DaSuMed

Datenschutz für medizinische und soziale Einrichtungen

Ausgabe 06/2019

A. Gesetzesinfos

1. Digitales Versorgungs-Gesetz – qualifizierte Anforderungen an die IT-Sicherheit

Am 19.12.2019 traten die wesentlichen Teile des Digitale Versorgungsgesetzes in Kraft (https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27447350%27%5D&skin=pdf&tlevel=-2&nohist=1). Neben Themen, wie „App auf Rezept“, „eRezept“, „Forschungdatenzentrum“ etc. dürfte für Krankenhäuser und Arztpraxen vermutlich Art. 1 Ziff. 10 (bzw. §75 b SGB V „Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung“) in den Fokus geraten: Bis zum 30.6.2020 ist es Aufgabe der KBV in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung festlegen. Diese Richtlinie betrifft alle Einrichtungen der vertragsärztlichen/vertragszahnärztlichen Versorgung, also insbesondere sowohl Arztpraxen als auch Krankenhäuser. Ausgenommen sind nur die Einrichtungen, bei denen „bereits angemessene Vorkehrungen nach § 8a Absatz 1 des BSI-Gesetzes getroffen“ wurden (§ 75b Abs. 4 SGB V). Das dürfte für die Wenigsten gelten.

2. Implantatregistergesetz

Im Wesentlichen ab dem 01.01.2020 tritt das Implantatregistergesetz in Kraft (https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27447340%27%5D&skin=pdf&tlevel=-2&nohist=1). Es enthält Regelungen zur Datenverarbeitung, zu Meldepflichten und zur Beschränkung von Betroffenenrechten.

3. EU-Whistleblower-Richtlinie

Am 23.10.2019 wurde die Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, veröffentlicht. Bis dato war der Schutz von Hinweisgebern in der EU nur bruchstückhaft geregelt. Mit der Richtlinie wird nun ein EU-weiter Mindeststandard für den Schutz von Hinweisgebern eingeführt. Ziel der Richtlinie ist es, Verstöße gegen das Unionsrecht aufzudecken und zu unterbinden. Personen, die im Rahmen ihrer beruflichen Tätigkeit mögliche Verstöße bemerken, sollen diese anzuzeigen können ohne Repressalien aus ihrem Umfeld zu befürchten.

Nach den neuen Vorschriften werden Unternehmen mit mehr als 50 Mitarbeitern dazu verpflichtet, sichere Kanäle für die Meldung von Verstößen einzurichten. Hinweisgeber sind nach der Richtlinie nicht verpflichtet, die internen Kanäle auszuschöpfen, bevor sie sich an externe Stellen wenden. Für

Mark Rüdlin
Rechtsanwalt und Datenschutzbeauftragter
Lerchenstraße 28
22767 Hamburg
Telefon 040 69 79 72 80
Telefax 040 69 79 72 90
ra@markruedlin.de
www.markruedlin.de

Unternehmen kann es jedoch vorteilhaft sein, die internen Kanäle möglichst attraktiv auszugestalten, um Missstände im Unternehmen zunächst intern aufzuklären und unterbinden zu können.
Die neue EU-Whistleblower-Richtlinie ist bis zum 17. Dezember 2021 durch den deutschen Gesetzgeber umgesetzt werden.

4. ePrivacy-Verordnung endgültig gescheitert

Die Verhandlungen zur ePrivacy-Verordnung sind im Ministerrat endgültig gescheitert. Nun will die Kommission einen neuen Anlauf unternehmen (https://www.heise.de/newsticker/meldung/E-Privacy-EU-Staaten-lassen-Verordnung-scheitern-Kommission-will-Neustart-4603164.html).

B. DSGVO

1. 14,5 Mio. € Bußgeld der Berliner Behörde gegen Deutsche Wohnen

Am 30.Oktober 2019 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen die Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund 14,5 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) erlassen (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf). Hintergrund war eine Verwaltungssoftware, die keine Möglichkeit eröffnet nicht mehr archivierungspflichtige Daten (insbesondere sensible Daten, wie Gehaltsbescheinigungen etc.) löschen zu können.

2. 9,5 Mio.€ Bußgeld gegen 1&1 Telecom GmbH

Weil 1&1 zur Kundenidentifikation nur Namen und Geburtsdatum erfragt und keine weiteren Maßnahmen zum Schutz der Kundendaten etabliert hatte, sprach der BfDI ein Bußgeld in Höhe von 9,5 Mio. € aus. 1&1 will sich dagegen zur Wehr setzen (https://newsroom.1und1.de/2019/12/09/11-klagt-gegen-bussgeldbescheid-der-datenschutzbehoerde/#page-content).

