DaSuMed
Datenschutz für medizinische und soziale Einrichtungen
Ausgabe 05/2019

A. Gesetzesinfos

DSAnpUG-EU

Der Bundesrat hat das zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU verabschiedet. Damit werden in über 150 Gesetzen datenschutzrechtliche Anpassungen vorgenommen, zumeist allerdings nur geringe redaktionelle Änderungen. Insbesondere (https://www.bundesrat.de/DE/plenum/bundesrat-kompakt/19/980/980-pk.html?nn=4352766#top-3) wurden die noch nicht geänderten Sozialgesetzbücher angepasst.

B. DSGVO

1. Bußgeldhöhenbemessung

Die Datenschutzaufsichtsbehörden haben sich auf ein gemeinsames Modell zur Berechnung von Bußgeldern geeinigt (https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf).

Die Berechnung erfolgt in fünf Schritten (Originalzitat aus dem Konzept der DSK):

> *Vor diesem Hintergrund erfolgt die Bußgeldzumessung in Verfahren ge-gen Unternehmen in fünf Schritten. Zunächst wird das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt(2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.)und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.).*

Im Ergebnis wird dieses Vorgehen zu einer vermutlich deutlichen Anhebung von Bußgeldern führen.

Inzwischen hat sich jemand die Mühe gemacht und einen Berechnungsgenerator online gestellt (https://www.werning.com/dsgvo-bussgeldrechner/). Die Seite http://www.enforcementtracker.com/ bietet einen Überblick über die (bekannten) Bußgelder und Sanktionen, die europäische Datenschutzbehörden bislang verhängt haben.

2. Neue deutsche Rekordbußgelder

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat ein Bußgeld über fast 200.000 € gegen die Firma Delivery Hero (inzwischen von Takeway aus den Niederlanden übernommen) verhängt. Hintergrund waren eine Vielzahl sich wiederholender Datenschutzverstöße. Beispielsweise bekam eine Person noch 15 Werbe-Emails, obwohl sie einer Zusendung

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

widersprochen hatte (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/presse-mitteilungen/2019/20190919-PM-Bussgelder.pdf).

3. 30.000 € Bußgeld wegen fehlerhaftem Cookie-Banner

Die spanische Aussichtsbehörde der Billigfluggesellschaft Vueling Airlines SA (Vueling) ein Bußgeld in Höhe von 30.000 Euro auferlegt, da diese für die eigene Webseite einen unzureichenden Cookie-Banner verwendet hatte (https://www.aepd.es/resoluciones/PS-00300-2019_ORI.pdf?utm_source=POLITICO.EU&utm_campaign=fc1f5e664f-EMAIL_CAMPAIGN_2019_10_17_04_52&utm_medium=email&utm_term=0_10959edeb5-fc1f5e664f-190359285).

4. FAQ zu Google Fonts, Google Maps, reCAPTCHA, Cookie Banner etc.

Das BayLDA hat eine FAQ-Liste mit kurzen und prägnanten Einschätzungen zu mehr als 100 Einzelfragen veröffentlicht und damit eine klare Positionierung vorgenommen (https://www.lda.bayern.de/de/faq.html). Inwieweit diese Positionen richtig oder gar gerichtsfest sind, ist eine andere Frage.

5. Entscheidungen zum Datenschutzrecht in Österreich

Die österreichischen Datenschutzbehörde hat seit Inkrafttreten der DSGVO zahlreiche Überlegungen zur Interpretation der DSGVO auf den Weg gebracht. Eine Wiener Anwaltskanzlei hat dies zusammengestellt: https://geistwert.at/es-war-einmal-und-was-seither-geschah-oder-oesterreichisches-datenschutzrecht-seit-der-dsgvo-dsg-2018-und-der-liebe-eugh/.

6. Bußgeld für unberechtigte Dateneinsicht eines Polizeibeamten

Der LfDI Baden-Württemberg hat einem Polizeibeamten ein Bußgeld in Höhe von 1.400 € auferlegt, weil er über eine Halterabfragte beim Kraftfahrtbundesamt und eine anschließende SARS-Abfrage bei der Bundesnetzagentur die Mobilfunknummer einer privaten Bekanntschaft ermittelt und diese verwendet hatte. Die unberechtigte Nutzung der Inhalte von Krankenhausinformationssystemen und vergleichbarer Systeme kann vergleichbare Wirkungen auslösen.

