AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe April/Mai 2019 | Seite 1

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

INHALT

SEITE 1
Deutschlands beste Klinik-Websites: Vierter Datenschutz-Check

SEITE 5
Interdisziplinäre Videokonferenzen

SEITE 7
Kurznotiz:
Erste Details zum Recht auf kostenlose Kopie von Seiten der Aufsichtsbehörde

Deutschlands beste Klinik-Websites: Vierter Datenschutz-Check

Im Januar 2019 wurde nunmehr zum 16. Mal der Award für „Deutschlands Beste Klinik-Website“ vergeben. Der jährliche Wettbewerb wird von Prof. Frank Elste (DHBW Mosbach) geleitet und steht unter der Schirmherrschaft von Novartis. Wie in den letzten drei Jahren auch haben wir die zehn erstplatzierten Websites im Anschluss einem eigenen Check unterzogen und dabei geprüft, wie es um den Datenschutz der Klinik-Websites steht.

Sven Venzke-Caprarese

Rückblick: Ergebnisse der Vergangenheit

Die Prüfungen der zehn bestplatzierten Websites haben in den letzten drei Jahren teilweise überraschende Ergebnisse gezeigt. Im Jahr 2015 unterstützten z.B. nur 20 % der geprüften Klinik-Websites eine sichere Datenübertragung per https. Im Jahr 2016 waren es immerhin 60% und im Jahr 2017 konnten 80 % der zehn geprüften Klinikwebsites per *https* aufgerufen werden, wobei zwei Seiten daneben auch *http* unterstützen und nicht automatisch auf *https* wechselten. Besonders brisant war im vorletzten Jahr eine Website, die Ärzte zur Eingabe von personenbezogenen Gesundheitsdaten und Diagnosen in unverschlüsselte Webformulare im Rahmen der Anmeldung von Tumor-Konferenzen aufforderte. Insgesamt überstanden in den letzten drei Jahren nur zwei von 30 geprüften Klinik-Websites den Datenschutz-Check. Neben der fehlenden Verschlüsselung waren Ausschlusskriterien häufig die nicht rechtskonforme Einbindung von Trackingtools,

fehlende Datenschutzerklärungen, unmittelbar eingebundene Social-Plugins und die laut Datenschutzerklärung zu lange Speicherfrist für IP-Adressen.

Für die Websites des Jahres 2018 sieht es besser aus!

Der Datenschutz-Check der Top 10 Klinik-Websites des 16. Awards zeichnet ein besseres Bild als die Prüfungen der Vergangenheit. Dies mag zum einen an der gesteigerten Sensibilität der Websitebetreiber im Hinblick auf das Wirksamwerden der Datenschutzgrundverordnung liegen. Zum anderen wurden im Rahmen des 16. Awards auch erstmals juristische Kriterien „wie Einhaltung des Telemediengesetzes und die Anpassung an die Datenschutz-Grundverordnung“ in die Platzierung einbezogen. Um welche Kriterien es sich dabei genau handelt, ist mangels Veröffentlichung des Kriterienkatalogs leider nicht bekannt. Insgesamt ist der Datenschutzstand der top platzierten Klinik-Websites aber deutlich besser als in den Vorjahren.

