AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

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

Ausgabe November/Dezember 2022 | **Seite 1**

Inhalt

Schulungen smart organisieren

Eine der häufigsten Ursachen für Datenpannen und Sicherheitsvorfälle ist die Schwachstelle Mensch. Für das Datenschutzmanagement ist die Schulung und Sensibilisierung von Beschäftigten daher von zentraler Bedeutung und mindestens genauso wichtig wie der Einsatz sicherer Technologien.

Sven Venzke-Caprarese

Pflicht zur Schulung

Wenn man sich die Frage stellt, ob die DS-GVO eine Pflicht zur Durchführung von Datenschutzschulungen kennt, sucht man möglicherweise etwas länger im Gesetzestext.

Die Antwort findet sich schließlich etwas versteckt in Art. 39 Abs. 1 lit. b DS-GVO. Diese Norm regelt zwar auf den ersten Blick „nur“ die Aufgaben des Datenschutzbeauftragten. Bei genauerer Betrachtung findet sich hierunter aber auch die Pflicht des Datenschutzbeauftragten zur Überwachung der Datenschutzstrategie des Verantwortlichen im Hinblick auf die Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter*innen. Aus Art. 39 Abs. 1 lit. b DS-GVO lässt sich also folgern, dass der Verantwortliche eine Schulungsstrategie benötigt!

Zudem fordern Art. 24 DS-GVO und Art. 32 DS-GVO, dass neben technischen auch organisatorische Maßnahmen umgesetzt werden müssen, um die Rechtmäßigkeit und die Sicherheit der Verarbeitung zu gewährleisten.

Es bleibt also festzustellen, dass eine Pflicht zur Schulung besteht.

Auch die Aufsichtsbehörden gehen davon aus, dass die Schulung und die Sensibilisierung von Beschäftigten eine Kernpflicht des Verantwortlichen darstellen.

Was eine gute Schulungsstrategie auszeichnet

Eine gute Schulungsstrategie sollte alle Beschäftigten umfassen, die personenbezogene Daten verarbeiten.

Dabei sollten insbesondere neue Mitarbeiter*innen, die personenbezogene Daten verarbeiten, zeitnah angemessen zum Umgang mit personenbezogenen Daten sensibilisiert werden. An dieser Stelle kann z.B. mit einem Merkblatt zum Datenschutz gearbeitet werden, welches direkt bei Beschäftigungsbeginn ausgehändigt wird.

Spätestens in den ersten vier bis sechs Wochen empfiehlt es sich jedoch, einen vertiefenden Datenschutzgrundkurs als Schulung anzubieten. Einen solchen Kurs sollten alle Mitarbeiter*innen mindestes einmal durchlaufen haben. Sollte eine Vor-Ort-Schulung in der Praxis nicht für jeden neuen Beschäftigten umgesetzt werden können, kann z.B. auch ein passendes eLearning eingesetzt werden, welches jedoch zur Situation des Beschäftigten in der Organisation passen sollte. Themen, die keinesfalls fehlen sollten, sind dabei z.B. das Verbot mit Erlaubnisvorbehalt, der Umgang mit Datenpannen und Betroffenenrechten sowie der technische Schutz von Daten im Alltag.

Bei der erstmaligen Schulung sollte es jedoch nicht bleiben. So ist es empfehlenswert, die Schulung in regelmäßigen Abständen zu wiederholen und dabei z.B. auf neue Facetten oder Schwerpunkte einzugehen. Was hierbei unter „regelmäßig“ zu verstehen ist, muss jede Organisation für sich festlegen. Ein Auffrischungskurs pro Jahr dürfte aber in der Regel ausreichen. Ggf. kann dieser Auffrischungskurs auch kürzer ausfallen als die erste Schulungsmaßnahme und bestimmte Themen im Detail beleuchten.

Bei der Schulung von Beschäftigten muss jedoch beachtet werden, dass nicht jeder Arbeitsplatz gleich ist. Deshalb zeichnet sich eine gute Schulungsstrategie auch dadurch aus, dass sie Besonderheiten berücksichtigt. Beschäftigte der Personalabteilung werden daher regelmäßig nach Absolvierung des Grundkurses andere Schulungsinhalte benötigen als Beschäftigte der IT-Abteilung oder als Mitglieder der Mitarbeitervertretung.