C. Urteile und Beschlüsse von Gerichten

1. Das Setzen von Cookies erfordert die aktive Einwilligung des Internetnutzers

Das Setzen von Cookies erfordert die aktive Einwilligung des Internetnutzers, so der EuGH mit Urteil vom 01.10.2019, Az.: C-673/17 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=de&mode=req&dir=&occ=first&part=1&cid=1436279).
Ohne übertrieben komplizierten Begründungsaufwand verweist das Gericht mehr oder weniger klar auf nachvollziehbare Sprache der einschlägigen EU-Normen. Und kommt zu folgenden fünf Ergebnissen:

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

(1) Cookies: Für alle Cookies (die nicht unter die enge Ausnahme nach Art. 5 Abs. 3 Satz 2 der e-Privacy-Richtlinie in der Fassung von 2009 fallen) muss eine aktive Einwilligung über ein Opt-in erfolgen. Sprich: Das Zustimmungshäkchen darf nicht schon vorab gesetzt sein.
(2) Voraussetzung für eine wirksame Einwilligung ist eine klare Information darüber, in was man einwilligt.
(3) Die Cookie-Vorschrift gilt sowohl für Cookies, die personenbezogene Daten speichern, wie für solche, die nur nicht-personenbezogene Daten erfassen. Also für alle Cookies (die nicht unter die enge Ausnahme nach Art. 5 Abs. 3 Satz 2 der ePrivacy-Richtlinie in der Fassung von 2009 fallen).
(4) In den Datenschutzinformationen muss auf jeden Fall auch über die Speicherzeit der Cookies im Browser informiert werden. Und über alle Dritten, an die Daten weitergeleitet werden und deren Verwendungszwecke.
(5) Weil vom deutschen Gericht nicht als Frage vorgelegt, sagt das Urteil ausdrücklich (siehe Randnummer 64) nichts zur Frage, ob ein Angebot (z.B. eine kostenfreie Nutzung einer Website) gekoppelt werden darf an die Einwilligung in ein Cookie (für Werbetracking). Das wird diskutiert unter dem für wirksame Einwilligungen erforderlichem Merkmal „ohne Zwang“ (in der Fachliteratur unter dem Schlagwort „Koppelungsverbot“).

Fazit:

Da viele Besucher der Websites die Einwilligungen nicht erteilen werden, wird sich wahrscheinlich das gesamte System des Onlinemarketings neu aufstellen.

Handlungsbedarf:

Nach diesem Urteil sind alle einfachen Cookie Banner irrelevant. Zugespitzt formuliert: Man kann Websites auch genauso gut ganz ohne ein Banner betreiben.
(1) Jeder Onlinedienst (Website, App, etc.), der mindestens ein Cookie setzt, muss eine Funktion für Cookie Consent anbieten (das ist deutlich mehr als ein herkömmliches Cookie-Banner). Die Einwilligung muss erfolgt sein, BEVOR der Cookie gesetzt wird.
(2) Jeder Cookie muss mit ausreichenden Informationen in den Datenschutzinfos vorgestellt werden.
(3) Für alle Third Party-Cookies müssen – falls nicht bereits vorliegend – (belastbare) Informationen von deren Anbietern zur Verarbeitung der Daten in deren Bereich eingeholt werden. Nur so kann man diese Angaben in die eigene DS-Info aufnehmen. Sprich: Google, Facebook, Oracle und diverse andere Dienstleister, mit denen man zusammenarbeitet, müssen unter Umständen weitere Informationen zur Verfügung stellen.

Der einfache Weg:

Dies ist die große Stunde der Cookie Consent-Tools. Deren Anbieter sollten die notwendigen Informationen zusammentragen, soweit das noch nicht geschehen ist, und über das Consent-Tool anbieten.
Die Betreiber von Websites müssen dann „nur" ein leistungsstarkes Consent-Tool in ihre Seiten einbauen.

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

Und abhängig vom eigenen Geschäftsmodell muss man schauen, wie hart Einbußen dadurch sind, dass bisherige Funktionen zur „zielgruppengerechten“ Ausspielung von Inhalten und Kampagnen nicht mehr möglich ist.

