DaSuMed
Datenschutz für medizinische und soziale Einrichtungen
Ausgabe 04/2020

A. Gesetzesinfos

1. Patientendaten-Schutz-Gesetz (PDSG)

Das PDSG (https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/P/PDSG-Bundestag_Drs-18793.pdf) bringt eine Reihe gravierender Änderungen. Unter anderem werden alle Krankenhäuser - nicht nur die gemäß KRITIS-Verordnung als „Kritische Infrastruktur“ eingestuften – verpflichtet, ab 1.1.2022 verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von IT-Störungen zu treffen und spätestens alle zwei Jahre an den Stand der Technik anzupassen.

Der BfDI hat auf die europarechtswidrige Verarbeitung hingewiesen (vgl. Presserklärung: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/20_BfDI-zu-PDSG.html).

2. Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemediensowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze

1.1 Das BMWi plant ein Gesetz, Vorschriften rund um die Privatsphäre für Online-Dienste inklusive Messenger aus der Datenschutzgrundverordnung (DSGVO), dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG) zu vereinheitlichen (https://www.heise.de/downloads/18/2/9/4/6/4/2/1/20200731_RefE_TTDSG_cleaned.pdf). Neben Aspekten der Vereinheitlichung können Vorgaben wie die zur **Bestandsdatenauskunft** (BVerfG, Beschluss vom 27. Mai 2020 - 1 BvR 1873/13, 1 BvR 2618/13) umgesetzt werden. Interessant: es finden sich Ideen zur **Cookie-Einwilligung** per Browsereinstellung und legitimierend auf vertraglicher Grundlage (ausführlich dazu: Niko Härting, Neuer Gesetzesentwurf aus dem BMWi: Cookie-Einwilligung per Browsereinstellung und Cookie-Einsatz auf vertraglicher Grundlage, https://www.cr-online.de/blog/2020/08/03/neuer-gesetzesentwurf-aus-dem-bmwi-cookie-einwilligung-per-browsereinstellung-und-cookie-einsatz-auf-vertraglicher-grundlage/).

3. Datentransparenz-Verordnung

Die Datentransparenz-Verordnung wurde neu gefasst (https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl120s1371.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl120s1371.pdf%27%5D__1593166667603). Die Verordnung erfüllt die Vorgaben aus den §§ 303a bis 303f SGB V und regelt insbesondere auch die Aufgabenübertragung der Vertrauensstelle nach § 303c SGB V und des Forschungsdatenzentrums nach § 303d SGB V. In § 3 wird geregelt, welche Daten die Krankenkassen an die Datensammelstelle übermitteln, § 5 regelt den Umgang mit der Pseudonymisierung, § 7 bestimmt das Vorgehen bei einer Antragstellung an das Forschungsdatenzentrum, § 10 die Datenbereitstellung.

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

B. DSGVO

1. Bußgeld gegen AOK Baden-Württemberg

Der LfDI Baden-Württemberg hat gegen die AOK Baden-Württemberg ein Bußgeld in Höhe von 1.240.000 wegen unzureichender technisch-organisatorischer Maßnahmen im Rahmen eines Gewinnspiels € verhängt (https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/).

2. Anonymisierung

Der BfDI hat ein Positionspapierzur Anonymisierung unter der DSGVOunter besonderer Berücksichtigung der TK-Branche veröffentlicht (file:///Users/markruedlin/Downloads/Positionspapier-Anonymisierung.pdf).

3. Auftragsverarbeitung

Die niedersächsische Datenschutzbehörde hat eine umfangreiche FAQ-Übersicht zum Thema Auftragsverarbeitung veröffentlicht (https://lfd.niedersachsen.de/startseite/infothek/faqs_zur_ds_gvo/faq-auftragsverarbeitung-189637.html).

4. DSGVO-konformes Drucken

Bitkom hat einen Leitfaden „DS-GVO-konformes Drucken Drucken, Scannen, Faxen, Kopieren“ veröffentlicht (https://www.bitkom.org/sites/default/files/2020-06/20200625_lf_ds-gvo-konformes_drucken.pdf).