Verantwortliche sollten sich klar machen: Menschliche Fehler sind eine der häufigsten Ursachen für Datenpannen und können oftmals durch Schulungen verhindert werden. Auch besondere Situationen können das Erfordernis einer Schulung auslösen. Wissen Beschäftige z.B., welche Verhaltensregeln für eine sichere Datenverarbeitung im Home-Office eingehalten werden sollen?

Ein ganzer Werkzeugkoffer an Schulungsmöglichkeiten

Insgesamt haben Verantwortliche eine Reihe von Instrumenten zur Schulung zur Verfügung, etwa

- Merkblätter,
- Vor-Ort- bzw. Video-Schulungen (auch durch Dritte),
- eLearning-Kurse,
- besondere Awareness-Kampagnen.

Es wäre an dieser Stelle allerdings ein Trugschluss, wenn Verantwortliche denken, es sei nach dem Gesetz die Aufgabe des Datenschutzbeauftragten, die entsprechenden Schulungen und Sensibilisierungen durchzuführen.

Natürlich können die Maßnahmen vom Datenschutzbeauftragten durchgeführt werden – das Gesetz sieht diese Pflicht aber originär beim Verantwortlichen. Die Aufgabe des Datenschutzbeauftragten ist per Gesetz lediglich die Überwachung der vom Verantwortlichen organisierten Schulungen. Das ist auch richtig so, denn insbesondere in großen Organisationen sind Datenschutzbeauftrage ansonsten schnell zeitlich überfordert.

Gut geschult ist hoffentlich auch gut dokumentiert

Gemäß Art. 5 Abs. 2 DS-GVO ist der Verantwortliche sowohl im Hinblick auf die allgemeine Schulungsstrategie als auch im Hinblick auf die konkrete Durchführung von Schulungen rechenschaftspflichtig.

Das bedeutet, dass die jeweilige Gesundheitseinrichtung ein abstraktes Schulungskonzept vorhalten sollte, welches die Schulungsstrategie beschreibt.

Darüber hinaus sollte jede durchgeführte Schulungsteilnahme dokumentiert werden und den Teilnehmer*innen Nachweise ausgestellt werden, die auch innerhalb der Organisation aufbewahrt werden sollten.

