AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Sept./Okt. 2018 | Seite 1

www.aok-verlag.info/ds-im-blick

INHALT

Neues Datenschutzrecht in den Kirchen

Nicht nur im weltlichen Bereich kamen für Gesundheitseinrichtungen mit der Europäischen Datenschutzgrundverordnung (DSGVO) neue Herausforderungen. Auch im kirchlichen Bereich hat sich einiges geändert.

Dr. Sebastian Ertel

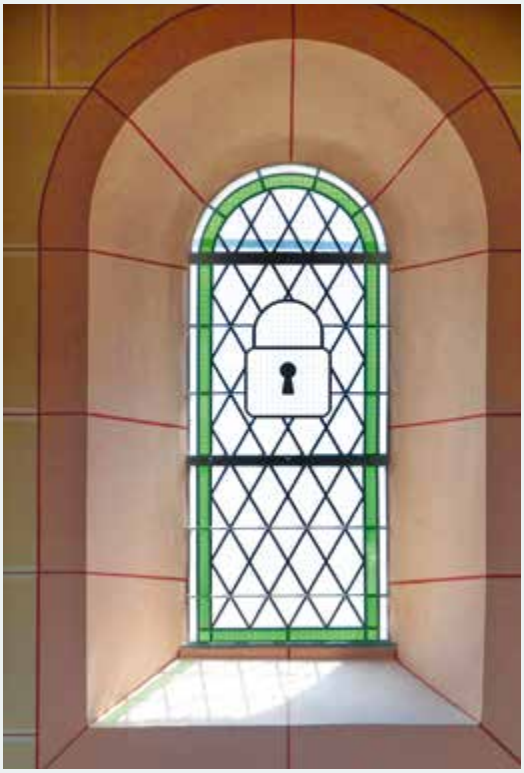
In der Katholischen Kirche wurde die Anordnung über den Kirchlichen Datenschutz (KDO) durch das Gesetz über den Kirchlichen Datenschutz (KDG) abgelöst. In der Evangelischen Kirche besteht weiterhin das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD), dieses wurde aber inhaltlich komplett überarbeitet.

Seit dem 24.5. alles neu

KDG und DSG-EKD traten am 24.5.2018 in Kraft, also einen Tag vor dem Anwendungsbeginn der DSGVO. Hintergrund ist Art. 91 DSGVO, der die (fortbestehende) Selbstverwaltung der Kirche in datenschutzrechtlichen Angelegenheiten regelt. Voraussetzung: Zum Start der DSGVO (25.5.) mussten kirchliche Regelungen, die im Einklang mit der DSGVO stehen, bestehen.

Vieles neu, wenig anders

Damit die kirchlichen Regelungen im Einklang mit der DSGVO stehen, mussten sich diese stark annähern. Gleichwohl wurden verschiedene Sonderregelungen geschaffen, die in Teilbereichen der Berücksichtigung kirchlicher Aspekte Rechnung tragen. Während die DSGVO eine zweijährige Umstellungsfrist vorsah, war diese im kirchlichen Datenschutzrecht etwas länger als ein halbes Jahr. Daher wurden für viele spezialgesetzliche Regelungen (Patientendatenschutzordnung, Schuldatenschutzordnung) Übergangsfristen geschaffen. Diese Regelungen gelten je nach Diözese/Gliedkirche bis Mitte 2019 fort, müssen aber im Lichte von KDG bzw. DSG-EKD ausgelegt werden. Diese Fristen sollen den kirchlichen Gesetzgebern die Möglichkeit einräumen, neue Spezialregelungen zu erlassen.



Datenschutzbeauftragter

In der Katholischen Kirche haben Diözesen, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbände, unabhängig von der Anzahl der datenverarbeitenden Personen, einen Datenschutzbeauftragten zu bestellen. Für alle sonstigen Einrichtungen (z. B. Caritasverbände) muss ein Datenschutzbeauftragter nur bestellt werden, wenn mindestens zehn Personen ständig personenbezogene Daten verarbeiten oder, unabhängig von der Anzahl der datenverarbeitenden Personen, sensible Daten verarbeitet werden. Letzteres ist in der Evangelischen Kirche das einzige maßgebliche Kriterium (mindestens 10 Personen oder sensible Daten).

