AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe April 2016 | Seite 1

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

INHALT

SEITE 1
Deutschlands beste Klinik-Websites im Datenschutz-Check

SEITE 5
Auslagerung von Datenverarbeitungen

SEITE 8
Babygalerie im Internet
Nutzung von Mitarbeiterfotos für den Internetauftritt: Nur mit schriftlicher Einwilligung

Deutschlands beste Klinik-Websites im Datenschutz-Check

Die Anforderungen an das Design und die Funktion moderner Klinik-Websites sind hoch – die datenschutzrechtlichen Anforderungen allerdings auch.

Sven Venzke-Caprarese, Dr. Sebastian Ertel

Jedes Jahr werden in Deutschland die besten Klinik-Websites gekürt. Als Maßstab gelten u. a. Design, Bedienung, Inhalte, Informationsqualität, Einsatz moderner Techniken des Web 2.0 und Integration von Social-Web-Funktionen. Aus über 200 eingereichten Websites wurden Ende 2015 die zehn Besten gekürt und die Ergebnisse veröffentlicht. Diese TOP 10 Websites repräsentieren gewissermaßen die Erwartungen an moderne Websites von Kliniken. Grund genug, anhand dieser Beispiele einen kurzen Blick auf die elementarsten datenschutzrechtlichen Rahmenbedingungen zu werfen, die der Betrieb einer solchen Website mit sich bringt. Geprüft wurden sechs Punkte, die Sie für Ihre Klinik-Website ebenfalls prüfen können.

Sichere Verbindung

Moderne Klinik-Websites bieten Besuchern eine Reihe von Kommunikationsmöglichkeiten. Neun der zehn untersuchten Websites boten z. B. die Möglichkeit, personenbezogene Daten über Kontakt- und Bewertungsformulare, Terminplaner, elektronische Grußkarten sowie Login-Bereiche einzugeben. Überraschenderweise schienen dabei nur zwei der zehn Websites eine https-Verbindung zu verwenden, wobei eine Website TLS 1.0 und die andere TLS 1.2 zur Verschlüsselung des Datenverkehrs nutzte.
Bereits für normale Websites fordern Datenschutzaufsichtsbehörden seit längerem, dass alle personenbezogenen Daten, die über die Website eingegeben werden, verschlüsselt zu transportieren sind. Besonders deutlich formuliert dies z. B. die Bayerische Aufsichtsbehörde in ihrem 26. Tätigkeitsbericht

aus dem Jahr 2015: „Sobald personenbezogene Daten – und dazu zählt grundsätzlich auch schon ein Kontaktformular – übertragen werden, ist eine TLS/SSL-Verschlüsselung unumgänglich“. Es gibt noch einen weiteren Grund, weshalb Websitebetreiber die Umstellung von http auf https vornehmen sollten: Durch das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz wurde § 13 Abs. 7 Telemediengesetz (TMG) neu gefasst. Websitebetreiber sind demnach verpflichtet, ihre Seiten so zu gestalten, dass sie gegen die Verletzung des Schutzes personenbezogener Daten gesichert sind. Eine solche Sicherungsmaßnahme ist nach dem TMG insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. Werden diese Vorgaben nicht beachtet, können nach § 16 TMG sogar Bußgelder drohen. Als angemessen sicher gelten derzeit die Verschlüsselungsverfahren TLS 1.0 (dieses sollte aber nur noch vorübergehend genutzt werden) sowie TLS 1.1 und TLS 1.2.

Das wurde getestet:

Verbindung über https	Können personenbezogene Daten eingegeben werden? Falls ja, verfügt die Website über eine Verschlüsselung mindestens der Stufe TLS 1.0?
Trackingtools	Wird der Nutzer über den Einsatz von Trackingtools informiert? Existiert eine Opt-Out-Möglichkeit? Funktioniert ein Opt-Out auch in der Mobilansicht auf dem Smartphone? Wird die IP-Adresse anonymisiert?
Social Plugins	Werden Social Plugins direkt eingebunden oder werden Lösungen wie „Zwei-Klick“ bzw. „Shariff“ genutzt?
Videoplayer	Werden Videoplayer datensparsam eingebunden?
Datenschutzerklärung	Verfügt die Website über eine Datenschutzerklärung, die zur Website passt?
Mobilansicht	Ist die Datenschutzerklärung auch in der Mobilansicht noch hinreichend erkennbar und erreichbar?