Schulungen in großen Gesundheitseinrichtungen organisieren

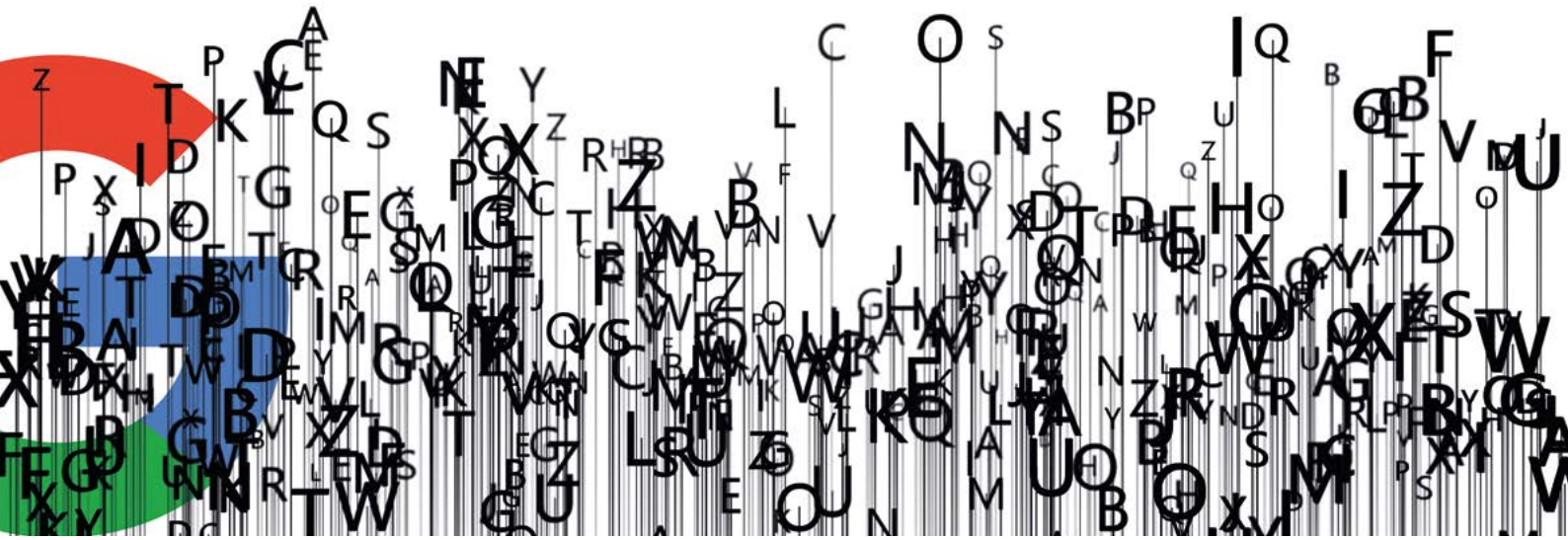
Ab einer gewissen Größe der Gesundheitseinrichtung wird es vermutlich schwierig, ohne den Einsatz von eLearning und Learning-Management-Systemen auszukommen. Verantwortliche sollten sich darüber im Klaren sein, dass es gerade in Gesundheitseinrichtungen vermutlich noch viele weitere Anforderungen an Schulungen, Sensibilisierungen und Unterweisungen gibt. So sind neben dem Datenschutz in der Regel auch Informationssicherheit (Stichwort Phishing und Schadsoftware), Compliance, Arbeitssicherheit, Hygieneregeln etc. ein Thema.

Ggf. existiert in diesem Rahmen innerhalb der Organisation bereits ein Ansprechpartner für das übergreifende Lernmanagement der Beschäftigten und möglicherweise ist auch schon ein Learning-Management-System (LMS) vorhanden, mit dem Schulungen organisiert, Einladungen versendet sowie Teilnehmernachweise erstellt und gespeichert werden können.

Ein gutes LMS bietet die Möglichkeit, Vor-Ort-Schulungen (Einladung und Teilnehmernachweis) und Videokonferenzschulungen zu organisieren (Einladung und Teilnehmernachweis), eigene Inhalte für eine Datenschutzschulung einzubinden (z.B. als PowerPoint, welches dann als eLearning über den Browser wie eine normale Webseite ausgespielt wird) oder auch eingekaufte Schulungsinhalte aus unterschiedlichen Quellen auszuspielen (z.B. im Scorm Format).

Fazit

Das Thema Schulung und Sensibilisierung von Beschäftigten sollte strategisch angegangen werden. Es ist oftmals weder ausreichend noch zielführend, einmal im Jahr eine große Vor-Ort-Schulung für alle anzubieten. Klären Sie als Datenschutzbeauftragter mit dem Verantwortlichen daher die Schulungsstrategie der Gesundheitseinrichtung und dokumentieren Sie diese. Weisen Sie in diesem Rahmen darauf hin, dass es oftmals eine Überforderung der Ressourcen des Datenschutzbeauftragten bedeuten kann, wenn alle neuen Mitarbeiter*innen kurzfristig durch Sie geschult und auch regelmäßige (Spezial-)Schulungen für Beschäftigte durch Sie angeboten werden sollen. Wenn die Ressourcen da sind, kann dieser Weg zwar gegangen werden. Es existieren aber auch andere Instrumente, die Sie als Datenschutzbeauftragten entlasten können.



Abmahnung wegen der Nutzung von Google Fonts auf der Webseite

Aktuell bricht eine gewaltige Abmahnwelle über Webseitenbetreiber herein. Betroffen sind die Webseitenbetreiber, die wissentlich oder unwissentlich Schriften des Unternehmens Google remote eingebunden haben. Pro Abmahnung werden bis zu 250 Euro (Schadensersatz und Rechtsanwaltsgebühren) gefordert, hinzu kommt die Arbeit, die mit deren Bearbeitung anfällt.

