schutzgesetz)
  - Art. 82 DSG-VO sieht eine Haftung für materielle und immaterielle Schäden vor
    - Daher dürfte die bisherige deutsche Rechtsprechung und nationale Rechtslage, welche immaterielle Schadenersatzansprüche nur bei schweren Verletzungen des Allgemeinen Persönlichkeitsrechts und ferner nur im Zusammenhang mit der Auftragsdatenverarbeitung gewährte, nicht mehr haltbar sein (siehe noch OLG Düsseldorf – Urt. v. 21.08.2015 – 16 U 152/14 zu § 7 Abs. 1 BDSG, § 82 Satz 1 SGB X bzw. § 8 Abs. 2 BDSG, § 82 Satz 2 SGB X)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- CAVE: Fehleinschätzung des Betreibers einer Einrichtung, ob sie eine kritische Infrastruktur im Sinne des BSI-G darstellt, geht zu dessen Lasten (vgl. Köhler, EnWZ 2015, 407, 409, betreffend die Energiewirtschaft)
- Zur Haftung der Betreiber und deren Organen bei Cyber-Angriffen: Mehrbrey/Schreibauer, MMR 2016, 75

- **Haftung des Bundes** für Handeln des BSI gegenüber Betreibern kritischer Infrastrukturen, § 8 b Abs. 2 Ziff. 4 BSI-G (Hornung, NJW 2015, 3334, 3340)
- Haftung der **Anbieter von IT-Sicherheit**
  - Produkthaftung
  - § 823 Abs. 1 BGB
- Öffentlich-Private Kooperation zwischen Betreibern kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen = Projekt UP KRITIS
- Siehe zum Ganzen: Rath/Kuss/Bach, K&R 2015, 437; Roßnagel, DVBl 2015, 1206; Gerling, RDV 2015, 167; Lurz/Scheben/Dolle, BB 2015, 2755

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **E-Health-Gesetz: Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze vom 21.12.2015** (BGBl I 2015, 2408)
- Inkrafttreten: 29.12.2015
- Schaffung einer **Telematik-Infrastruktur**
  - Legaldefinition in § 291 a Abs. 7 Satz 1 SGB V: „Die insbesondere für die Nutzung der elektronischen Gesundheitskarte und ihrer Anwendungen erforderliche interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur“.
  - Im E-Health-Gesetz ist bereits angelegt, dass die Telematik-Infrastruktur über die Funktionen der elektronischen Gesundheitskarte hinaus im Gesundheitswesen und der Gesundheitsforschung Anwendung finden soll (vgl. § 291 a Abs. 7 Satz 3 SGB V)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Prüfauftrag an KBV und GKV-Spitzenverband Bund, inwieweit bislang papiergebundene Verfahren zur **Organisation der vertragsärztlichen Versorgung durch elektronische Kommunikationsverfahren** ersetzt werden können
- Frist zur Vorlage des Ergebnisses der Prüfung: 31.12.2016, § 87 Abs. 1 Satz 6 SGB V
- § 291 Abs. 2 b Satz 3 SGB V ist „scharfgeschaltet“: Vertragsärzten, welche bei der erstmaligen Inanspruchnahme ihrer Leistungen durch einen Versicherten die von den Krankenkassen angebotene Dienste zur **Onlineprüfung der Leistungspflicht** nicht nutzen, ist ab dem 01.07.2018 die **Vergütung** vertragsärztlicher Leistungen pauschal um 1 % zu **kürzen**, § 291 Abs. 2 b Satz 10 SGB V
- „Verzahnung“ von BSI, Bundesbeauftragtem für den Datenschutz und der Gesellschaft für Telematik zwecks Schaffung sicherer Verfahren zur Übermittlung medizinischer Dokumente über die Telematik-Infrastruktur bis zum 31.12.2016, § 291 b Abs. 1 e SGB V