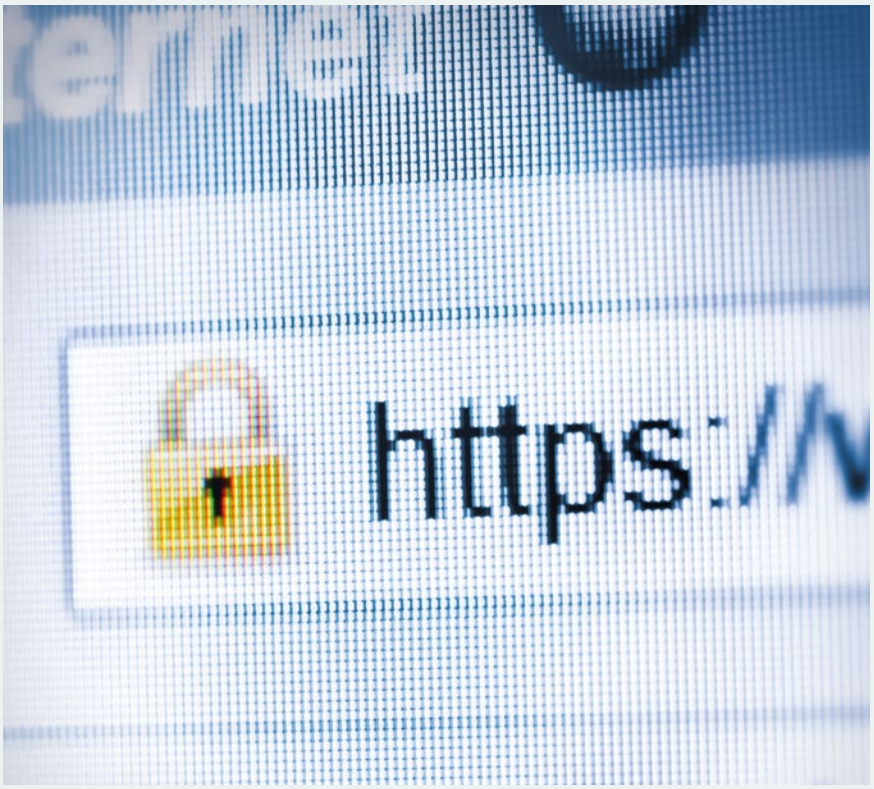
Anhand der im Januar veröffentlichten Gewinnerliste des Awards prüften wir die Klinik-Websites erneut auf datenschutzrelevante Punkte. Die Prüfung erfolgte Anfang März 2019.

https vs. http

Alle zehn Websites unterstützen den Aufruf per *https*. An dieser Stelle zeigt sich also eine deutliche Verbesserung zu den Vorjahren. Lediglich eine der zehn Websites war auch über *http* aufzurufen, ohne automatisch auf *https* zu wechseln. Bei näherer Betrachtung führte auch die weitere Navigation innerhalb der Seite – bis hin zum Kontaktformular – nicht zu einer Umstellung auf *https*. Diese Website schied somit aus unserem Wettbewerb aus.

Echtes Tracking? Echtes Banner!

Neun der zehn geprüften Websites nutzten einen Cookie-Banner. Lediglich ein Cookie-Banner war technisch in der Lage, das Webtracking so lange zu unterbinden, bis sich der Nutzer mit dem Tracking einverstanden erklärt hatte. Eine Website nutzte ein Banner, obwohl überhaupt keine Tracking-Tools eingebunden waren. Die restlichen sieben Websites verfügten über Banner, die keine technische Funktion aufwiesen und das Tracking bzw. die Analyse auch auf der Einstiegsseite nicht unterdrückten. Auf einer Website wurde das Banner durch ein Bild der Startseite verdeckt. Auf wieder anderen Seiten verdeckte das Banner den Link zum Impressum der Seite. Insgesamt zeigte sich bei der Prüfung, dass die Nutzung von Cookie-Bannern in der Praxis ein größeres Problem darstellt.



Mangels klarer Vorgaben für die Gestaltung von Cookie-Bannern seitens der Aufsichtsbehörden blieben an dieser Stelle erst einmal alle Websites im Rennen, die lediglich Webanalysetools zur Besuchermessung verwendeten (Google Analytics und Matomo/Piwik).

Eine Website verwendete darüber hinaus allerdings auch Tools, die regelmäßig Werbezwecken dienen und Nutzer diensteanbieterübergreifend tracken. Konkret handelte es sich hierbei u.a. um Google Remarketing und DoubleClick Ad Exchange. Aus folgenden Gründen schied die Website an dieser Stelle aus:

- Das verwendete Cookie-Banner wies keine technische Funktion auf – es wurde also bereits auf der Einstiegsseite zu Werbezwecken getrackt (mangelnde Funktion).
- Die Weiternutzung der Website wurde als konkludente Einwilligung gewertet, ohne dass die Nutzer sich ausdrücklich mit dem Tracking einverstanden erklären mussten (mangelnde Ausdrücklichkeit).
- Nutzern wurde die Möglichkeit verwehrt, die Einwilligung nicht zu erteilen (Kopplung).
- Zwar wurde auf eine Vielzahl von

Widerrufsmöglichkeiten hingewiesen (u. a. Deaktivierung von Cookies, Vornahme von Einstellungen im Google-Konto, Widerspruch über http://www.networkadvertising.org/choices/). Diese Widerspruchsmöglichkeiten dürften nach Ansicht der Aufsichtsbehörden aber nicht ausreichen (vgl. Allgemeine Hinweise und Anforderungen für Verantwortliche zum Einsatz von Facebook Custom Audience des BayLDA zu Ziffer 2 c). Erforderlich gewesen wäre z. B. ein Cookie-Banner, welches tatsächlich die Aktivierung und Deaktivierung der eingebunden Trackingtools steuert. Eine gute Übersicht über Bannerlösungen, die diese Funktionen unterstützt hätten, findet sich hier.