Rechtmäßigkeit der Verarbeitung

In der DSGVO sind in Art. 6 Abs. 1 DSGVO insgesamt sechs Möglichkeiten für eine rechtmäßige Datenverarbeitung aufgeführt. Das KDG kennt sieben und das DSG-EKD acht Möglichkeiten. Grundsätzlich sind sich diese sehr ähnlich. Zwei Besonderheiten sollen dennoch hervorgehoben werden: Einerseits kann eine Datenverarbeitung rechtmäßig sein, wenn diese zur Erfüllung einer rechtlichen Verpflichtung, der die kirchliche Stelle unterliegt, erforderlich ist (§ 6 Nr. 6 DSG-EKD) bzw. die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im kirchlichen Interesse liegt (§ 6 Abs. 1 lit. f KDG). Welche Fallkonstellationen hiervon umfasst sind und welche Relevanz die Regelungen haben, wird sich wohl erst in der Praxis zeigen.

Andererseits berechtigt sowohl Art. 6 Abs. 1 S. 1 lit. f DSGVO als auch § 6 Abs. 1 lit. g KDG zur Datenverarbeitung, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Die entsprechenden Regelungen des DSG-EKD stellen hier nur auf den Dritten ab: „die Verarbeitung ist zur Wahrung der berechtigten Interessen eines Dritten erforderlich“. Eigene berechtigte Interessen des Verantwortlichen können daher nicht die Grundlage einer Datenverarbeitung sein. Relevant könnte dies für den Bereich der Werbung sein. Die personalisierte Bewerbung neuer Leistungen einer Pflege- oder Gesundheitseinrichtung liegt im Eigeninteresse und wäre nach dem DSG-EKD wohl nicht realisierbar.

Einwilligung

Auch im Bereich der Einwilligung in eine Datenverarbeitung gibt es Besonderheiten. Während DSGVO (Art. 7 Abs. 1) und DSG-EKD (§ 11 Abs. 1) keine Formerfordernisse fordern, verlangt das KDG (§ 8 Abs. 2) grundsätzlich die Schriftform. Sofern eine Einwilligung von Minderjährigen in Bezug auf Dienste der Informationsgesellschaft eingeholt werden soll, kann der Minderjährige die Erklärung selbst abgeben, wenn er das sechzehnte Lebensjahr vollendet hat (Art. 8 Abs. 1 DSGVO, § 8 Abs. 8 KDG) bzw. religionsmündig (14. Lebensjahr – § 5 Gesetz über die religiöse Kindererziehung) ist (§ 12 DSG-EKD). In allen anderen Fällen bedarf es grundsätzlich der Einwilligung der Erziehungsberechtigten. Eine nicht explizit genannte Ausnahme besteht, wenn der Betroffene Beratungshilfe (Beratungsleistung bei sexueller oder sonstiger Gewalt) über das Internet in Anspruch nimmt und die Einholung der Einwilligung der Erziehungsberechtigten nicht zumutbar ist (sexueller Missbrauch durch einen oder beide Erziehungsberechtigte).