3. 105.000 € Geldbuße gegen Uniklinik Mainz in Rheinland-Pfalz

Mehrere datenschutzrechtliche Verstöße des Uniklinikums Mainz (Patientenverwechslung bei der Aufnahme des Patienten) wurden von der dortigen Aufsichtsbehörde mit einem Bußgeld in Höhe von 105.000 € geahndet (https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/geldbusse-gegen-krankenhaus-aufgrund-von-datenschutz-defiziten-beim-patientenmanagement/). Das Bußgeld soll Signalwirkung entfalten, so die Behörde.

4. Erfahrungsbericht der zur Anwendung der DSGVO

Seit Anfang Dezember liegt der Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO vor (https://www.baden-

Mark Rüdlin
Rechtsanwalt und Datenschutzbeauftragter
Lerchenstraße 28
22767 Hamburg
Telefon 040 69 79 72 80
Telefax 040 69 79 72 90
ra@markruedlin.de
www.markruedlin.de

wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191113_Erfahrungsbericht-zur-Anwendung-der-DS-GVO-Endfassung.pdf). Es gibt noch viel zu tun ...

5. Standard-Datenschutz-Modell 2.0

Die DSK hat die Version 2 des Standard-Datenschutz-Modells veröffentlicht (https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/SDM-Handbuch_V_2.0.pdf), leider nach wie vor ohne Referenzmaßnahmen-Katalog.

6. Überprüfungsbericht zum Privacy Shield

Das European Data Protection Board hat den dritten Überprüfungsbericht zum Privacy Shield veröffentlicht (https://edpb.europa.eu/sites/edpb/files/files/file1/edpbprivacyshield3rdannualreport.pdf_en.pdf). Das Privacy Shild ist die (umstrittene) Rechtsgrundlage bei Datenübermittlungen mit amerikanischen Unternehmen. Ergebnis: vorerst kann weiter auf das Privacy Shield gesetzt werden.

7. Datenschutzkonformer Einsatz von Windows 10

Die DSK hat in Kooperationn mit Microsoft eine Prüfschema zum datenschutzkonformen Einsatz von Windows 10 zur Verfügung gestellt (https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Datenschutz_bei_Windows_10_-_Pruefschema_V1.0.pdf).

8. Gesundheitswebseiten und Gesundheits-Apps

Die DSK hat eine Entschließung zum Umgang mit Gesundheitswebseiten und Gesundheits-Apps und der Weitergabe sensibler Daten an unbefugte Dritte veröffentlicht (https://www.datenschutzkonferenz-online.de/media/en/20191106_entschlie%C3%9Fung_gesundheitswebseiten_dsk.pdf).

9. Technische Anforderungen an Messenger-Dienste

In einem Whitepaper hat die DSK technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich beschrieben (https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf).

10. Gesundheitseinrichtungen müssen Datenschutz gewährleisten

In einer weiteren Entschließung der DSK wird darauf hingewiesen, das Gesundheitseinrichtungen unabhängig von der Größe der Einrichtung den Schutz von Patientendaten gewährleisten müssen (https://www.datenschutzkonferenz-online.de/media/en/20191106_entschlie%C3%9Fung_gesundheitseinrichtungen_dsk.pdf).

11. KI – Systeme: DSK Empfehlung zu Technisch-organisatorische Maßnahmen

In einem Positionspapier hat die DSK umfangreiche Empfehlungen zu technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen veröffentlicht (https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf).

Mark Rüdlin
Rechtsanwalt und Datenschutzbeauftragter
Lerchenstraße 28
22767 Hamburg
Telefon 040 69 79 72 80
Telefax 040 69 79 72 90
ra@markruedlin.de
www.markruedlin.de

C. Urteile und Beschlüsse von Gerichten

1. Bundesverfassungsgericht zementiert Recht auf Vergessen

Das BVerfG hat mit Beschluss vom 06.11.2019, Az.: 1 BvR 16/13 das Recht auf Vergessen vor dem Hintergrund umfassender Informationsmöglichkeiten durch Internetrecherchen bekräftigt und die Verfassungsbeschwerde eines Beschwerdeführers gegen die Bereithaltung von mehr als 30 Jahre zurückliegenden Presseberichten in einem Onlinearchiv als begründet angesehen.