Datenschutzkonformes Webtracking

Acht der zehn untersuchten Websites verwendeten Trackingsoftware. Sechs Websites nutzten Google Analytics, eine Website nutzte Piwik und eine Website nutzte beide Dienste gleichzeitig.
Lediglich eine dieser Websites erfüllte alle Anforderungen unserer Prüfung: Der Besucher wurde in der Datenschutzerklärung über die Verwendung der Trackingsoftware aufgeklärt. Zudem waren Widerspruchsmöglichkeiten vorgesehen, die sowohl auf herkömmlichen Clients als auch auf Smartphones und Tablets ausgeübt werden konnten. Darüber hinaus wurde eine Anonymisierungsfunktion für die IP-Adresse genutzt.
Die anderen Websites mit Trackingfunktionen wiesen Verbesserungspotential auf. Eine Website erläuterte in der Datenschutzerklärung zwar die Nutzung von Google Analytics und die Anonymisierung der IP-Adresse. Eine entsprechende Anonymisierung wurde bei der Implementierung des Google-Scriptcodes allerdings vergessen.
Nahezu alle Websites hatten Probleme mit der Widerspruchsmöglichkeit. Zum Teil fehlte diese vollständig, was hauptsächlich die Websites betraf, die Piwik nutzten. Durchgängig fehlte eine Widerspruchsmöglichkeit für Smartphones und Tablets. Eine umfassende Widerspruchsmöglichkeit ist nach § 15 Abs. 3 TMG jedoch unerlässlich und in der Praxis auch durchaus möglich. Wie es richtig geht, erklärt eine Anleitung des Hamburgischen Datenschutzbeauftragten am Beispiel von Google Analytics.
Sowohl Piwik als auch Google Analytics können datenschutzkonform genutzt werden. Datenschutzbeauftragte können die eigene Klinik-Website wie folgt prüfen: Mit Hilfe des Browser-Plugins Ghostery kann zunächst festgestellt werden, welche Trackingsoftware von der Klinik-Website genutzt wird.
Ein Blick in die Datenschutzerklärung gibt Aufschluss über die angebotenen Informationen und Widerspruchsmöglichkeiten.

Die Funktionsfähigkeit des Widerspruchs sollte ausprobiert werden, auch auf dem Smartphone. Hier zeigt sich schnell, dass allein die Option, ein Browser-Plugin zu installieren, nicht ausreicht. Wird Google Analytics verwendet, kann in einem letzten Schritt noch die Anonymisierung der IP-Adresse geprüft werden. Dabei muss der Quelltext der Website nach dem entsprechenden Google Script durchsucht und geprüft werden, ob die Anonymisierungsfunktion genutzt wurde. Hierzu kann der Quelltext z. B. nach dem Ausdruck „anonymizeIp“ durchsucht werden.

Social Plugins

Erstaunlicherweise nutzten nur vier der zehn Websites Social Media Plugins wie etwa den Facebook Like- oder den Twitter Share-Button. Drei Websites verwendeten zur Einbindung die datenschutzkonforme „Zwei-Klick-Lösung“. Keine Website verwendete die ebenfalls datenschutzkonforme Weiterentwicklung „Shariff“. Eine Website verwendete unmittelbar eingebundene Social Plugins.

Die unmittelbare Einbindung von Social Media Plugins steht seit Jahren in der Kritik der deutschen Aufsichtsbehörden. Dies liegt vor allem daran, dass die direkte Einbindung entsprechender Funktionen dazu führt, dass bereits der Aufruf der Website zu einem Verbindungsaufbau mit dem Social Media-Netzwerk führt. Dabei kommt es nicht darauf an, ob der Besucher sich bei dem Netzwerk überhaupt registriert hat, ob er eingeloggt ist oder ob er die entsprechende Funktion genutzt hat oder nicht. Gleichwohl können Social Plugins datenschutzkonform eingebunden werden. Insbesondere die seit 2014 verfügbare Shariff-Lösung steht im Hinblick auf Design und Funktion dem direkt eingebundenen Social Media Plugin in nichts mehr nach.