Informationspflichten

Der Grundsatz der Transparenz der Datenverarbeitung findet sich auch in den neuen kirchlichen Datenschutzgesetzen wieder. Auch hier wird zunächst davon ausgegangen, dass die Information über die konkrete Datenverarbeitung „bei Erhebung“ erfolgen muss. Allerdings gibt es im Gegensatz zur DSGVO einige Ausnahmen. So muss eine unmittelbare Information beispielsweise dann nicht erfolgen, wenn diese „einen unverhältnismäßigen Aufwand erfordern würde (§ 17 Abs. 4 DSG-EKD) und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere wegen des Zusammenhangs, in dem die Daten erhoben wurden, als gering anzusehen ist (zusätzlich § 15 Abs. 4 KDG)“. Eine solche Fallgestalt liegt beispielsweise vor, wenn die Datenerhebung infolge eines telefonischen Erstkontaktes erfolgt und die Datenverarbeitung keine erwähnenswerten Besonderheiten mit sich bringt (eine relevante

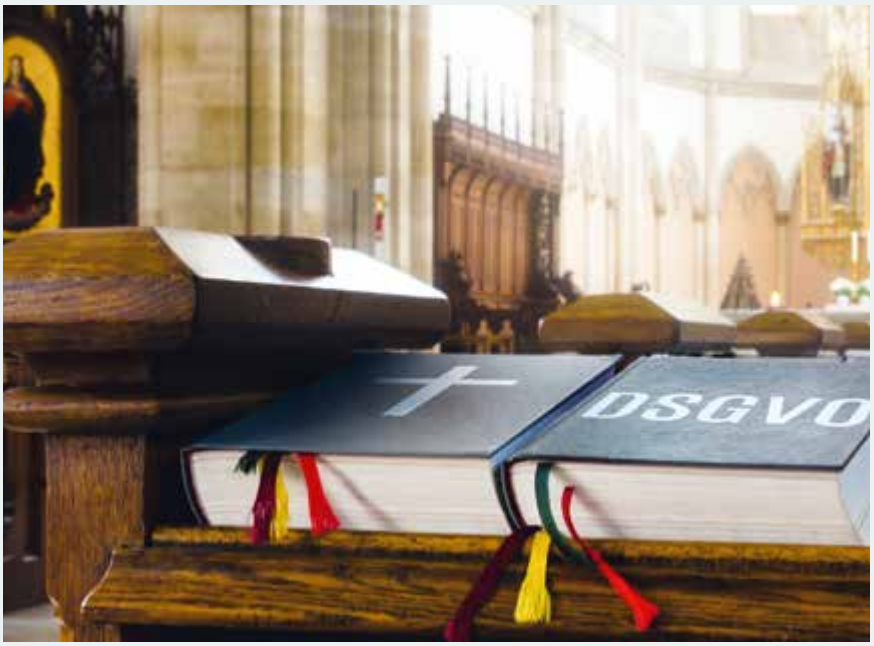
Besonderheit wäre beispielsweise der Datentransfer in die USA, mehrere verantwortliche Stellen, Profiling). In diesen Fällen genügt es, wenn die Informationen nachgereicht werden. Zum Teil wird auch vertreten, dass in diesen Fällen die Informationspflicht gänzlich entfallen kann. Das KDG sieht zudem vor, dass die Informationspflicht zurücktreten muss, wenn Dritte ein überwiegendes Geheimhaltungsinteresse vorweisen können oder durch die Auskunft die Wahrnehmung des Auftrags der Kirche gefährdet wird (§ 15 Abs. 5 KDG).

Auftragsverarbeitung

Ein im Anwendungsbereich der DSGVO äußerst umstrittener Punkt betrifft den ehemaligen § 11 Abs. 5 Bundesdatenschutzgesetz (BDSG). Nach diesem war eine Auftragsverarbeitung auch dann gegeben, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Eine entsprechende Regelung findet sich weder in Art. 28 DSGVO noch im BDSG-neu. Die Folge: Die Anwendung der Voraussetzungen des Art. 28 DSGVO bei Prüfungs- oder Wartungsdienstleistungen ist stark umstritten (nach Ansicht der Landesdatenschutzbeauftragen aber wohl gegeben). Einfacher ist es hier für die kirchlichen Einrichtungen: Eine dem § 11 Abs. 5 BDSG-alt entsprechende Regelung findet sich in den § 29 Abs. 12 KDG und § 30 Abs. 6 DSG-EKD.