2. Umfassender Auskunftsanspruch zu Gesundheitsdaten

Das LG Landau/Pfalz hat mit Beschluss vom 17.09.2019, Az.: 4 O 389/17 einen umfassenden Auskunftsanspruch eines Patienten nach Art. 15 DSGVO bejaht:

„Die Beklagte verkennt, dass der Begriff der „personenbezogenen Daten“ nach Art. EWG_DSGVO Artikel 4 DS-GVO weit gefasst ist und nach der Legaldefinition in Art. EWG_DSGVO Artikel 4 Nr. EWG_DSGVO Artikel 4 Nummer 1 DS-GVO alle Informationen umfasst, die sich auf eine identifizierbare natürliche Person beziehen. Unter die Vorschrift fallen demnach sämtliche Informationen, die die Identifizierbarkeit einer Person ermöglichen können. Nach diesen Grundsätzen stellen auch ärztliche Unterlagen, Gutachten oder sonstige vergleichbare Mitteilungen anderer Quellen „personenbezogene Daten“ in diesen Sinne dar. ... Die hierin enthaltenen Informationen beschränken sich im Wesentlichen auf die persönlichen Stammdaten des Klägers wie Name, Geburtsdatum, Anschrift und Beruf sowie eine Auflistung darüber, wegen welcher Krankheiten des Klägers in welchem Zeitraum Leistungen erstattet wurden. Ungeachtet dessen, dass die Auflistung der Erstattungen bei Weitem nicht vollständig sein dürfte, enthält die Mitteilung an den Kläger weder Angaben zur Herkunft der Daten, zum Empfänger, an den die Daten weitergegeben werden sowie Angaben zum Zweck der Speicherung (vgl. hierzu Art. EWG_DSGVO Artikel 15 Abs. EWG_DSGVO Artikel 15 Absatz 1 a), b) und c) DS-GVO). Es finden sich zudem weder Angaben zum Beitragskonto noch zu ärztlichen Befundberichten bzw. Angaben zu intern erstatteten Gutachten. Die Einholung solcher Gutachten liegt vorliegend insbesondere unter Berücksichtigung des Krankheitsbildes des Klägers auf der Hand. „

Das Gericht stützt damit das Akteneinsichtsrecht auf Art. 15 DSGVO. In der Folge sind Akteneinsichtswünsche von Patienten kostenfrei zu bearbeiten, § 630g BGB mit dem Hinweis auf eine Kostenpflicht einer Akteneinsicht greift nach diesem Instanzurteil nicht mehr.

3. Abmahnbarkeit von Datenschutzverstößen

Das OLG Naumburg hat mit Urteil vom 07.11.2019; Az.: 9 U 6/19 die Abmahnbarkeit von Datenschutzverstößen durch Wettbewerber bei der Verarbeitung von Gesundheitsdaten bei Online-Apotheken-Bestellungen festgestellt.

Mark Rüdlin
Rechtsanwalt und
Datenschutzbeauftragter
Lerchenstraße 28
22767 Hamburg
Telefon 040 69 79 72 80
Telefax 040 69 79 72 90
ra@markruedlin.de
www.markruedlin.de

4. Arbeitszeiterfassung mittels Fingerprint unzulässig

Die Arbeitszeiterfassung durch ein Zeiterfassungssystem mittels Fingerprint ist nicht erforderlich im Sinne von § 26 Abs. 1 BDSG und damit ohne Einwilligung der betroffenen Person nicht zulässig, so das ArbG Berlin mit Urteil vom 16.10.2019, Az.: 29 Ca 5451/19. Denn für die Begründung oder Aufrechterhaltung des Beschäftigtenverhältnisses ist dies nicht erforderlich.

5. Kein Anspruch Betroffener auf bestimmte aufsichtsrechtliche Maßnahmen

Das VG Ansbach hat mit Urteil vom 08.08.2019, Az.: AN 14 K 19.272 entschieden, dass Betroffene keinen Anspruch gegen eine Aufsichtsbehörde auf bestimmte aufsichtsrechtliche Maßnahmen geltend machen können. Einzig ein Anspruch auf fehlerfreie Ermessensausübung ist angezeigt. Schon am 08.05.2019 hatte das SG Frankfurt/Oder, Az.: S 49 SF 8/19 ein vergleichbares Urteil gesprochen.

6. Kein gerichtlicher Rechtsschutz gegen aufsichtsbehördliche Beanstandung

Das VG Stuttgart hat mit Urteil vom 21.02.2019, Az.: 14 K 17293/17 festgestellt, dass gegen eine Beanstandung einer Aufsichtsbehörde weder eine Anfechtungsklage noch eine Feststellungsklage zulässig ist, da der Beanstandung kein materielle Rechtswirkung zukommt.