5. Tätigkeitsbericht 2019 BfDI

Der BfDI hat den Tätigkeitsbericht 2019 veröffentlicht (https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/28TB_19.html?nn=5217016).

6. Bußgelder wegen Fehler bei Corona-Gästelisten

Der HfDI hat Bußgelder wegen fortgesetzter Fehler um Umgang mit Corona-Gästelisten – insbesondere offen ausliegende Gästelisten - ausgesprochen (https://datenschutz-hamburg.de/pressemitteilungen/2020/08/2020-08-14-gaestelisten).

C. Urteile und Beschlüsse von Gerichten

1. EuGH erklärt Privacy Shield für ungültig

Der EuGH hat mit Urteil vom 16.07.2020, Az.: C311/18 das Privacy Shield für ungültig erklärt (http://curia.europa.eu/juris/document/document.jsf;jsessionid=83114E33B502C8CBF3BFFE375AB3C9F2?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=10008985). Die Kurzfassung kann der

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

Presseerklärung entnommen werden (https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf). Das Privacy Shield war die Legitimationsgrundlage für Datentransfers in die U.S.A. und dürfte fast alle Unternehmen betreffen. Damit sind fast alle Unternehmen in Deutschland betroffen, da kaum jemand ohne amerikanische Produkte und Softwareanwendungen arbeitet. Die **EDSA** hat FAQ (Frequently Asked Questionson the judgment of the Court of Justice of the European Union in Case C-311/18 -Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems - https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf) hierzu veröffentlicht. Die DSK hat in einer Pressemitteilung ebenfalls Stellung genommen (https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf).

Die EU-Standardvertragsklauseln hingegen bleiben nach der Entscheidung des EuGH grundsätzlich gültig, bedürfen aber grundsätzlich zusätzlicher Maßnahmen, so die DSK. Dr. Carlo Piltz (Das SchremsII-Urteil des EuGH: Folgen für die Praxis des Einsatzes von Standarddatenschutzklauseln, https://www.delegedata.de/wp-content/uploads/2020/07/Blog-SchremsII_CP.pdf) beispielsweise sieht dafür auch praktische Umsetzungsmöglichkeiten.

Inzwischen stößt NOYB – European Center for Digital Rights in Wien – dutzendfache Beschwerden gegen diversen Unternehmen bei den jeweils zuständigen Aufsichtsbehörden an (https://noyb.eu/en/eu-us-transfers-complaint-overview), so dass sich diese in absehbarer Zeit positionieren müssen.

Wie berichtet wird, haben EU-Kommission und das US-Handelsministerium und die Kommission mit Gesprächen begonnen. Dabei soll auszuloten werden, ob und wie der EU-US-Privacy Shield gestärkt werden könnte, um den Anforderungen EuGH-Urteils vom 16.07.2020 im Fall Schrems II zu genügen.

https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836

Welche Lösungswege sich abzeichnen, ist unklar. Der Landesdatenschutzbeauftragte von Baden-Württemberg fordert zwischen den Aufsichtsbehörden abgestimmte und pragmatische Lösungen (https://www.badische-zeitung.de/ich-werde-keine-alleingaenge-machen).

Meine Empfehlung: Verbände, die deutschen Aufsichtsbehörden und letztlich die Europäische Kommission müssen in den nächsten Wochen und Monaten ausloten, wie das Urteil umgesetzt werden und trotzdem die Stabilität und Integrität der in der Patientenversorgung eingesetzten IT-Systeme gewährleisten werden kann. Aktuell heißt das schlicht: abwarten.

2. Online-Pflichtangaben zur alternativen Streitbeilegung

Der EuGH hat mit Urteil vom 25.06.2020, Az.: C-380/19 deutlich gemacht, dass Pflichtgaben zur alternativen Streitbelegung in einer Erklärung der Webseite erwähnt werden müssen, auch wenn das Unternehmer über diese Webseite keine Verträge mit Verbrauchern abschließt.