Dafür müssen kirchliche Einrichtungen mit anderen Problemen kämpfen. Diese treten immer dann auf, wenn sie sich weltlicher Dienstleister bedienen. Letztere weigern sich häufig, die entsprechenden kirchlichen Verträge zur Auftragsverarbeitung zu unterzeichnen. Die Diözesandatenschutzbeauftragten bzw. die Datenschutzbeauftragten der Evangelischen Kirche akzeptieren grundsätzlich den DSGVO-Vertrag, wenn dieser einen kirchenspezifischen Annex beinhaltet:

- Der Auftragnehmerin ist bekannt, dass die Auftraggeberin dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)/Gesetz über den Kirchlichen Datenschutz (KDG) unterliegt. Sie bestätigt die Kenntnis dieser Regelungen und deren Beachtung.



Umfasst die Auftragsverarbeitung Gesundheitsdaten muss ferner darauf geachtet werden, dass entsprechende Ausführungen zu § 203 Strafgesetzbuch mit aufgenommen sind. Da sich solche regelmäßig nicht in den Standardverträgen finden, können diese über den Annex mit aufgenommen werden.

Geldbußen

Verfehlungen kirchlicher Einrichtungen können nunmehr mit Geldbußen bis 500.000 Euro geahndet werden (§§ 45 Abs. 4 DSG-EKD, 51 Abs. 5 KDG). Dabei reduziert sich die Anzahl der Unternehmen, gegen die ein Bußgeld verhängt werden kann, in der katholischen Kirche erheblich. Nach § 51 Abs. 6 KDG darf eine Geldbuße nur gegen die Institutionen verhängt werden, die am Wettbewerb teilnehmen. Für Generalvikariate, Ordinariate, Kirchengemeinden und pastorale Räume werden daher datenschutzrechtliche Vergehen nicht bußgeldsanktioniert. Eine derartige Differenzierung sieht das DSG-EKD nicht vor.

Rechtsweg

Der von einer Beanstandung der Datenschutzaufsicht betroffenen Stelle stehen nunmehr auch Rechtsbehelfe zur Verfügung. In der Evangelischen Kirche steht hierzu der Rechtsweg zu den kirchlichen Verwaltungsgerichten zur Verfügung, dem zum Teil ein Widerspruchsverfahren vorausgehen muss (§ 47 DSG-EKD). In der Katholischen Kirche wurde eine eigene Gerichtsbarkeit geschaffen und eine Kirchliche Datenschutzgerichtsordnung (KDSGO) erlassen. Diese sieht einen Zwei-Instanzen-Zug vor. Ein Vorverfahren ist hier nicht erforderlich.

Der NEUE Datenschutz im Gesundheitswesen

Broschüre HIER bestellen

Europäische Datenschutz-Grundverordnung, ein ganz neues BDSG und unzählige novellierte Datenschutzvorschriften auf Bundes- und Landesebene – ab Mai 2018 wird die datenschutzrechtliche Landschaft in Europa und hierzulande eine grundlegend andere sein.

Die Broschüre soll Datenschutzverantwortlichen in Gesundheitseinrichtungen eine Hilfestellung an die Hand geben, sich in das neue Recht einzuarbeiten und die Datenverarbeitung in Gesundheitseinrichtungen auch künftig rechtskonform zu gestalten. Das Fachbuch vermittelt die neuen gesetzlichen Grundlagen, führt praxisnah in die Datenschutzorganisation einer Gesundheitseinrichtung ein und erläutert am Beispiel des Krankenhauses die zentralen rechtlichen Herausforderungen für Datenschutzverantwortliche.

Neben dem Datenschutz wird dabei auch das neue und zunehmend wichtigere Recht der IT-Sicherheit beleuchtet.