7. Unzulässige Ausgestaltungen des Ärzte-Bewertungsportals Jameda

Das OLG Köln hat mit zwei Urteilen vom 14.11.2019 (Az.: Az.15 U 89/19 - und Az. 15 U 126/19) mehrere Ausgestaltungsmerkmale als unzulässig bewertet und Löschungsansprüche der betroffenen Ärzte bejaht. Als „neutraler Informationsmittler“ ist es unzlässig bei Basiskunden auf eine Liste weiter Ärzte zu verweisen, bei zahlenden Kunden hingegen nicht. Ebenso unzulässig ist es zahlende Kunden mit Bild darzustellen, wohingegen nicht zahlende Ärzte nur mit einem grauen Schattenriss zu sehen sind.

8. Schmerzensgeld für Verletzung der ärztlichen Schweigepflicht

Die Verletzung der ärztlichen Schweigepflicht – hier: Rechnung über zwei Botox-Spritzen – löst ein Schmerzensgeld in Höhe von 1.200 € aus, so das OLG Frankfurt/M, Bes. vom 11.07.2019, Az.: 2 O 247/18.

9. Elektronische Daten sind keine Sachen

Elektronische Daten – zum Beispiel in Frage stehende Daten in einem Insolvenzverfahren - sind keine körperlichen Gegenstände und damit keine Sachen im Sinne von § 90 BGB und können daher auch nicht mit einem Herausgabeanspruch geltend gemacht werden, so das OLG Brandenburg mit Urteil vom 06.11.2019, Az.: 4 U 123/19.

10. Videoüberwachung in Fitness-Centern

Mit Urteil vom 19.11.2019 hat das VG Schleswig hat Videokameras in Umkleiden, auf Trainingsflächen und in Aufenthaltsbereichen für unzulässig erklärt (https://www.datenschutzzentrum.de/artikel/1303-Videoueberwachung-im-Fitness-Studio-nicht-in-Umkleiden!.html).

Mark Rüdlin
Rechtsanwalt und
Datenschutzbeauftragter
Lerchenstraße 28
22767 Hamburg
Telefon 040 69 79 72 80
Telefax 040 69 79 72 90
ra@markruedlin.de
www.markruedlin.de

D. Sonstiges

1. Patientendaten an falsche Empfänger

Immer wieder werden Patientendaten an falsche Empfänger geschickt. Manchmal geschieht dies völlig unbeschwert, wie der Fall von Asklepius in Hamburg zeigt (https://www.ndr.de/nachrichten/hamburg/Patientendaten-an-falsche-Empfaenger-verschickt,patientendaten122.html).

2. Stand der Technik

Der Bundesverband IT-Sicherheit e.V. hat eine neue Standortbestimmung zum „Stand der Technik" vorgenommen (https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-09_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf).

3. Facebook-Fanpages

Facebook hat auf die Kritik u.a. der DSK reagiert und ein neues Joint Control-Agreement rausgegeben, um den Anforderungen aus dem Facebook-Urteil 2018 (ULD / Wirtschaftsakademie) gerecht zu werden (https://www.facebook.com/legal/terms/page_controller_addendum). Damit scheint vorerst Entspannung einzutreten, insbesondere auch wenn man der Interpretation auf dieser Webseite folgen möchte: https://datenschutz-generator.de/facebook-update-seiten-insights-fanpages

4. Gematik – Whitepaper zu Datenschutz und Informationssicherheit

Die Gematik hat ein Whitepaper zum Thema „Datenschutz und Informationssicherheit – Wie werden Gesundheitsdaten in der Telematikinfrastruktur geschützt?" veröffentlicht (https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_whitepaper_web_Stand_270916.pdf).

5. Datenschutzethik-Kommission

Die vor einem Jahr eingesetzte Datenschutzethik-Kommission hat Ihren Bericht vorgelegt (https://datenethikkommission.de/gutachten/).

6. Neue Fassungen der Skripte „Internetrecht" und „IT-Recht"

Die Skripte „Internetrecht" und „IT-Recht" von Prof. Thomas Hoeren aus Münster liegen in aktualisierter Fassung vor (http://vg01.met.vgwort.de/na/2a7470310b6d490bb398dabfa77f009c?l=https://www.itm.nrw/wp-content/uploads/Skript-Internetrecht-Oktober-2019.pdf; http://vg01.met.vgwort.de/na/710a4dbc6b614cba8e14f5de86eea99e?l=https://www.itm.nrw/wp-content/uploads/Skript-IT-Recht-Stand-Oktober-2019.pdf).

Mark Rüdlin
Rechtsanwalt und Datenschutzbeauftragter
Lerchenstraße 28
22767 Hamburg
Telefon 040 69 79 72 80
Telefax 040 69 79 72 90
ra@markruedlin.de
www.markruedlin.de