2. Anordnung der Abschaltung einer Facebook-Fanpage

Das BVerwG hat mit Urteil vom 11.09.2019, Az: 6 C 15.18 festgestellt, dass eine Datenschutzaufsichtsbehörde den Betreiber einer Facebook-Fanpage diesen zur Abschaltung derselben verpflichten kann, wenn die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist.

3. Keine weltweite Löschung von Suchmaschinenergebnissen

Der EuGH hat mit Urteil vom 24.09.2019, Az.: C-507/17 den Suchmaschinenbetreiber Google freigestellt vorzunehmende Löschungen weltweit durchzuführen.

4. Einblick des Betriebsrats in Bruttolohnlisten

Das BAG hat mit Beschluss vom 07.05.2019, Az.: 1 ABR 53/17 das Recht des Betriebsrates bestätigt, Einblick in nicht anonymisierte Bruttoentgeltlisten zu nehmen.

5. Teilnahme am Streitbeilegungsverfahren muss hinreichend eindeutig sein

„Die auf einer Webseite und/oder in den Allgemeinen Geschäftsbedingungen eines Unternehmers enthaltene Mitteilung, die Bereitschaft zu einer Teilnahme an einem Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle könne "im Einzelfall" erklärt werden, ist nicht ausreichend klar und verständlich im Sinne des § 36 Abs. 1 Nr. 1 VSBG,“ so der BGH mit Urteil vom 21.08.2019, Az.: VIII ZR 265/18.

6. Bei Löschungen auch an Google Cache denken

Das OLG Frankfurt/M. hat mit Urteil vom 22.08.2019, Az.: 6 U 83/19 eine Haftung für eine, aufgrund einer Unterlassungserklärung vorgenommenen Löschung von Inhalten auch auf Inhalte, die noch im Google-Cache zu finden sind, ausgeweitet. Denn über „Google Search Console“ hatten sich zu löschende Inhalte auch zeitgleich bei Google löschen lassen.

7. Arbeitnehmer-Schadensersatz bei unzulässiger Videoüberwachung

Das LAG Rostock hat mit Urteil vom 24.05.2019, Az.: 2 Sa 214/18 einem Angestellten einen Schadensersatz in Höhe von 2.000 € aufgrund einer unzulässigen Videoüberwachung zugesprochen.

8. Betriebsratsvorsitzende kann auch Datenschutzbeauftragte sein

Das Sächsische Landesarbeitsgericht hat mit Urteil vom 19. August 2019, Az.: 9 Sa 268/18 die stark diskutierte Frage entschieden, dass eine Betriebsratsvorsitzende auch Datenschutzbeauftragte sein kann und kein Interessenskonflikt zwischen diesen Tätigkeiten vorliegt. Das Bundesarbeitsgericht hatte dies bereits mit Urteil vom 23.03.2011, Az.: 10 AZR 562/09 für einfache Betriebsratsmitglieder attestiert.

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

9. Kein Schadensersatz bei Email-Versand von personenbezogenen Daten mittels Email mangels Schaden

Das AG Bochum hat mit Beschluss vom 11.03.2019 - Az.: 65 C 485/18 eine Schadensersatz mangels Schaden in einem Fall ausgeschlossen, in dem ein Betreuer seine Bestellungsurkunde per Email an eine dritte Stelle gesandt hatte.

10. Persönlichkeitsrechtsverletzung durch nicht-anonymisierte Nutzung von Google Analytics

Das LG Dresden hat mit Urteil vom 11.01.2019, Az.: 1a O 1582/18 die nicht anonymisierte Übermittlung der IP-Adresse von Webseitenbesucher an Google mittels Einbindung des Tracking-Werkzeugs Google Analytics als Verletzung des allgemeinen Persönlichkeitsrechts gewertet.

11. Immaterieller Schadensersatz wegen Datenschutzverstoß

Das LG Feldkirch hat in einem nicht rechtskräftigen Urteil die österreichische Post gemäß Art. 82 DSGVO zu einem immateriellen Schadensersatz verurteilt, diese die Parteiaffinität von Millionen Kunden rechtsgrundlos berechnet und gespeichert hat (https://www.addendum.org/datenhandel/schadenersatz/).