Dr. Sebastian Ertel

Was ist Google Fonts

Google Fonts ist eine Datenbank der Google Inc. mit mehr als 1.400 Schriften. Diese Schriften können direkt in die eigene Webseite eingebunden werden. Zum Teil erfolgt die Einbindung aber auch indirekt und damit unbewusst, etwa wenn andere Produkte aus dem Hause Google auf der Webseite eingebunden sind, beispielsweise YouTube oder Google Maps.

Was ist das Problem?

Wird eine Google Schrift in der Webseite eingebunden, passiert Folgendes: Mit dem Aufruf einer Webseite erfolgt eine Kontaktaufnahme zu einem Google-Server in den USA, auf dem die Schrift zum Abruf hinterlegt ist, damit dieser die Schrift für die Anzeige der Webseite bereitstellen kann. Hierzu wird die IP-Adresse (ein personenbezogenes Datum) mit an den Google Server übermittelt. Das ist notwendig, damit der Google-Server weiß, wohin er die Schrift schicken soll.

Das Problem hierbei ist, dass die USA als datenschutzrechtliches Drittland gelten. Eine Datenübermittlung dorthin (die vorliegend in der Mitteilung der IP-Adresse besteht), ist seit dem Ende des Privacy Shield (ein Abkommen zwischen der Europäischen Kommission und den USA zum Datentransfer, welches vom Europäischen Gerichtshof für unzulässig erklärt wurde) nicht mehr ohne weiteres möglich: Der Webseitenbesucher muss seine Einwilligung erklären, dass zum Zwecke des Ladens der Google Schrift seine IP-Adresse an die Google-Server in den USA übermittelt werden. Dies kann beispielsweise über ein Cookie-Banner erfolgen. Ist dieses jedoch schlecht konfiguriert oder fehlt gänzlich, wird der Datentransfer ohne die erforderliche Einwilligung vollzogen.

Was ist die Folge?

Die Abmahner berufen sich auf ein Urteil vom Landgericht München I vom 20.01.2022 (Az.: 3 O 17493/20). In diesem Verfahren mussten sich die Richter mit der datenschutzwidrigen Einbindung von Google Fonts auseinandersetzen und urteilten einen Schadensersatz von 100 EUR aus.

Auf Grundlage dieses Urteils mahnen aktuell zwei Rechtsanwaltskanzleien im Auftrag ihrer Mandanten Webseitenbetreiber ab, die ohne die erforderliche Einwilligung Google Fonts eingebunden haben. Es wird vermutet, dass mehrere 10.000 Abmahnungen versandt wurden.

Was sollte man tun?

Es sollte dringend geprüft werden, ob auf den eigenen Webseiten Google Fonts eingebunden ist und wie diese Einbindung erfolgte.

a) Google Fonts ist lokal eingebunden.

   In diesem Fall müssen Sie keine weiteren Maßnahmen ergreifen.

b) Google Fonts ist remote eingebunden, eine Einwilligung wird über das Cookie-Banner eingeholt.

   In diesem Fall müssen Sie keine weiteren Maßnahmen ergreifen.

c) Google Fonts ist remote bzw. über andere Google Produkte eingebunden, es wird keine Einwilligung eingeholt.

In diesem Fall sollten Sie zunächst prüfen, ob die Schrift direkt oder über ein Google-Produkt eingebunden ist und diese(s) erst einmal von der Seite entfernen. Wird die Schrift direkt genutzt, sollte diese lokal eingebunden (Anleitungen finden sich vielfach im Netz) oder darauf verzichtet werden. Erfolgt die Einbindung hingegen indirekt über ein anderes Google-Produkt, muss diese so erfolgen, dass das Produkt nur geladen wird, wenn der Webseitenbesucher seine Einwilligung (über das Cookie-Banner, die 2-Klick-Lösung oder die Shariff-Lösung) erklärt.

Wie ist auf eine Abmahnung zu reagieren?

Sollte eine Abmahnung wegen Google Fonts eingehen, sollte darauf auch reagiert werden. Oberste Priorität hat die Entfernung der Remote-Einbindung der Schrift bzw. die Prüfung, ob die Einbindung der Schrift im Zusammenhang mit der Nutzung eines anderen Google-Produktes besteht. Dieses sollte zunächst von der Webseite entfernt und, sofern darauf nicht verzichtet werden kann, anschließend datenschutzkonform eingebunden werden.