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Schaffung von Schnittstellen zur „systemneutralen Archivierung von Patientendaten sowie zur Übertragung von Patientendaten bei einem Systemwechsel“ in informationstechnische Systeme, § 291 d SGB V
  - Wann?: „Sobald wie möglich“
  - Anwendungsfelder: vertragsärztliche sowie vertragszahnärztliche Versorgung; Krankenhäuser
  - Erleichterung der Migration von Behandlungsdaten bei Praxisübernahmen (Begr. RegE BT-Drucksache 18/5293, 54)
- Noch in Entwurf der Bundesregierung (BT-Drucksache 18/5293) enthalten: Elektronischer Entlassbrief, § 291 f SGB V-E, als Ergänzung der Verpflichtung zum Entlassmanagement, § 39 Abs. 1 a SGB V
- Gesetz geworden ist aber lediglich die Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung, § 291 f SGB V **(„E-Arztbrief“)**
  - Schutz gegen unberechtigte Zugriffe durch „geeignete technische Maßnahmen entsprechend dem aktuellen Stand der Technik“, § 291 f Abs. 1 Satz 3 SGB V
  - Einsatz des elektronischen Heilberufsausweises mit qualifizierter elektronischer Signatur

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Zuschlag von pauschal 55 Cent für die Übermittlung eines elektronischen Briefs im Jahr 2017
- Ab 2018: Höhe des Zuschlags wird durch Vertragspartner nach § 291 a Abs. 7 b Satz 2 SGB vereinbart, § 291 f Abs. 5 SGB V
- Zertifizierung eines Praxisverwaltungssystems (Richtlinie der KBV, voraussichtlich Sommer 2016)
- **Weitere Themenfelder** des E-Health-Gesetzes:
  - Medikationsplan, § 31 a SGB V
  - Telemedizin, § 87 Abs. 2 a S. 16-S. 22 und § 291 g BGB (vgl. Vortrag von Markus Henkel)
  - Elektronische Patientenakte ab 2019, § 291 a Abs. 5 c SGB V
    - Problem ist die sichere und vollständige Löschung falsch eingespielter Daten (vgl. Studie in den USA, JMed Internet Res 2016, 18 (1): e8)
- Überblick zum E-Health-Gesetz: Paland/Holland, NZS 2016, 247

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Bedeutung der Einwilligung

- § 4 a Abs. 3 BDSG
- §§ 12 Abs. 1, 13 Abs. 2 TMG
- Definition der Einwilligung in Art. 4 Nr. 11 DSG-VO
- **Art. 7 Datenschutz-Grundverordnung**: **Bedingungen für die Einwilligung**
  - Es kommt auf die Notwendigkeit der Verarbeitung der Daten für die Erfüllung des Vertrages an, Art. 7 Abs. 4 DSG-VO
  - Erwägungsgrund 34 gemäß Kommissionsvorschlag sah demgegenüber vor: Eine Einwilligung kann nicht als Rechtsgrundlage für eine Verarbeitung herangezogen werden, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein „erhebliches Ungleichgewicht“ besteht (dies wäre ggf. problematisch im Arzt-Patienten-Verhältnis)
  - Davon abweichend stellte der Vorschlag des Rats nicht auf ein „erhebliches Ungleichgewicht“ ab, sondern auf das Kriterium der Erforderlichkeit.

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Regelungen in Landeskrankenhausgesetzen, z.B. § 12 Abs. 2 Hess. KHG
- Bedeutung der Einwilligung insbesondere nach dem Urteil des EuGH zu **Safe Harbor**: Einwilligung der Betroffenen in internationale Datentransfers nach gehöriger Information als Lösung?
  - So Heckmann/Starnecker, JM 2016, 58, 61
  - für unpraktikabel gehalten (vgl. Gemeinsame Stellungnahme von bvitg und GDD und DMDS, Seite 8; ebenso Grau/Granetzny, NZA 2016, 405, 407)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

C. Rechtliche Würdigung einzelner Anwendungsfelder

- **Überwachung in Krankenhaus und Pflegeheim sowie in häuslicher Umgebung (AAL)**
  - § 6 a BDSG: Der Einzelne darf nicht zum bloßen Objekt einer technikgestützten Verarbeitung zur Bewertung von Persönlichkeitsmerkmalen werden
  - Ähnlicher Regelungsgehalt in Art. 22 DS-GVO
  - Soweit das intelligente Videoüberwachungssystem daran anknüpft, dass eine Pflegekraft die Situation abschließend bewertet, sind die Anforderungen von § 6 a BDSG eingehalten (so auch: Bretthauer/Krempel/Birnstill, CR 2015, 239, 245)
  - Zumindest kurzfristig werden die von der Kamera erhobenen Daten im Arbeitsspeicher zwischengespeichert, so dass personenbezogene Daten im Sinne von § 6 b BDSG erhoben und gespeichert werden
  - Ähnlich Art. 6 Abs. 1 d, Art. 6 Abs. 1 f DS-GVO: Schutz „lebenswichtiger Interessen der betroffenen Person“; „Wahrung der berechtigten Interessen“