Eine weitere Website schied an dieser Stelle aus, da sie Google Analytics verwendete, ohne die IP-Adresse zu anonymisieren.

Noch eine Website schied aus, da sie zwar auf die Möglichkeit hinwies, durch Klick auf einen Link dem Tracking durch Google Analytics per Opt-Out Cookie zu widersprechen. Ein entsprechender Link war jedoch nicht hinterlegt.

Eine andere Seite unterstützte gar keinen Widerspruch per Opt-Out Cookie und schied ebenfalls aus.

Fünf Websites befanden sich zu diesem Zeitpunkt noch im Rennen.

Social Media Plugins

Eine Seite verwendete unmittelbar eingebundene Social Plugins. Hierbei handelte es sich um das Facebook Seiten-Plugin und das Twitter Seiten-Plugin. Eine Zwei-Klick-Lösung, welche die entsprechenden Inhalte erst nach ausdrücklichem Klick freigegeben hätte, wurde nicht genutzt. Die Seite war aber bei den vorherigen Prüfpunkten ohnehin schon ausgeschieden.

Keine der anderen Seiten nutzte unmittelbar eingebundene Social Plugins. Drei Klinik-Websites nutzten die Sharrif-Lösung, um Social Media Plugins einzubinden, was datenschutzrechtlich zulässig ist.

YouTube-Videos

Alle fünf verbleibenden Klinik-Websites nutzten eingebettete YouTube-Videos. Zwei dieser Websites betteten die entsprechenden Videos im erweiterten Datenschutzmodus ein. Eine Site nutzte eine Art 2-Klick-Lösung zur Einbindung der Videos.

Zwei Websites betteten die Videos unmittelbar und ohne erweiterten Datenschutzmodus ein. Dies führte dazu, dass bereits bei Aufruf der entsprechenden Seiten ein Doubleklick-Cookie des Werbenetzwerks von Google gesetzt wurde. Beide Sites erhielt einen Punktabzug, blieben jedoch im Rennen.

Externe Schriftarten

Von den fünf verbleibenden Seiten nutzte eine Website externe Schriftarten von Adobe Fonts und erhielt ebenfalls einen Punktabzug.

Weitere Punktabzüge

Drei Seiten nutzten Google Maps und erhielten einen Punktabzug. Eine Website wies in der Datenschutzerklärung auf die Nutzung von Google Analytics hin, ohne dies zu nutzen und ohne die entsprechenden Widerspruchsmöglichkeiten anzubieten. Eine Website formulierte die gesamte Datenschutzerklärung als Einwilligung. Dies wurde jeweils mit Punktabzügen bewertet.

Ergebnis

Von den zehn geprüften Websites schieden fünf aus. Die verbleibenden fünf Websites erhielten zwar jeweils Punktabzüge. Dennoch haben diese fünf Websites unseren kurzen Websitecheck überstanden – also mehr Websites als die letzten drei Jahre zusammengenommen.

Den ersten Platz unseres kleinen Wettbewerbs teilen sich dieses Jahr das Klinikum der Stadt Ludwigshafen am Rhein und die Kliniken der Stadt Köln.

Datenschutz im Gesundheitswesen

Mit Geltung der Europäischen Datenschutz-Grundverordnung und der damit verbundenen umfassenden Anpassung der nationalen Datenschutzvorschriften haben sich die datenschutzrechtlichen Rahmenbedingungen auch für Gesundheitseinrichtungen seit Mai 2018 grundlegend geändert.

Die Broschüre soll Datenschutzverantwortlichen dabei helfen, die Datenverarbeitung in Gesundheitseinrichtungen auch künftig rechtskonform zu gestalten. Das Handbuch vermittelt die neuen gesetzlichen Grundlagen, führt praxisnah in die Datenschutzorganisation ein und erläutert am Beispiel des Krankenhauses die zentralen datenschutzrechtlichen Herausforderungen.