Die Gefahr, wegen direkt eingebundenen Social Media Plugins abgemahnt zu werden, ist seit Februar 2016 durch die Einführung des „Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“ übrigens stark gestiegen. Denn hierdurch haben Verbraucherschutzzentralen eigene Klagebefugnisse erhalten. Im März hat z. B. die Verbraucherzentrale NRW vor dem Landgericht Düsseldorf die Unterlassung der direkten Einbindung des Facebook Like-Buttons gegen den Betreiber einer Website erwirkt.

Videoplayer

Sieben von zehn Kliniken verfügten über einen eigenen YouTube-Auftritt. Zwei der sieben Kliniken verwiesen auf ihrer Website lediglich auf die entsprechenden Videos und zeigten die entsprechenden Vorschaubilder an, ohne dass der Videoplayer von YouTube bereits im Hintergrund geladen wurde. Fünf Kliniken betteten die YouTube-Videos direkt in ihre Website ein – allerdings erfolgte die Einbettung nicht im „erweiterten Datenschutzmodus“. Diesen Modus bietet YouTube seit längerem an. Man findet die Option auf der YouTube-Seite, auf der sich das Video befindet, welches eingebettet werden soll. Nach einem Klick auf „Teilen“, „Einbetten“, „Mehr anzeigen“ kann schließlich der „erweiterte Datenschutzmodus“ aktiviert werden. Videos, die in diesem Modus eingebettet werden, setzen deutlich weniger Cookies als Videos, die im normalen Modus eingebettet werden. In welchem Modus die Videos eingebettet sind, lässt sich schnell ausmachen: Verweist der Link des eingebetteten Videos auf www.youtube.com, handelt es sich um den normalen Modus. Verweist das eingebettete Video allerdings auf www.youtube-nocookie.com, wurde der erweiterte Datenschutzmodus genutzt.

Datenschutzerklärung

Grundsätzlich verfügten alle Websites über eine Datenschutzerklärung. Lediglich eine Website lieferte auf Grund einer technischen Panne an entsprechender Stelle eine leere Seite ohne Inhalte aus. Nach einer kurzen Information des Websitebetreibers wurde dieser Fehler jedoch unverzüglich behoben. Inhaltlich waren die Datenschutzerklärungen meist nachvollziehbar. Eine Website klärte jedoch über die Verwendung von Google Analytics auf, ohne dies zu nutzen. Eine weitere Website arbeitete mit einer offensichtlich nicht angepassten Musterdatenschutzerklärung, die über alle möglichen Datenverarbeitungen informierte, die jedoch auf der Seite nicht festzustel-

len waren – darunter auch zahlreiche Werbenetzwerk- und Trackingfunktionen.

Mobilansicht

Viele Websites verfügen mittlerweile über ein sog. responsive Design – also eine alternative Darstellung der Website für bestimmte Auflösungen. Nutzt eine Website dieses responsive Design, kann es durchaus vorkommen, dass die Website auf einem Smartphone völlig anders aussieht als auf einem Desktop-Client. Es lohnt sich daher, auch die Smartphoneansicht bei einem Datenschutzcheck der Klinik-Website im Blick zu behalten. So waren z. B. bei einer der untersuchten Websites in der Mobilansicht weder das Impressum noch die Datenschutzerklärung auffindbar.

Fazit

Bereits dieser kurze Datenschutz-Check zeigt, dass es in der Praxis häufig nicht einfach ist, alle datenschutzrechtlichen Anforderungen einzuhalten. Nehmen Sie diesen Beitrag deshalb vielleicht als Anregung, die eigene Klinik-Website einem kurzen Datenschutzcheck zu unterziehen. Dabei müssen Sie es nicht bei den hier vorgestellten sechs Prüfpunkten belassen. Denn der Betrieb einer Klinik-Website wird regelmäßig eine Reihe weiterer Fragen aufwerfen. Diese können von der Veröffentlichung von Mitarbeiter- und Patientenfotos auf der Website sowie Besonderheiten bei Babygalerien, über die Einschaltung von externen Webhostingdiensten, die Absicherung des Webservers bis hin zur Gestaltung eines Bestellprozesses für Newsletter oder der Frage der Verwendung von IP-Adressen noch viele andere Themen berühren.