- Grundsatz der Datensparsamkeit ist gewährleistet, da ein Klarbild nur im Fall eines potentiellen Sturzes auf das mobile Endgerät einer Pflegeperson übertragen wird
- Pflicht zur Information des Betroffenen, Art. 13 und Art. 14 DS-GVO
- Legitimation durch Einwilligung des Betroffenen, Art. 6 Abs. 1 a Datenschutz-Grundverordnung

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Krankenhausinformationssysteme**
  - Orientierungshilfe Krankenhausinformationssysteme (2. Fassung, Stand März 2014, www.datenschutz-bayern.de)
  - **Auftragsdatenverarbeitung**, § 11 BDSG/Art. 28 DSG-VO
    - Definition des sog. Auftragsverarbeiters, Art. 4 Nr. 8 DSG-VO
    - Ausgangspunkt für Privilegierung: Auftragsdatenverarbeitung stellt keine Übermittlung im Sinne von § 3 Abs. 4 Satz 2 BDSG dar
    - Rechtfertigung für Privilegierung liegt darin, dass der Dienstleister die Daten alleine entsprechend der Vorgaben des Auftraggebers verarbeitet, ohne eigene Spielräume zu haben

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **„Outsourcing“ von Daten in einer Cloud als Auftragsdatenverarbeitung?**
  - Es gibt unterschiedliche Ausgestaltungen von Cloud-Lösungen
    - Modell 1: Bereitstellen standortunabhängiger IT-Ressourcen
    - Modell 2: Bereitstellen einer vorbereiteten Plattform zum Betrieb eigener Anwendungen
    - Modell 3: Zurverfügungstellen vollständiger Anwendungen („Software-as-a-service“)
  - Dazu: Foitzick/Plankemann, CCZ 2015, 180
- Momentan: Größere Cloud-Anbieter mit Niederlassungen in Deutschland und Nutzern in allen europäischen Mitgliedstaaten müssen Datenschutzgesetze aller Mitgliedstaaten beachten; Vereinheitlichung durch Datenschutz-Grundverordnung?

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Abgrenzung der Auftragsdatenverarbeitung zur nicht-privilegierten Funktionsübertragung, bei der Daten übermittelt werden:
  - Wenn der Stelle, der die Daten überlassen werden, ein eigener Handlungsspielraum eingeräumt ist, diese einer vertraglich abgesicherten Weisungsbefugnis unterliegt und die überlassende Stelle damit sowohl in tatsächlicher als auch in rechtlicher Hinsicht auf die Datenverarbeitung einwirken kann, liegt Auftragsdatenverarbeitung vor.
  - Demgegenüber werden bei der Funktionsübertragung Aufgaben einem Dritten ganz oder teilweise überantwortet; der Dritte wird insoweit selbst zur verantwortlichen Stelle im Sinne des Datenschutzrechts.

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Bei der Beauftragung von außerhalb der EU gelegenen Unternehmen handelt es sich per se um eine Funktionsübertragung (Kühling/Klar, DuD 2013, 794)
- Darüber hinaus liegt keine Auftragsdatenverarbeitung vor, wenn ein Zugriff auf die Daten (auch) aus einem Drittstaat möglich ist. Insoweit ist der Standort des Datenverarbeiters nicht allein entscheidend (Foitzick/Plankemann, CCZ 2015, 180, 184)
- Dann ist der Datenverarbeiter Dritter im Sinne von § 3 Abs. 8 Satz 3 BDSG, welchem die Daten im Sinne von § 3 Abs. 4 Satz 2 BDSG übermittelt werden.
- Dies bedarf einer Ermächtigungsgrundlage im BDSG für die Weitergabe von Gesundheitsdaten an einen solchen Dienstleister
- Nach der Rechtsprechung des BSG (10.12.2008 – B 6 KA 37/07 R) genügt dies im GKV-Bereich nicht, es bedarf einer bereichsspezifischen Ermächtigungsgrundlage im SGB V.