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

3. Für Strafverfolgungsbehörden gilt nicht die DSGVO

Mit Urteil vom 07.04.2020, Az.: II B 82/19 hat der BFH die DSGVO im Falle einer Finanzfahndung aufgrund von Art. 2 Abs. 2 Ziff. d DSGVO für nicht anwendbar erklärt und auf § 500 StPO und damit den dritten Teil des BDSG verwiesen.

4. Online-Werbung für ärztliche Fernbehandlung wettbewerbswidrig

Das OLG München I hat mit Urteil vom 09.07.2020, Az.: 6 U 5180/19 eine Online-Werbung für ärztliche Fernbehandlung als wettbewerbswidrig gebrandmarkt.

5. Corona-Daten-Erhebung DSGVO-konform

Das OVG Münster hat mit Beschluss vom 23.06.2020, Az.: 13 B 695/20.NE in einem Eilverfahren die Kontaktdatenerfassung im Rahmen einer Coronaschutzverordnung als mit der DSGVO konform erklärt.

6. Faxübermittlung wird als Datenschutzverstoß angesehen

Das OVG Lüneburg hat mit Beschluss vom 22.07.2020, Az.: 6 A 211/17 die Übermittlung personenbezogener Daten (konkret: Name, Anschrift, Kfz-Kennzeichen) als Datenschutzverstoß angesehen, da diese Technik keine Verschlüsselungsmöglichkeit bietet. *Ob dies mit dem Fernmeldegeheimnis (§ 88 TKG) vereinbar ist, erscheint zweifelhaft.*

7. Einsichtsrecht Betriebsrat in elektronische Personalakte nur mit Arbeitnehmer-Zustimmung

Das LAG Düsseldorf hat mit Beschluss vom 23.06.2020, Az.: 3 TaBV 65/19 ein Einsichtsrecht des Betriebsrats in die Personalakte eines Mitarbeiters nur mit dessen Zustimmung für rechtmäßig erklärt, da sonst eine Verletzung des allgemeinen Persönlichkeitsrechts droht.

8. Zeiterfassung mittels Fingerabdruck nicht datenschutzkonform

Das LAG Berlin-Brandenburg hat mit Urteil vom 04.06.2020, Az.: 10 Sa 2130/19 der Zeiterfassung mittels Fingerabdruck im Zusammenhang mit einer biometrischen Zeiterfassung eine Absage erteilt. Zwar sei das Verfahren für Zwecke des Beschäftigungsverhältnisses geeignet. Aber es gäbe mildere Mittel (z. B. Chipkartennutzung), so dass eine Interessenabwägung zugunsten des klagenden Beschäftigten ausfiel.

9. Umfassendes Auskunftsrecht (Akteneinsicht) bejaht

Das LG München I hat mit Urteil vom 06.04.2020, Az.: 3 O 909/19 das Auskunftsrecht (Akteneinsicht) nach Art. 15 Abs. 3 DSGVO sehr weit ausgelegt und die (kostenfreie) Bereitstellung sämtlicher personenbezogenen Daten von Art. 15 Abs. 3 DSGVO umfasst gesehen.

10. Keine Kosten für Akteneinsicht im Krankenhaus gegenüber Patienten

Das LG Dresden hat mit Urteil vom 29.05.2020, Az. unbekannt, festgestellt, dass Patienten gemäß Art. 15 DSGVO keine Kosten für eine Akteneinsicht zu tragen. § 630g BGB sah das Gericht nicht als einschlägig an.

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

11. Einsichtsrecht Betriebsrat in Personalakte

Das LAG Düsseldorf entschied am 23.06.2020, Az.: 3 TaBV 65/19, dass der Betriebsrat ohne Zustimmung der betroffenen Arbeitnehmer keine Einsicht in die kompletten elektronischen Personalakten eines Unternehmens bekommen darf.