Vertiefungshinweise im Handbuch „Datenschutz im Gesundheitswesen“ (DSiGW):

- Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel C/12 (Internetauftritt)

Auslagerung von Datenverarbeitungen

Die Einbindung externer Dienstleister in die eigene Unternehmensstruktur hat in den letzten Jahren enorm an Bedeutung gewonnen. In vielen Fällen werden finanzielle Aspekte ausschlaggebend sein. Der externe Dienstleister liefert die benötigte Hardware und Manpower, um die Datenverarbeitung im Vergleich zu einer internen Lösung kostengünstiger anzubieten. Da die Dienstleistung die Kernkompetenz des Externen darstellt, hat dieser grundsätzlich auch ein größeres Fachwissen. Dies müsste sich ein interner Mitarbeiter erst aufwendig aneignen und sich ständig auf dem aktuellen Stand halten. Dazu kommt das Problem der fehlenden praktischen Anwendung dieses Fachwissens.

Dr. Sebastian Ertel, Sven Venzke-Caprarese,

Auftragsdatenverarbeitung?

Für die datenschutzrechtliche Beurteilung der Einbindung externer Dienstleister ist maßgeblich, ob diese in Form einer Auftragsdatenverarbeitung (ADV) erfolgt. Die ADV ist dadurch geprägt, dass

- der Auftragnehmer (AN) den Weisungen des Auftraggebers (AG) unterworfen ist,
- der AN die Daten nicht für eigene Interessen erheben, verarbeiten oder nutzen darf,
- der AG für die Zulässigkeit der Datenverarbeitung verantwortlich ist,
- zwischen AN und Betroffenem keine eigenständige rechtliche Beziehung besteht und
- die Weitergabe der Daten an den AN keiner gesetzlichen Grundlage (Übermittlungsbefugnis) bedarf.

Im Rahmen einer ADV wird der AN so eng an den AG gebunden, dass dieser, bildlich gesprochen, wie eine Abteilung innerhalb des AG behandelt wird.

Klassische ADV

Als ADV sind typischerweise folgende Dienstleistungen ausgestaltet:

- Entwicklung, Wartung und Pflege von Software
- Wartung von Hardware
- Bereitstellung und Betrieb des kompletten Rechenzentrums
- Lagerung, Archivierung und Verfilmung von Unterlagen
- Vernichtung von Datenträgern
- Funktionsübertragung

Das Gegenstück zur ADV ist die Funktionsübertragung (FÜ). Diese ist dadurch charakterisiert, dass

- keine Weisungsgebundenheit besteht,
- der AN die Daten für eigene Zwecke erhebt, verarbeitet oder nutzt,
- der AG den Einfluss auf die Datenerhebung, -verarbeitung und -nutzung verliert,
- die Verantwortlichkeit für die Zulässigkeit der Datenverarbeitung auf den AN übergeht,
- die Datenweitergabe an eine gesetzliche Grundlage (Übermittlungsbefugnis) geknüpft ist.

Bei der FÜ verliert der AG also grundsätzlich die Möglichkeit, auf die weitere Verarbeitung der Daten einzuwirken.

Gesetzliche Regelungen

Allgemeine Regelungen zur ADV finden sich im Bundes- bzw. in den einzelnen Landesdatenschutzgesetzen sowie in den allgemeinen kirchlichen Gesetzen (z. B. KDO und DSG-EKD). Spezialgesetzliche Regelungen, die die Verarbeitung von Patientendaten im Auftrag regeln, finden sich in den Landeskrankenhausgesetzen, den Datenschutzdurchführungsverordnungen der Evangelischen Kirche oder den Anordnungen zum Schutz von Patientendaten in der katholischen Kirche.