Ist mit der Abmahnung ein Auskunftsersuchen nach Art. 15 DS-GVO verbunden, muss dieses binnen eines Monats beantwortet werden. Der LfDI Hessen weist in diesem Zusammenhang darauf hin, dass „das Auskunftsrecht dem Betroffenen dazu dient, sich der Verarbeitung seiner personenbezogenen Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Sollte mit dem Auskunftsbegehren allerdings keine Rechtmäßigkeitsprüfung zur Durchsetzung der Betroffenenrechte angestrebt, sondern vielmehr verordnungsfremde Ziele verfolgt werden, kann das Auskunftsbegehren am Einwand der Rechtsmissbräuchlichkeit scheitern (vgl. Art. 12 Abs. 5 DS-GVO).“ Das könnte vorliegend der Fall sein, da dem Abmahnenden die relevanten Informationen bereits vorliegen und das Auskunftsbegehren keine neuen, nicht bereits vorhandene Erkenntnisse liefert.

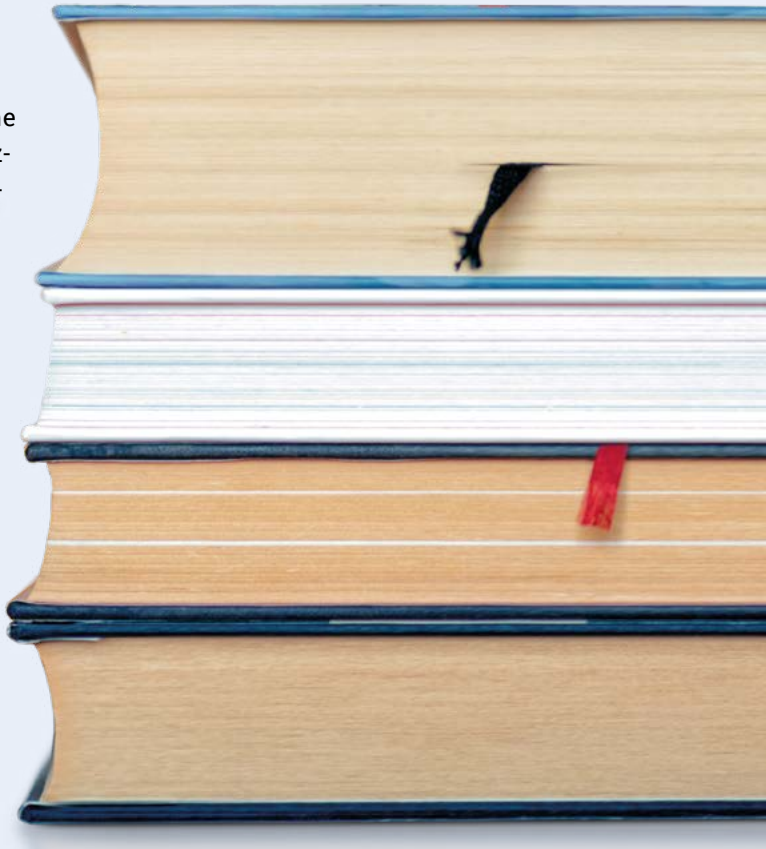
Die Abmahnung selber bietet mehrere Angriffspunkte (z.B. fehlende Originalvollmacht, Rechtsmissbräuchlichkeit wegen Massenabmahnung). Ob die geltend gemachten Beträge gezahlt werden sollen, muss letztlich von der Einrichtungsleitung entschieden werden. Wenn auf die Abmahnung mit einem Antwortschreiben reagiert werden soll, finden sich im Netz verschiedene Generatoren für ein solches Dokument, beispielsweise unter https://kremer-rechtsanwaelte.de/anti-abmahner/

Fazit

Prüfen Sie kurzfristig, ob bei der Einbindung externer Dienste auf der Webseite die erforderlichen Einwilligungen eingeholt werden. Sollte dies nicht der Fall sein, ist hier kurzfristig nachzubessern. Haben Sie eine Abmahnung erhalten, sollten Sie sowohl bzgl. der Webseite also auch hinsichtlich der Abmahnung aktiv werden.