Broschüre DIN A5, ca. 380 Seiten
Preis: 89,90 € pro Stück inkl. MwSt. und versandkostenfreier Zusendung im Inland
Art. Nr.: 43100 | **ISBN: 978-3-553-43100-2**

Aus dem Inhalt (Auszug):

- **A – Rechtliche Grundlagen**
  DS-GVO, neues BDSG und Auswirkungen für den Gesundheitsdatenschutz
- **B – Datenschutzorganisation**
  Praktische Umsetzung der DS-GVO in Gesundheitseinrichtungen durch den Datenschutzbeauftragten
- **C – Datenschutz im Krankenhaus**
  Patientendatenschutz im Betriebsgeschehen sicherstellen
- **D – Der Internetauftritt**
  Internetauftritt und Social Media-Plattformen rechtssicher ausgestalten
- **E – Datensicherheit**
  Rahmenvorschriften zur IT-Sicherheit und bereichsspezifische Vorgaben für den Gesundheits- und Medizinbereich

AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215 | Mail fachinfo@aok-verlag.de
Jetzt Broschüre bestellen unter: aok-verlag.info/de/der-neue-datenschutz-im-gesundheitswesen

Der Webauftritt in Zeiten der DSGVO

Seit gut drei Monaten ist die Europäische Datenschutzgrundverordnung (DSGVO) nun wirksam. Bereits im Vorfeld haben viele Unternehmen und Gesundheitseinrichtungen ihren Internetauftritt überarbeitet. Doch nicht nur die DSGVO hat zu Anpassungsbedarf geführt.

Sven Venzke-Caprarese

Insbesondere eine Positionsbestimmung der Aufsichtsbehörden aus April 2018 zum Einsatz von Trackingtools sowie eine im Juni dieses Jahres ergangene Entscheidung des Europäischen Gerichtshofs zum Betrieb von Fanpages bei Facebook haben Auswirkungen auf Websitebetreiber. Die rechtlichen Rahmenbedingungen für Websitebetreiber sind insgesamt strenger geworden. Die im Vorfeld der DSGVO von einigen Websitebetreibern befürchteten Abmahn- und Klagewellen sind bis jetzt allerdings ausgeblieben. Dennoch kann es nicht schaden, sich als Websitebetreiber auch hier auf dem aktuellen Stand zu halten. Nicht zuletzt, weil die Webseite das Aushängeschild der Einrichtung ist.

Der folgende Beitrag gibt einen kurzen Überblick über die wichtigsten Punkte.

Anpassungsbedarf durch die DSGVO

Gesundheitseinrichtungen, die bisher einen rechtskonformen Internetauftritt betrieben haben, müssen im Hinblick auf die DSGVO insbesondere ihre Datenschutzerklärung um die Pflichtangaben des Art. 13 DSGVO ergänzen. Neben der Angabe der Kontaktdaten der verantwortlichen Stelle und eines etwaigen Datenschutzbeauftragten fordert Art. 13 DSGVO einen Hinweis auf die Betroffenenrechte sowie auf das Beschwerderecht bei einer Aufsichtsbehörde.

Daneben müssen gem. Art. 13 DSGVO für einzelne Datenerhebungen unter anderem Zweck, Rechtsgrundlage, Speicherdauer, Datenempfänger und etwaige Widerrufsrechte angegeben werden. Dies betrifft z. B. den Umgang mit IP-Adressen, den Einsatz von Trackingtools, die Nutzung von Kontaktformularen und Newsletteranmeldeboxen, die Bereitstellung von Login-Bereichen und Bewerberplattformen etc.

Im Hinblick auf den Internetauftritt müssen zudem weitere Anpassungen vorgenommen werden, die jedoch für Besucher nicht nach außen sichtbar sind. So müssen die mit dem Internetauftritt zusammenhängenden Verfahren in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO aufgenommen und Verträge mit etwaigen Dienstleistern, z. B. in den Bereichen Hosting und Newsletterversand, gem. Art. 28 DSGVO angepasst werden.