Ärztliche Schweigepflicht

Informationen, die ein Arzt oder sonstiger Angehöriger eines Heilberufes in Ausübung seiner Tätigkeit zur Kenntnis genommen hat, stehen unter dem Schutz der ärztlichen Schweigepflicht. Ihre unbefugte Offenbarung wird durch § 203 StGB unter Strafe gestellt. Unbefugt

ist eine Offenbarung immer dann, wenn diese nicht durch Gesetz oder eine Schweigepflichtentbindungserklärung (Einwilligung) legitimiert werden kann. Das Strafgesetzbuch und das allgemeine Datenschutzrecht stehen dabei in einem Spannungsverhältnis. Denn eine Auftragsdatenverarbeitung nach den allgemeinen datenschutzrechtlichen Regelungen begründet noch keine Offenbarungsbefugnis.

Keine spezialgesetzlichen Regelungen

Bestehen keine spezialgesetzlichen Regelungen für den Krankenhausbereich (solche fehlen in Brandenburg, Hessen, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein), kann nur auf die allgemeinen Gesetze zurückgegriffen werden. Diese regeln allerdings nur allgemein die Auslagerung von Dienstleistungen in Form einer ADV und gehen nicht auf die spezifischen Besonderheiten ein, die die ärztliche Schweigepflicht mit sich bringt. Daher kann eine klassische Auftragsdatenverarbeitung bei fehlenden spezialgesetzlichen Regelungen ohne Zusatzmaßnahmen (Verschlüsselung, Schweigepflichtentbindungserklärung) nicht gesetzeskonform umgesetzt werden.

Vorsicht

Die einzelnen Länderregelungen sind allerdings mit Vorsicht anzuwenden, denn auch bei den spezialgesetzlichen Regelungen gibt es zum Teil gravierende Einschränkungen und Unterschiede.

Eine Darstellung, die sämtliche Regelungen umfasst, ist im Rahmen dieses Newsletters angesichts der Tatsache, dass es elf landesspezifische Spezialregelungen und darüber hinaus eine kaum zu überblickende Anzahl an kirchlichen Regelungen gibt, zwar nicht möglich. Jedoch lässt sich die Rechtslage prinzipiell auf drei Gestaltungen reduzieren:

- In Baden-Württemberg, Bayern, Berlin und Bremen darf die ADV im Grundsatz nur durch ein anderes Krankenhaus oder eine öffentliche Stelle (Nordrhein-Westfalen) durchgeführt werden. Abweichend hiervon darf eine Datenverarbeitung ausgelagert werden, wenn diese automatisiert durch ein Rechenzentrum erfolgt (Baden-Württemberg), zur verwaltungsgemäßen Abwicklung der Behandlung des Patienten erforderlich ist (Bayern), wenn der AN keinen Personenbezug herstellen kann bzw. bei einer Archivierung die Daten verschlüsselt wurden (Berlin). Ein detaillierter Blick ins Gesetz ist an dieser Stelle unumgänglich.
- In Mecklenburg-Vorpommern, Saarland und Thüringen ist die ADV bzw. die Offenbarung zulässig, wenn Störungen im Betriebsablauf sonst nicht vermieden werden können oder die Datenverarbeitung durch die Auslagerung erheblich kostengünstiger gestaltet wird.
- In Rheinland-Pfalz, Sachsen und der Katholischen sowie der Evangelischen Kirche ist die ADV nur erlaubt, wenn die Geheimhaltungspflichten des § 203 StGB gewährleistet werden. Hier stellt sich die Frage, was darunter zu verstehen ist:
  - » Genügt eine Verpflichtung des AN auf die Verschwiegenheit nach § 203 StGB? Ist dies überhaupt möglich, wenn der AN kein Berufsgeheimnisträger ist oder
  - » müssen die Daten vielmehr verschlüsselt und somit einem Zugriff des AN entzogen sein?
  - » Steht der Verweis auf § 203 StGB einer ADV entgegen?