Kurznotiz

OH KIS – überarbeitete Fassung zum Jahreswechsel erwartet



Die Orientierungshilfe Krankenhausinformationssysteme (OH KIS) formuliert die Anforderungen für die datenschutzkonforme Nutzung der Informationssysteme in Gesundheitseinrichtungen, speziell in Krankenhäusern. Die OH KIS liegt aktuell in der 2. Fassung (2014) vor. Das Regelwerk bietet viele gute und wichtige Ansätze, war aber auch zum Teil erheblicher Kritik ausgesetzt. Hersteller kritisierten, dass deren Hinweise bei der Erstellung nicht berücksichtigt wurden. Auch würden in der OH KIS Begrifflichkeiten verwendet, die im Krankenhausalltag eine andere Bedeutung haben können, sodass hier Missverständnisse und Fehlinterpretationen möglich seien. Größter Kritikpunkt ist das Alter der aktuellen Fassung und die fehlende Berücksichtigung der DS-GVO.

Zumindest der letzte Punkt soll zeitnah seine Erledigung finden. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit soll federführend an der 3. Fassung der OH KIS arbeiten. Diese soll zum Jahreswechsel abgeschlossen sein. Auf der Webseite finden sich (noch) keine Informationen.

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-0 | Fax 02642 931-215
Mail: fachinfo@aok-verlag.de | Web: http://www.aok-verlag.info | Herausgeber: AOK-Verlag GmbH, Remagen
Geschäftsführung: 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: GettyImages, AOK-Verlag

Praxishandbuch für Datenschutzbeauftragte im Gesundheitswesen

Welche Patientendaten dürfen an wen und in welcher Form übermittelt werden? Wie ist ein Empfangsbereich im Krankenhaus zu strukturieren, damit die Privatsphäre jedes Einzelnen gewährleistet wird? Wie muss ein Datenschutzkonzept aussehen, damit es als Grundlage für einen Audit dienen kann? Und wer hat eigentlich auf welche Patientendaten Zugriff?

Die Herausforderung ist, dass die innerbetrieblichen Abläufe durch die Umsetzung datenschutzrechtlicher Vorgaben nicht beeinträchtigt werden sollen - ein Spagat, der gemeistert werden muss. Hinzu kommt, dass viele Datenschutzbeauftragte diese Tätigkeit neben ihrem Hauptaufgabengebiet ausüben und sich ein fundiertes Wissen im IT-Bereich erst aneignen müssen, um mit Kollegen oder Externen auf Augenhöhe zu kommunizieren.

Das Handbuch „Datenschutz im Gesundheitswesen“ greift die typischen Arbeits- und Problemfelder auf und liefert Lösungen, die Rechtssicherheit, Nachhaltigkeit und Akzeptanz bei Aufsichtsbehörden bieten. Der Schwerpunkt des Handbuches liegt in der praktischen Umsetzung der datenschutzrechtlichen Vorgaben im betrieblichen Alltag, bspw. bei den spezifischen Anforderungen in den verschiedenen Bereichen des Gesundheitswesens, wie Krankenhaus oder Arztpraxis.

Im exklusiven Online-Kundenbereich finden Sie das Werk als E-Book. Mittels pdf-Download laden Sie kapitelweise Ihr Handbuch herunter und können es direkt an Ihrem Rechner einsetzen. So sind Sie unabhängig von Ihrem Arbeitsort und haben jederzeit Zugriff auf die Datenschutzbestimmungen.

- 2 Ordner mit Register im Format DIN A5,
- ca. 1.500 Seiten Inhalt
- ISBN: 978-3-553-43000-5
- Preis **195,00 €** inkl. MwSt.
- Uneingeschränkter Online-Zugriff
  inkl. 3-4 kostenpflichtige Nachtragslieferungen
  pro Jahr zum Preis von jeweils **89,90 €** inkl. MwSt.
  und versandkostenfreier Zusendung im Inland.