Neben dem Datenschutz wird dabei auch das neue für Gesundheitseinrichtungen zunehmend wichtigere Feld der IT-Sicherheit beleuchtet.

Broschüre HIER bestellen

Broschüre DIN A5, ca. 380 Seiten
Preis: 89,90 € pro Stück inkl. MwSt. und versandkostenfreier Zusendung im Inland
Art. Nr.: 43110 | **ISBN: 978-3-553-43110-1**

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

Interdisziplinäre Videokonferenzen

Unsere Gesellschaft erlaubt es häufig nicht, dass Mitglieder eines Gremiums bei gemeinsamen Sitzungen am selben Ort sein können. Aber auch bei der Einholung eines Konsils wird der Austausch der erforderlichen Informationen nicht immer persönlich möglich sein. Zunehmend gibt es daher Überlegungen, in der Praxis eigene Videokonferenztools oder sogar die Videofunktion von Messenger-Diensten zu nutzen.

Dr. Sebastian Ertel

Weitergabe an Dritte

Bevor Überlegungen zur konkreten Umsetzung gemacht werden können, steht an erster Stelle die Frage, ob eine solche Nutzung überhaupt erfolgen darf. Die Gesundheitsdaten unterliegen der Schweigepflicht der Berufsgeheimnisträger. Eine unbefugte Offenbarung kann straf- und standesrechtliche Konsequenzen nach sich ziehen.

Je nach Art der konkreten Datenweitergabe bedarf es einer gesetzlichen Befugnis, eines fehlenden Widerspruchs des Patienten nach hinreichender Aufklärung oder einer Einwilligung desselben. Wenn eine solche Befugnis vorliegt, muss zusätzlich geprüft werden, ob es hinsichtlich des Dienstleisters, der das Kommunikationsmedium anbietet bzw. betreibt, ebenfalls einer Offenbarungsbefugnis bedarf.

Interdisziplinäre Konferenzen

Als praktikabler Anwendungsbereich gilt beispielsweise die Tumorkonferenz. Diese ist interdisziplinär und dient dem Zweck, entsprechend der vorliegenden Operations- und Untersuchungsergebnisse eine individuelle Therapieempfehlung für Patienten zu erstellen. Die Teilnehmer stammen aus den unterschiedlichsten Fachrichtungen und können auch aus mehr als zehn Personen bestehen.

Konsile

Auch bei der Einholung eines Konsils ist eine Videokonferenz denkbar. Der Konsiliararzt ist in der Regel an einem anderen Krankenhaus, gegebenenfalls sogar im Ausland tätig.

Messenger-Dienste

Einfach und schnell wäre die Nutzung der Videofunktion eines Messenger-Dienstes, beispielsweise des Brachenprimus WhatsApp mit mehr als 30 Mio. aktiven Nutzern (Stand 2017). Aufgrund der anhaltenden Kritik an dem Dienst, insbesondere der Datenmigration an die Konzernmutter Facebook Inc., ist ein Rückgriff hierauf die denkbar schlechteste Alternative. Da auch viele andere Dienste ihre Tücken haben und die Handhabung nicht immer praktikabel ist, sollte von einem Einsatz grundsätzlich abgesehen werden.

Skype

Eine der bekanntesten Videokonferenz-Anwendungen ist sicherlich Skype. Das Tool geriet 2016 in den Fokus der Landesdatenschutzbeauftragten Nordrhein-Westfalen und Berlin, im Zusammenhang mit dessen Einsatz bei Video-Vorstellungsgesprächen. Die Behörden kritisierten insbesondere, dass Kommunikation für bis zu 90 Tage auf Servern in den USA zwischengespeichert wird, es findet somit eine Datenübermittlung von besonderen Arten personenbezogener Daten (Gesundheitsdaten) in ein Drittland statt.