Die Herausforderung für den Datenschutzbeauftragten besteht darin, anhand der einschlägigen gesetzlichen Regelungen die jeweils für seine Einrichtung zulässigen ADV-Konstellationen und Voraussetzungen zu identifizieren.

ADV zulässig, und jetzt?

Kann eine Datenverarbeitung ausgelagert werden, ist ein schriftlicher Vertrag mit dem Dienstleister zu unterzeichnen. Die inhaltlichen Anforderungen variieren je nach Gesetz. Bei der vertraglichen Gestaltung sollte der Anforderungskatalog des § 11 Abs. 2 BDSG als Maßstab herangezogen werden, auch wenn das BDSG für die Einrichtung nicht gilt. Dieser ist so differenziert, dass er die Anforderungen der spezialgesetzlichen Regelungen regelmäßig mit umfasst.

Technisch-organisatorische Maßnahmen

Vor der Auslagerung und dem Beginn der Datenverarbeitung muss sich der AG von den durch den AN getroffenen technisch-organisatorischen Maßnahmen (TOM) überzeugen. Die Art der zu treffenden

Maßnahmen hängt maßgeblich von der konkreten Datenverarbeitung ab. Die erforderlichen Maßnahmen zur Einhaltung des Trennungsgebotes sind bei einem Rechenzentrumsbetrieb wesentlich komplexer als bei einer Aktenvernichtung.

Die TOM sind zwingend zum Bestandteil des ADV-Vertrages zu machen, da sie hierdurch für den AN verbindlich sind und durch den AG besser überprüft werden können. Zudem sollten diese möglichst detailliert dargestellt und geprüft werden, denn der Schutzbedarf wird regelmäßig sehr hoch sein.

Kurz-Checkliste Auftragsdatenverarbeitung und § 203 StGB

Einschlägige Gesetze?	
Auftragsdatenverarbeitung trotz § 203 StGB grundsätzlich erlaubt?	
ADV-spezifische Einschränkungen?	
Konkrete ADV zulässig?	
Gesetzeskonformer Vertrag zur ADV abgeschlossen?	
Wo ist der Vertrag in der Einrichtung hinterlegt?	
Sind die TOM differenziert dargestellt?	
Wurden die TOM vor Beginn der Datenverarbeitung geprüft?	
Wiederholungsprüfung der TOM während der ADV?	

Fazit

Sofern Daten in den Anwendungsbereich des § 203 StGB fallen, sind die Anforderungen an eine ADV von Bundesland zu Bundesland sehr unterschiedlich. Um es klar zu sagen: Ein und dieselbe Datenverarbeitung kann auf Seiten des AG in dem einen Bundesland eine Straftat darstellen, in dem anderen nicht. Diese unterschiedliche Behandlung ist wenig sachgerecht. Zudem stellt sich die Frage, ob eine fehlende Privilegierung der ADV im Bereich des § 203 StGB überhaupt noch zeitgemäß ist oder ob Krankenhäuser in einigen Bundesländern hier nicht vor enorme praktische Probleme gestellt werden.

Vertiefungshinweise im Handbuch „Datenschutz im Gesundheitswesen“ (DSiGW):

- Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel A/2.4 (Auftragsdatenverarbeitung und Outsourcing), Kapitel A/7.2.4 (Auftragsdatenverarbeitung und Outsourcing kirchliche Einrichtungen)

Babygalerie im Internet

Krankenhäuser mit Geburtenstationen stellen auf ihrer Website regelmäßig eine Babygalerie bereit. Neben dem Namen und dem Bild des Neugeborenen werden oftmals auch genaues Geburtsdatum, Gewicht, Größe und Kopfumfang veröffentlicht. Teilweise werden sogar die Vor- und Nachnamen der Eltern angegeben.
Als Grundlage für die Veröffentlichung dieser Daten kommt nur eine Einwilligungserklärung der stolzen Eltern in Betracht. Die Einwilligung muss dabei sehr detailliert auf den Umfang der Veröffentlichung eingehen. Es muss also bereits aus der Einwilligung klar hervorgehen, welche Daten genau und auch wie lange die Daten veröffentlicht werden. Zudem sind die Risiken darzustellen, die eine Veröffentlichung im Internet mit sich bringt.