12. Kein Recht des Betriebsrats auf Aushändigung von Lohnlisten

Der Betriebsrat hat keinen Anspruch auf Aushändigung von Brutto-Lohnlisten, auch nicht um die gleiche Entlohnung von Frauen und Männern im Unternehmen überprüfen zu können. Der Betriebsrat kann lediglich die Einsichtnahme in die Entgeltlisten verlangen und sich dabei Notizen machen zu können, so das LAG München mit Beschluss vom 22.04.2020, Az: 6 TaBV 33/19

13. Arbeitgeber darf nicht allgemein nach Strafverfahren fragen

Arbeitgeber dürfen im Einstellungsverfahren potenzielle neue Mitarbeiter nicht allgemein nach Vorstrafen und laufenden strafrechtlichen Ermittlungsverfahren fragen. Dies ist nur zulässig, wenn Vorstrafen für die Art des zu besetzenden Arbeitsplatzes von Bedeutung sind, so das AG Bonn hat mit Urteil vom 26.05.2020.

14. 3000 € Bußgeld für fehlerhaftes Impressum

Das LG Essen hat mit Urteil vom 03.06.2020, Az.: 44 O 34/19 eine Vertragsstrafe von 3.000 € wegen eines fehlerhaften Impressums (konkret: fehlende Aufsichtsbehörde) als angemessen angesehen, da es sich um keine Bagatelle handelt.

15. Automatisch generierte Facebook-Seite ist rechtswidrig

Eine automatisch generierte, sogenannte nicht-verwaltete Seite, die Facebook generiert hat, ist ohne Zustimmung der betroffenen Firma wegen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb (einer Anwaltskanzlei) rechtswidrig, so das LG Hamburg mit Urteil vom 13.02.2020, Az.: 13 O 372/18.

16. Einschränkung der Rechtsbehelfe

Das VG Regensburg hat mit Urteil vom 06.08.2020, Az.: RN 9 K 19.1061 über die DSGVO hinausgehende Rechtsbehelfe – insbesondere eine allgemeine Leistungsklage in Gestalt einer Unterlassungsklage – aufgrund von Art. 79 DSGVO ausgeschlossen. Im Falle einer bloßen rechtswidrigen Datenverarbeitung ohne Rechtsverletzung steht der betroffenen Person das Beschwerderecht nach Art. 77 Abs. 1 DSGVO und in der Folge das Recht auf gerichtlichen Rechtsbehelf gegen die Aufsichtsbehörde nach Art. 78 Abs. 1 DSGVO zu.

17. DSGVO-Schadensersatz hat ernsthafte Beeinträchtigungen als Voraussetzungen

Das AG Frankfurt/M. hat mit Urteil vom 10.07.2020, Az.: 385 C 155/19 einen DSGVO-Schadensersatz wegen unerlaubtem Datenabfluss wegen nur geringer Beeinträchtigung abgelehnt.

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. Checkliste Patch-Management

Das BayLDA hat eine Checkliste „Patch Management“ veröffentlicht (https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf). Die Handreichung unterstützt kleine und mittlere Unternehmen dabei, festzustellen, wo und wie ein bedarfsgerechtes Aktualisieren der eingesetzten Softwaresysteme durchzuführen ist und ist auch für Freiberufler, Selbstständige und andere Verantwortliche von Nutzen sein.

2. Worauf Berufsgeheimnisträger (z. B. Ärzte) bei Emails achten müssen

Der LfDI Rheinland-Pfalz hat eine aktuelle Stellungnahme veröffentlicht unter welchen Umständen den Berufsgeheimnisträger – wie Ärzte – per Email mit externen Stellen (z. B. Patienten) datenschutzkonform kommunizieren können: Transportverschlüsselung oder ausdrückliche Einwilligung in eine unsichere Kommunikation sind dabei die zentralen Aussagen (https://www.datenschutz.rlp.de/de/themenfelder-themen/e-mail-berufsgeheimnistraeger/).
Seit kurzem funktioniert eine PGP-Verschlüsselung nun auch mit dem Email-Client Thunderbird.

3. Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen

Die DSK hat am 17.07.2020 eine aktuelle Orientierungshilfe zur Videoüberwachung durch nicht-öffentliche Stellen veröffentlicht (https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/VUe-OH-DSK/OH-VUe_DSK-final.pdf).