Positionsbestimmung der Aufsichtsbehörden aus April 2018 zum Einsatz von Trackingtools

Vor allem der Einsatz von Trackingtools stellte Websitebetreiber in der Vergangenheit vor große Herausforderungen. Zumindest die Verwendung von Trackingtools, die der reinen Messung der eigenen Besucher durch den Websitebetreiber selbst oder seine Auftragsverarbeiter dienten, schien allerdings geklärt. Wollten Gesundheitseinrichtungen z. B. Trackingtools wie Google Analytics in der Standardimplementierung oder Matomo (ehemals

Piwik) nutzen, um Informationen über die Nutzung ihrer Seite zu erhalten, so konnte als Rechtsgrundlage § 15 Abs. 3 Telemediengesetz herangezogen werden. Dies bedeutete, dass die entsprechenden Trackingtools auch ohne Einwilligung der Websitebesucher verwendet werden durften, wenn das Tracking nur anhand von Pseudonymen und mit anonymisierter IP-Adresse erfolgte und ein Hinweistext in der Datenschutzerklärung mit wirksamer Opt-Out-Möglichkeit aufgenommen wurde.

Die Irritation war daher groß, als am 26. April 2018 eine Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zu dem Schluss kam, dass *„die §§ 12, 13, 15 TMG bei der Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen, ab dem 25. Mai 2018 nicht mehr angewendet werden“ können und es „… jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking Mechanismen [bedarf], die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen“.*

Auch wenn diese Ansicht der Aufsichtsbehörden durchaus kritisiert werden kann, da sie die Möglichkeit des Einsatzes von Google Analytics, Matomo und ähnlichen Trackingtools auf Basis von Art. 6 Abs. 1 lit. f DSGVO (Interessenabwägung) auszuschließen scheint, sollten Websitebetreiber den Einsatz entsprechender Tools durch eine Einwilligung der Nutzer abdecken, um rechtliche Risiken zu vermeiden. In der Praxis bedeutet dies häufig, dass Websitebetreiber entsprechende Einwilligungsbanner vorschalten müssen. Die Anforderungen an solche Banner sind rechtlich jedoch kaum geklärt. Reicht es aus, ein Banner vorzuschalten, welches jede weitere Nutzung der Website als konkludente Einwilligung wertet? Oder muss das Banner dem Nutzer die Wahl bieten, sich ausdrücklich für oder gegen ein Tracking zu entscheiden? Rechtssicherer erscheint die letztere Alternative, wobei das Tracking tatsächlich erst beginnen sollte, wenn sich der Nutzer aktiv für ein solches entscheidet. Dabei sollte auf eine Kopplung der Einwilligungserteilung an die Möglichkeit des weiteren Websitebesuchs verzichtet werden. Der Nutzer sollte sich tatsächlich frei entscheiden können.

Klarheit wird an dieser Stelle vermutlich erst die derzeit auf EU-Ebene geplante und heftig diskutierte E-Privacy-Verordnung bringen. Diese wird jedoch voraussichtlich frühestens im Jahr 2020/2021 wirksam werden, da noch nicht einmal Einigkeit über den Verordnungstext hergestellt werden konnte und zudem mit einer Umsetzungsfrist von zwei Jahren zu rechnen ist.

Abmahnungen und Schadensersatzansprüche Betroffener

Die von einigen Websitebetreibern im Vorfeld der DSGVO befürchtete Abmahnwelle ist bis jetzt zum Glück ausgeblieben. Gleiches gilt für Klagen betroffener Personen nach Art. 82 DSGVO. Dennoch gab es einige Vorfälle, die es zu medialer Aufmerksamkeit gebracht haben und die Websitebetreiber im Blick behalten sollten:

- Abmahnung wegen der Nutzung von Google Analytics ohne Einwilligung: Kurz nach dem 25. Mai häuften sich Abmahnungen wegen des Einsatzes von Google Analytics ohne Opt-In und es kam zu entsprechenden Berichterstattungen. Im Ergebnis nutzte diese Abmahnung die bereits in diesem Newsletter dargestellte rechtliche Unsicherheit, die seit der entsprechenden Positionsbestimmung der Aufsichtsbehörden besteht. Dabei ist es fraglich, ob solche Abmahnungen im Hinblick auf Datenschutzverletzungen nach der DSGVO überhaupt zulässig sind und ob eine entsprechende Einbindung von Google Analytics tatsächlich einen Verstoß gegen die DSGVO darstellt. Zumindest im Fall eines betroffenen Apothekers konnte die Abmahnung diesem Bericht zufolge zurückgewiesen werden.
- Abmahnung wegen der Einbindung externer Schriftarten ohne Anpassung der Datenschutzerklärung: Eine weitere Abmahnung, die es

zu einer gewissen Aufmerksamkeit in der Berichterstattung brachte, wendete sich gegen die Einbindung externer Schriftarten in Websites. Betroffen waren insbesondere Websites, die Google Fonts von externen Quellen wie fonts.googleapis.com und fonts.gstatic.com nachluden. Auch hier stellt sich neben der Frage der Zulässigkeit der Abmahnung an sich die Frage, ob eine solche Nutzung tatsächlich einen Datenschutzverstoß darstellt. Websitebetreiber, die diese Rechtsunsicherheit vermeiden wollen, sollten nur lokale Webfonts nutzen, was übrigens auch im Hinblick auf Google Fonts möglich ist.

- Nutzung eines unverschlüsselten Kontaktformulars: Neben Abmahnversuchen schaffte es auch die Zahlungsaufforderung eines Betroffenen in die Berichterstattung. Gefordert wurde Schadensersatz in Höhe von 12.500 Euro für „persönliches Leid" als immateriellen Schaden, der durch die Nutzung eines unverschlüsselten Kontaktformulars entstanden sei. Ob ein solcher Anspruch vor Gericht Bestand hätte, ist trotz Art. 82 DSGVO höchst fraglich.

Urteil des Europäischen Gerichtshofs zum Betrieb von Fanpages bei Facebook

Mit Urteil vom 5. Juni 2018 hat der Europäische Gerichtshof entschieden, dass nicht nur Facebook, sondern auch der Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage ein für die Verarbeitung Verantwortlicher ist. Der EuGH geht dabei von einer gemeinsamen Verantwortung zwischen Facebook und Websitebetreiber aus, wobei „der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist". Zur Sprache kommen in dem Urteil insbesondere die Möglichkeiten des Fanpagebetreibers, demografische Daten über seine Besucher abzufragen sowie verhaltens- und interessenbasierte Werbung zu schalten. Kritisiert werden aber auch die von Facebook erstellten Besucherstatistiken, die dem Fanpagebetreiber zwar in anonymisierter Form angezeigt werden, deren Erstellung jedoch im Vorfeld anhand personenbezogener Daten erfolge.

Mit einer Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6. Juni 2018 reagierten die Aufsichtsbehörden und stellten Anforderungen an den Betrieb einer Fanpage auf - verkürzt dargestellt sind folgende Punkte erforderlich:

- Transparente Information über die Datenverarbeitung durch den Fanpagebetreiber und durch Facebook.
- Einwilligung des Nutzers in personenbezogenes Tracking.
- Abschluss einer Vereinbarung zur gemeinsamen Verantwortlichkeit.

Im Ergebnis muss festgestellt werden, dass es derzeit unklar ist, ob und ggf. wie eine Facebook Fanpage rechtskonform betrieben werden kann: Der Abschluss einer Vereinbarung nach Art. 26 DSGVO (gemeinsame Verantwortung) ist erforderlich, wird dem Fanpagebetreiber ohne die Mitwirkung von Facebook allerdings kaum möglich sein. Auch die Einholung einer Einwilligung in Verarbeitungen, die Facebook durchführt und auf die der Fanpagebetreiber keinen Einfluss hat (die er ggf. sogar noch nicht einmal kennt), wird dem Fanpagebetreiber nicht möglich sein.