Was hierbei oft nicht bedacht wird: Die Daten sind über die Website öffentlich zugänglich und können daher von jedermann eingesehen und gesammelt werden. In der Praxis machen sich Dritte diesen Umstand bereits zu eigen, indem sie mittels eines Skriptes die Textdaten von den Babygalerien abgreifen und beispielsweise auf einer eigenen Internetpräsenz darstellen. Machen Sie die Probe und geben einen weniger geläufigeren Namen eines Neugeborenen aus der Babygalerie bei Google ein. Teilweise kommt hierfür entgegen der ersten Erwartung sogar eine Rechtsgrundlage in Betracht. Denn § 28 Abs. 1 S. 1 Nr. 3 BDSG erlaubt einen erleichterten Umgang mit öffentlich verfügbaren Daten. Zwar ist das Foto weiterhin durch Regelungen des Kunsturhebergesetzes geschützt. Bei allen anderen Daten ist dies jedoch nicht so klar und eindeutig der Fall.
Wichtig ist, die Eltern mithilfe der Einwilligungserklärung vollumfänglich über diesen Umstand aufzuklären. Zudem sollte darauf hingewirkt werden, dass die Angaben zum Neugeborenen nicht mehr als Text, sondern ebenfalls als Bild eingebunden werden. Dies erschwert die Sammlung der Daten und deren Verwertung für andere Zwecke.

Vertiefungshinweise im Handbuch „Datenschutz im Gesundheitswesen“ (DSiGW):

- Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel C/12.1.10 (Veröffentlichung von Patienten- und Kundendaten)

Nutzung von Mitarbeiterfotos für den Internetauftritt: Nur mit schriftlicher Einwilligung

Sofern Gesundheitseinrichtungen für den eigenen Internetauftritt Fotos nutzen möchten, auf denen Mitarbeiter zu erkennen sind, ist hierfür grundsätzlich eine Einwilligung der abgebildeten Mitarbeiter erforderlich. Dies folgt nicht nur aus den jeweiligen Datenschutzgesetzen, sondern auch aus § 22 Kunsturhebergesetz.

Da das Kunsturhebergesetz die unbefugte Verbreitung von Personenbildnissen sogar unter Strafe stellt, ist bei der Einholung der Einwilligung besondere Vorsicht und Sorgfalt geboten. Hier stellte sich in der

Vergangenheit insbesondere eine Frage: Müssen Einwilligungen nach dem Kunsturhebergesetz schriftlich eingeholt werden oder nicht? Zwar ließ sich ein ausdrückliches Schriftformerfordernis nicht aus dem Kunsturhebergesetz entnehmen und auch das Zusammenspiel mit den datenschutzrechtlichen Vorschriften war nicht ganz klar. Allerdings musste bereits in der Vergangenheit dazu geraten werden, die entsprechenden Einwilligungserklärungen schriftlich einzuholen. Denn im Streitfall hätten bei rein mündlich oder gar konkludent erklärten Einwilligungen erhebliche Beweisprobleme bestanden.