12. Zeitliche Reichweite einer Einwilligung der Eltern für mittlerweile volljährige Tochter

Das LG Frankfurt/M. hat mit Urteil vom 29.08.2019, Az.: 2-03 O 454/18 entschieden, dass eine erneute Veröffentlichung einer zum Zeitpunkt der Berichterstattung Minderjährigen 19 Jahre nach der Erstveröffentlichung nicht bereits dadurch gerechtfertigt, dass die Anfertigung und Veröffentlichung des Fotos in mit Einwilligung des Vaters der Betroffenen erfolgte. Liegt keine eigene Einwilligung der 19-jährigen vor, hat sie selbst noch keine sie bindende Entscheidung hinsichtlich der Veröffentlichung getroffen.

13. Interne Vermerke unterliegen nicht dem Auskunftsrecht

Das AG München hat mit Urteil vom 04.09.2019, Az.: 155 C 1510/18 für interne Vermerke einen Auskunftsanspruch verneint.

D. Sonstiges

1. Aus für Google Analytics?

Das BayLDA hat ein Bußgeldverfahren für den Einsatz von Google Analytics, Google Double Click und Criteo auf Rechtsgrundlage des berechtigten Interesses mit Widerspruchsmöglichkeit eingeleitet. Dies würde dazu führen, dass für die Verwendung der vorgenannten Verfahren Einwilligungen einzuholen wären, was aller Wahrscheinlichkeit nach unrealistisch ist.

→ Verwender von Google Analytics und Co. Sollten prüfen, ob sie auf ein Einwilligungsverfahren umstellen oder auf ein anderes, bei ihnen selbst gehostetes Tracking-Tool umsteigen wollen.

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

2. Microsoft Office 365 grundsätzlich datenschutzkonform einsetzbar

Das niederländische Ministerium für Justiz und Sicherheit hat eine (neue) Datenschutzfolgenabschätzung zu Microsoft Office 365 (für das Produkt „Pro Plus Version 1905“) veröffentlicht und kam zu dem Ergebnis, dass eine Verwendung grundsätzlich datenschutzkonform möglich ist (https://www.government.nl/documents/publications/2019/07/22/dpia-office-365-proplus-version-1905). Allerdings wurden die mobilen Anwendungen und Web-Zugänge für MS Office 365 wurden in einer gesonderten Prüfung als datenschutzrechtlich unzulässig erachtet (https://www.government.nl/documents/publications/2019/07/23/dpia-microsoft-office-365-online-and-mobile-slm-rijk-23-july). Der Hessische Beauftragte für Datenschutz und Informationssicherheit hatte hingegen am 15.07.2019 in einer Stellungnahme den Einsatz an hessischen Schulen untersagt. Ein rechtssicherer Einsatz ist somit nicht feststellbar.

3. BSI erkennt Cyber-Sicherheitsstandard für Krankenhäuser an

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Eignung eines branchenspezifischen Sicherheitsstandards (B3S) festgestellt, mit dem Krankenhäuser ihre IT-Sicherheitsmaßnahmen nach dem Stand der Technik ausrichten können. Vorgelegt wurde der B3S von der DKG (Deutschen Krankenhausgesellschaft) - https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/B3S-Krankenhaeuser_231019.html. Der Standard ist abrufbar unter: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf.

4. Bundesärztekammer mit Standard-Informationen

Auf der Seite https://www.bundesaerztekammer.de/recht/aktuelle-rechtliche-themen/datenschutzrecht/ stellt die Bundesärztekammer Standard-Informationen zum Datenschutz und zur Schweigepflicht bereit.

5. Patientendaten ungeschützt im Netz

Sicherheitsforscher haben Millionen von Patientendaten ungesichert auf Servern im Netz entdeckt (https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_DE.pdf).

6. Britische Studie zum weltweiten Stand des Datenschutzes und staatlicher Überwachung

Das britischen Unternehmen Comparitech hat in einer Studie den Datenschutz und den Überwachungszustand in 47 Ländern untersucht (https://www.comparitech.com/blog/vpn-privacy/surveillance-states/).

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