Fanpagebetreiber, die sich diesem Risiko bewusst sind und dennoch eine Fanpage betreiben wollen, sollten mindestens eine eigene Datenschutzerklärung auf der Fanpage bereithalten, die auch über die o.g. Umstände informiert. Targetingmechanismen für Werbung, welche die Social Media Plattform bereitstellt und die auf Trackingdaten beruhen, sollten nicht genutzt werden (z. B. Werbung anhand von Interessen, Verhalten, Aufenthaltsorten, demografischen Merkmalen etc.). Insgesamt ist an dieser Stelle der weitere Verfahrensgang vor dem Bundesverwaltungsgericht zu beobachten.

Fazit

Der Betrieb einer Internetpräsenz wird in Zeiten der DSGVO nicht einfacher. Im Gegenteil. Viele zentrale Punkte sind mit neuen Rechtsunsicherheiten belastet und erfordern eine umsichtige Gestaltung.

Vertiefungshinweise:
Mehr Informationen zum datenschutzkonformen Betrieb einer Klinik-Website finden Sie in Kapitel D (Der Internetauftritt) des Fachbuchs

„Der NEUE Datenschutz im Gesundheitswesen“, AOK-Verlag GmbH, Remagen,
ISBN 978-3-553-43100-2

Ein Jahr nach der Bundestagswahl befindet sich ein neues E-Health-Gesetz in Vorbereitung. Neben einer Bewertung des bislang geltenden Gesetzes stellt sich die Frage nach den Wünschen und Erfordernissen an das neue Gesetz. Diese Fragen stehen im Fokus der hochkarätig besetzten Veranstaltung, zu der über 200 Teilnehmer aus allen Bereichen der Gesundheitswirtschaft erwartet werden.

Auszüge aus dem Programm:

- Keynote von Martin Litsch Vorstand des AOK Bundesverbandes
- Gelebte Realitäten in der Versorgung - Gesundheitsakten, Portale & Vernetzungslösungen:
- Verschiedene Player des Gesundheitswesens stellen Ihre Ansätze und Lösungen vor.
- Wieviel eHealthgesetz 2.0 braucht das Land? Mitglieder des Bundestages und Experten aus
- Wissenschaft und Versorgungspraxis besetzen die hochkarätige Diskussionsrunde.
- Workshop am 2. Tag: DGSVO – Datenschutz im Gesundheitswesen - Stigma vs. Chance

Weitere Informationen zum Programm und zu den Referenten sowie unserer Online-Anmeldung finden Sie unter:
www.gevko.de/de/symposium/

Kurznotiz:

Kriterienkatalog für den Wettbewerb „Deutschlands Beste Klinik-Website“ angepasst

Der unter der Schirmherrschaft von Novartis Pharma stehende Wettbewerb um Deutschlands Beste Klinik-Website war bereits im Jahr 2016, 2017 und 2018 Thema unseres Newsletters, da wir die zehn erstplatzierten Websites im Anschluss des Wettbewerbs jeweils einem kurzen Datenschutz-Check unterzogen. Unseren Check im letzten Jahr beendeten wir mit dem Worten: „Als Blick in die Zukunft wäre es wünschenswert, wenn auch datenschutzrechtliche Gesichtspunkte der Konzeptionierung einer Website bei der Wahl der Top 10 Klinik-Websites künftig Berücksichtigung fänden. Denn sowohl dieser als auch der Vorjahres-Datenschutz-Check zeigen, dass selbst große Klinik-Websites teilweise noch Verbesserungsbedarf aufweisen.“ Ein Blick in den Kriterienkatalog des diesjährigen Wettbewerbs zeigt, dass das Thema Datenschutz mittlerweile aufgenommen wurde. Unter Ziffer 14 findet sich das Kriterium: “Juristische Betrachtung, wie Einhaltung des Telemediengesetzes und die Anpassung an die Datenschutz-Grundverordnung“. Man darf gespannt sein, welche Bedeutung dieser Aspekt bei der Wahl 2019 spielt.