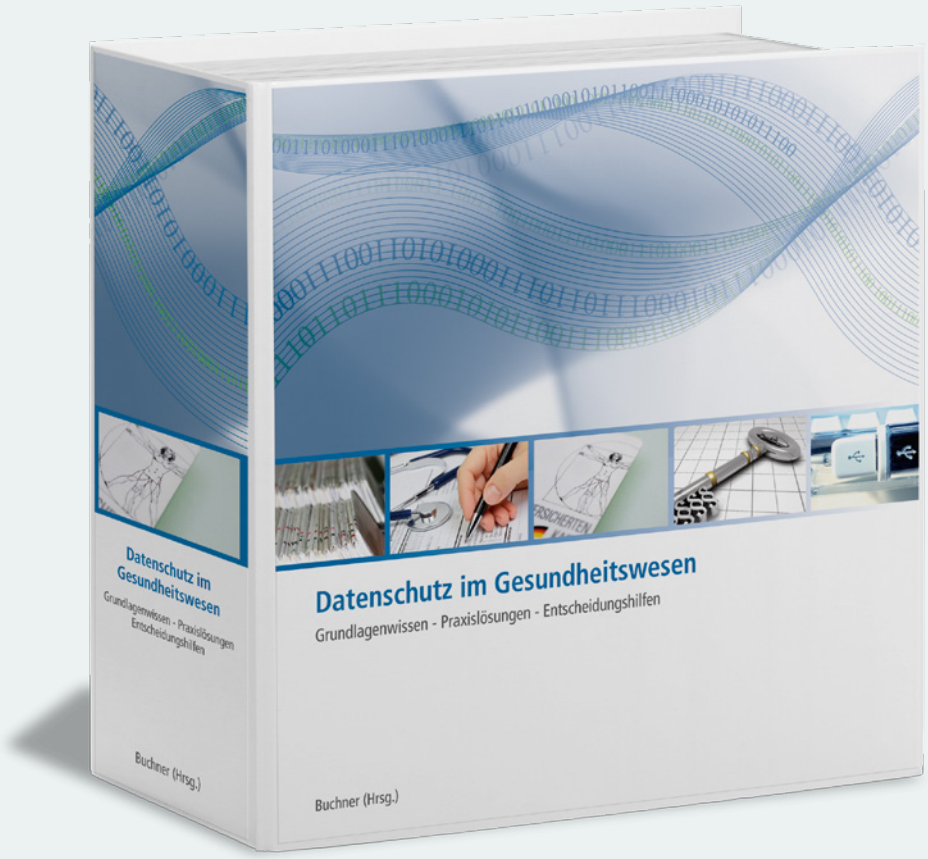
Das Bundesarbeitsgericht geht in einer Entscheidung aus dem Jahr 2014 (Urteil vom 11.12.2014, 8 AZR 1010/13) sogar einen Schritt weiter: Im Rahmen einer Abwägung kommt das Bundesarbeitsgericht zu dem Ergebnis, dass „auch und gerade“ im Arbeitsverhältnis die Einwilligung der Arbeitnehmer in die Veröffentlichung ihrer Bildnisse der Schriftform bedarf. Auch wenn die Begründung des Bundesarbeitsgerichts durchaus kritisch hinterfragt werden kann, zeigt diese Entscheidung einmal mehr, dass nur eine schriftliche Einwilligung Rechtssicherheit bringt.
Die oft genannten Ausnahmen des Einwilligungserfordernisses (Bildnisse der Zeitgeschichte, Personen als Beiwerk einer Landschaft, Bilder von Versammlungen) sind übrigens ebenfalls mit Vorsicht zu betrachten. Denn jeder dieser Ausnahmetatbestände muss sorgfältig geprüft werden. Ein Beispiel ist das Gruppenfoto der letzten Betriebsfeier, die regelmäßig gerade keine Versammlung im Sinne des Kunsturhebergesetzes darstellt.

Vertiefungshinweise im Handbuch „Datenschutz im Gesundheitswesen“ (DSiGW):

- Datenschutz im Gesundheitswesen (AOK-Verlag), Kapitel C/12.1.10 (Veröffentlichung von Patienten- und Kundendaten)

Handbuch „Datenschutz im Gesundheitswesen“

Neben diesem kostenlosen Fachinformationsdienst bieten wir ein umfangreiches Handbuch „Datenschutz im Gesundheitswesen“ an. In diesem finden Sie vertiefende Hinweise zu den Themen unseres Fachinformationsdienstes. Wir haben unseren Informationsdienst so gestaltet, dass die jeweiligen Themen für sich stehen und Sie keiner ergänzenden Lektüre bedürfen. Davon unabhängig leistet unser Fachbuch eine wichtige Hilfe für den Praxisalltag und stellt viele der im Fachinformationsdienst behandelten Themen nochmals umfassender und ausführlicher dar.



Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.300 Seiten Inhalt
ISBN: 978-3-553-43000-5
Preis 179.- inkl. MwSt.

Uneingeschränkter Online-Zugriff auf alle Arbeitshilfen inkl. 3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 74,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.