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Hält man hingegen das BDSG für eine taugliche Rechtsgrundlage, kommt eine Einwilligung des Betroffenen gem. § 4 a BDSG als Rechtfertigungsgrund in Betracht

- § 11 BDSG kann nach Maßgabe der Rechtsprechung des BSG (ebenfalls) nicht als Ermächtigungsgrundlage für Auftragsdatenverarbeitung herangezogen werden: § 80 SGB X ist lex specialis gegenüber den Regelungen des BDSG
- § 80 SGB X gilt nicht nur für den Umgang mit Sozialdaten, sondern z.B. über die Verweisungsnorm des § 295 a SGB V auch für den Umgang mit Gesundheitsdaten, unabhängig davon, ob eine Stelle im Sinne von § 35 Abs. 1 SGB I agiert

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Problem der Anwendung von § 80 SGB X
  - § 80 Abs. 5 SGB X sieht für den Fall der Vergabe des Auftrages an eine nicht-öffentliche Stelle im Sinne von §§ 67 Abs. 11, 81 Abs. 3 SGB X vor, dass der überwiegende Teil der Speicherung des gesamten Datenbestandes, also mindestens 50 %, beim Auftraggeber verbleiben muss. Muss mindestens die Hälfte des gesamten Datenbestandes beim (auslagernden) Krankenhaus verbleiben, ist ein Outsourcing aber unpraktikabel
  - Vergaberechtliche Bedenken gegen § 80 Abs. 5 SGB X (vgl. KG - Beschluss vom 16.09.2013 – VergR 4/13, CR 2014, 82)
  - Teilweise wird eine teleologische Reduktion von § 80 Abs. 5 Satz 2 SGB X vorgeschlagen (Rammos/Vonhoff, CR 2013, 265, 268; Schrotz/Zdanowiecki, CR 2015, 485, 489)
- Aber: Selbst bei einer Privilegierung nach § 80 SGB V bzw. § 11 BDSG stellt die Weitergabe von Daten nach wie vor eine „Nutzung“ im Sinne von § 3 Abs. 5 BDSG dar, welche einer Rechtfertigung nach § 28 Abs. 6 bis 9 BDSG bedarf.

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- Pflicht zur Dokumentation der Verarbeitungsvorgänge, Art. 30 DS-GVO
- Pflicht, im Rahmen von Auftragsverhältnissen, datenschutzfreundliche Voreinstellungen zu treffen, Art. 25 DS-GVO
- Seitenblick auf die Anwaltschaft: Seit 01.07.2015 sog. Non-legal Outsourcing, § 2 Abs. 3 lit. c BORA (dazu Hartung, AnwBl. 2015, 649)
- Einrichtung eines Informationssicherheitsmanagementsystems gem. ISO/IEC 27001? Das reicht aber nicht bei Gesundheitsdaten (vgl. Foitzik/Plankemann, CCZ 2015, 180, 183)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

- **Ersetzendes Scannen**
  - Handlungsleitfaden zur Handhabung von Einwilligungen (…) vom 07.10.2013 (Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.)
  - Technische Richtlinie des BSI Nr. 03138 vom 20.03.2013
  - Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis (DÄBl. 2014, A 963)

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

IT-gestützte Eingriffe in das Gehirn

- Gefahr der Beeinträchtigung der Integrität des Körpers durch Zugriff auf das Implantat und die dort erhobenen Daten
- Risiken durch Erhebung von Daten aus den nachfolgenden Veränderungen an anderen Körperteilen als denjenigen, in welche das Implantat eingebracht wurde
- Anwendbarkeit des IT-Sicherheitsgesetzes auf den Gesundheitsbereich
  - BSI-G: Betreiber kritischer Infrastrukturen
  - KritisVO