4. Ersetzendes Scannen

Seit 2013 schafft die TR 03138 (TR-RESISCAN) Rechtssicherheit für papierlose Archive. Um die Implementierung der Technischen Richtlinie zu erleichtern, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Ende Juli eine zusammenfassende Handlungshilfe veröffentlicht (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138-Handlungshilfe.pdf;jsessionid=BBDA774FA1024418373513C6F4C3914A.2_cid500?__blob=publicationFile&v=3).

5. Zoom datenschutzkonform

Der LfDI Baden-Württemberg hat die Verbesserungsbemühungen der Videokonferenzplattform Zoom gewürdigt und die Datenschutzkonformität bestätigt (https://www.baden-wuerttemberg.datenschutz.de/warnung-des-lfdi-wurde-gehoert-zoom-bessert-nach/).

6. Schutzkonzepte für Kinder und Jugendliche in medizinischen Einrichtungen künftig Teil des Qualitätsmanagements

Der Gemeinsame Bundesausschuss hat Schutzkonzepte für Kinder und Jugendliche in medizinischen Einrichtungen künftig als Teil des Qualitätsmanagements definiert (Presseerklärung: https://www.g-ba.de/presse/pressemitteilungen/875/)

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

7. Datenschutz bei Bild-, Ton- und Videoaufnahmen in KiTa's

Die Berliner Datenschutzbehörde hat eine ausführliche Broschüre zum Datenschutz bei Bild-, Ton- und Videoaufnahmen in KiTa's veröffentlicht (file:///Users/markruedlin/Downloads/datenschutz_in_kitas_2020-1.pdf).

8. Aktualisierung der Skripte „IT-Recht" und „Internetrecht"

Die umfassenden Skripte „IT-Recht" und „Internetrecht" des Instituts für Informations-, Telekommunikations- und Medenrecht in Münster wurden der jährlichen Aktualisierung unterzogen (http://vg01.met.vgwort.de/na/cf9f3122789e49d7b4b6e587753c6271?l=https://www.itm.nrw/wp-content/uploads/skript-internetrecht-juli-2020.pdf – IT-Recht; Internetrecht: http://vg01.met.vgwort.de/na/45509f4e0e8a41c9a7cc6f40c4a5854e?l=https://www.itm.nrw/wp-content/uploads/Skript-IT-Recht-Stand-Juni-2020-Stand-29.06..pdf).

9. PimEyes – Gesichter-Suchmaschine

Die Suchmaschine PimEyes des gleichnamigen polnischen Start-Up analysiert massenhaft (900 Mio.) Gesichter im Internet und speichert damit biometrische Daten ohne Rechtsgrundlage ab (https://www.rnd.de/digital/pimeyes-start-up-aus-polen-suchmaschine-fur-gesichter-bereitet-politikern-sorge-CKSGCP4JJHHCTZNRFGHPEVJMG4.html).

10. EU-Datenschutzbeauftragter nimmt Stellung zu Microsoft Produkte

Der EU-Datenschutzbeauftragte – nur zuständig für Organe und Einrichtungen der EU – hat sich kritisch zu Microsoft-Produkten geäußert (https://edps.europa.eu/data-protection/our-work/publications/papers/outcome-own-initiative-investigation-eu-institutions_en):

- Die mit Microsoft seitens der EU geschlossenen Verträge ermöglichen Microsoft teilweise selbst „Herr der Daten" zu sein.
- Die EU hat keine ausreichende Kontrolle hinsichtlich Microsoft als Auftragsverarbeiter, insbesondere über von Microsoft eingesetzte Unter-Auftragsverarbeiter.
- Der Speicherort der Daten sowie internationale Transfers sind unzureichend vertraglich vereinbart, angemessene Sicherheitsvorkehrungen zum Schutz der Daten, die den EU/EWR-Raum verlassen, fehlen.
- Die EU Organe/Einrichtungen wissen nicht genügend über Art, Umfang und Zweck der Verarbeitung und die Risiken für die Betroffenen, um ihren Transparenzverpflichtungen gegenüber den Betroffenen nachkommen zu können.

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