TeamViewer

Als weitere Alternative kommt TeamViewer in Betracht. Recherchiert man die Haltung der Aufsichtsbehörden zu diesem Tool, findet man nach längerer Suche eine Erwähnung im 12. Tätigkeitsbericht des Landesdatenschutzbeauftragten Mecklenburg-Vorpommerns. Kritikpunkt war hierbei, dass im Hinblick auf den für die verschlüsselte Kommunikation erforderlichen öffentlichen Schlüssel nicht sichergestellt werden könne, dass dieser tatsächlich vom angestrebten Kommunikationspartner stammt. Dieser würde vom TeamViewer-Server ohne Identifikationsnachweis übertragen. Aus diesem Grunde sah der Landesdatenschutzbeauftragte eine Anwendung bei Daten mit hohem Schutzbedarf (hierzu gehören Gesundheitsdaten zweifelsohne) als unzulässig an. Als Lösung des Problems wurde zur Nutzung des sogenannten SRP-Protokolls durch TeamViewer geraten. Mittels dieses Protokolls kann geprüft werden, ob beide Parteien, die über TeamViewer miteinander kommunizieren wollen, im Besitz eines gemeinsam vorher festgelegten Passwortes sind. Nur wenn dieser Umstand gegeben

ist, sind die Kommunikationspartner diejenigen, die auch tatsächlich miteinander kommunizieren wollen. Mittlerweise kommt das SRP-Protokoll bei TeamViewer zum Einsatz (https://www.teamviewer.com/de/trust-center/sicherheit/). Damit fällt der einzige bekannte Kritikpunkt weg.

Da sich zudem alle TeamViewer-Server innerhalb der Europäischen Union befinden, besteht auch keine Drittland-Problematik.

Alles gut und einfach los?

So einfach ist es dann doch nicht. Bevor die erste Sitzung initiiert wird, sollten noch verschiedene Aspekte berücksichtigt werden, mindestens jedoch:

- Nutzung der aktuellsten Software (da die Software nur so sicher ist, wie die schwächste eingesetzte Version, ist sicherzustellen, dass immer die aktuellste genutzt wird)
- Vertraulichkeit (es ist sicherzustellen, dass bei den Beteiligten nicht weitere Personen unerkannt im Raum anwesend sind und der Konferenz beiwohnen können)
- keine Aufzeichnung (es muss gewährleistet werden, dass keiner der Beteiligten die Konferenz - unbemerkt - aufzeichnet)
- Datensparsamkeit (auch bei der Konferenz unter Berufskollegen und -geheimnisträgern gilt der Grundsatz der Datensparsamkeit; es sind nur die Dokumente und Informationen mit den Beteiligten zu teilen, die für die Konferenz oder das Konsil zwingend notwendig sind – auf Namen oder andere Identifikationsdaten kann in der Regel verzichtet werden)

Kurznotiz:

Erste Details zum Recht auf kostenlose Kopie von Seiten der Aufsichtsbehörde

Bereits im letzten Newsletter hatten wir das Recht auf kostenlose Kopie gem. Art. 15 Abs. 3 DSGVO behandelt. In diesem Zusammenhang ist erwähnenswert, dass auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit dieses Recht in seinem 27. Tätigkeitsbericht für das Jahr 2018 thematisiert. Konkret wird im aktuellen Tätigkeitsbericht auf Seite 95 darauf hingewiesen, dass „ein elektronisch gestellter Antrag auf Zusendung einer Datenkopie im Sinne von Art. 15 Abs. 3 Satz 1 DSGVO […] nicht dadurch erfüllt wird, dass dem Betroffenen die persönliche Aushändigung einer Datenkopie gegen Vorlage des Personalausweises beim mehrere Stunden entfernten Verantwortlichen angeboten wird.“ Erstaunlicherweise thematisiert der Tätigkeitsbericht nicht, wie vorliegend eine Identitätsfeststellung des Betroffenen hätte durchgeführt werden können. Das Verlangen der Vorlage des Personalausweises vor Ort sei jedenfalls für den Betroffenen unverhältnismäßig aufwendig. Aus unserer Sicht wären vorliegend insbesondere folgende Möglichkeiten in Betracht gekommen:

- Aufforderung, eine Kopie des Personalausweises einzureichen, unter Hinweis auf die Möglichkeit, überschießende Daten zu schwärzen (Foto, Personalausweisnummer).
- Anschließende Übersendung der Daten in verschlüsselter Form per E-Mail und Übersendung des Passwortes an die letzte bekannte Wohnanschrift.
- Alternativ: Durchführung eines Postident-Verfahrens und Übermittlung der verschlüsselten Dateien per E-Mail.

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215 | Mail fachinfo@aok-verlag.de | Web http://www.aok-verlag.info
Herausgeber: AOK-Verlag GmbH, Remagen | Geschäftsführung: Otto Gmeiner, Frank Schmidt | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese | Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden. Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. | Bildnachweise: iStock