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

IT-gestützte Eingriffe in das Gehirn

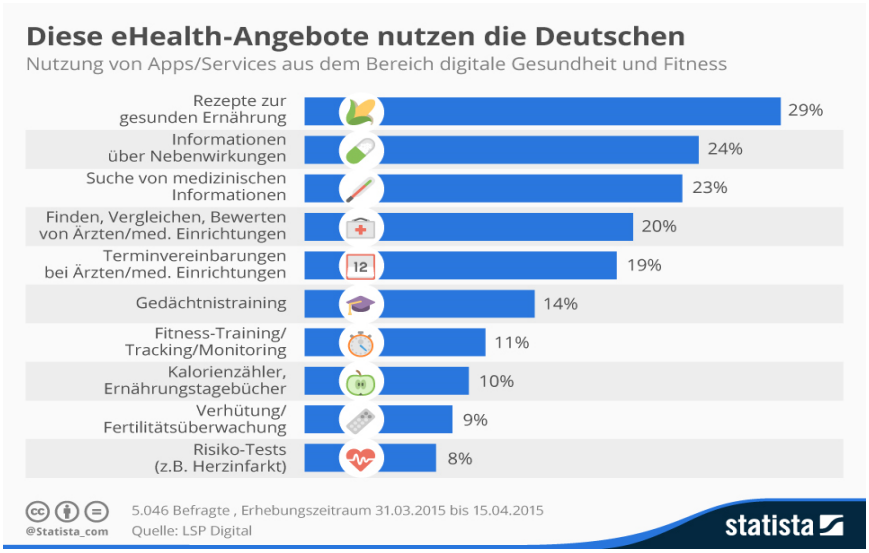
- Implantate, welche über eine Chipfunktion verfügen, werden von § 6 c BDSG erfasst
  - Rechtsfolge: Anwendung von Transparenzvorschriften
- Interesse der Hersteller von Implantaten an Informationsrückflüssen
- Wem „gehören“ die Daten? (BGB-Sachenrecht?)
- „Medical Devices“: Report to U.S. Congress, August 2012; Medizinprodukterecht

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

„Virtuelle Arztpraxis“/Einsatz mobiler Geräte in Arztpraxen

- Z.B. Klara GmbH in New York mit der sog. Derm App zur Vernetzung des Arztes mit Bestandspatienten
- Verbot der „ausschließlichen“ Fernbehandlung ohne unmittelbaren persönlichen Arzt-Patienten-Kontakt, § 7 Abs. 4 MBO-Ä
- Hinweise und Erläuterungen der Bundesärztekammer zu § 7 Abs. 4 MBO-Ä vom 11.12.2015
- Vgl. OLG Düsseldorf – Urt. v. 04.06.2013 – 20 U 137/12
- Zur Bildung spezifischer Qualitätsstandards und zur Haftung: Gaßner/Strömer, VersR 2015, 1219 sowie Kipker, Conference Paper 11/2015
- Anwendbarkeit des MPG auf mobile Geräte?
- Produkthaftungsgesetz; § 823 Abs. 1 BGB; § 433 BGB; § 631 BGB; § 651 BGB ; § 7 BDSG

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB



PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Fitness Apps

- **Zulässige Auswertung durch die gesetzliche Krankenversicherung?**
  - Sozialdaten im Sinne von § 67 Abs. 1 Satz 1 SGB X
  - §§ 284 ff. SGB V als leges speciales gegenüber §§ 67 ff. SGB X (vgl. BSG – Urt. v. 02.11.2010 – B 1 KR 12/10 R, Rdnr. 47, zitiert nach juris)
  - § 284 Abs. 1 Satz 5 SGB V
  - § 82 SGB X als lex specialis betreffend Schadenersatzansprüche bei Sozialdatenverarbeitung
  - Derzeit kein Anspruch auf immateriellen Schadenersatz außerhalb des Bereichs der automatisierten Auftragsdatenverarbeitung (vgl. OLG Düsseldorf – Urt. v. 21.08.2015 – 16 U 152/14)
  - Entsprechende Anwendung von § 8 BDSG

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

D. Fragen

- Ausbildung eines „Gesundheitsdatenschutzrechts“ (Monographie von Kingreen/Kühling (Hrsg.), 2015)
- Einerseits Befürchtung eines Silicon-Valley-Kapitalismus betreffend „Big Data“ (Weichert, DuD 2014, 831, 837) sowie Klage über „Unterkomplexität“ der Regelungen (Roßnagel/Nebel/Richter, ZD 2015, 455),
  andererseits wird ein hypertropher Datenschutz beklagt (Kingreen/Kühling, JZ 2015, 213, 214)
- Technisierung/Bürokratisierung der Arzt-Patienten-Beziehung?
- Das technisch Machbare stets für die Versorgung wünschenswert?

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB

Dr. Ole Ziegler
Fachanwalt für Medizinrecht
Fachanwalt für Handels- und Gesellschaftsrecht
Mediator

PLAGEMANN RECHTSANWÄLTE
Partnerschaft mbB
Niedenau 13 – 19
60325 Frankfurt am Main
ole.ziegler@plagemann-rae.de
Telefon +49 69 971206-42