AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe März 2017 | Seite 1

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

INHALT

Deutschlands beste Klinik-Websites: Zweiter Datenschutz-Check

Um auf die Wichtigkeit einer gut konzipierten Website hinzuweisen, werden in Deutschland seit 14 Jahren im Rahmen eines regelmäßigen Wettbewerbs die besten Klinik-Websites gekürt.

Sven Venzke-Caprarese

Um darüber hinaus darauf hinzuweisen, dass bei der Konzeption einer Klinik-Website auch datenschutzrechtliche Anforderungen eingehalten werden müssen, haben wir im vergangenen Jahr die Top 10 der deutschen Klinik-Websites einem Datenschutz-Check unterzogen. Damals mit ernüchterndem Ergebnis. Ende 2016 wurden nun zum 14. Mal Deutschlands beste Klinik-Websites gekürt. Wir haben dies zum Anlass genommen, unseren Datenschutz-Check auch in diesem Jahr durchzuführen. Dabei vergleichen wir die Ergebnisse des Websitechecks mit denen des Vorjahres und nennen die Websites, die aus datenschutz- und telemedienrechtlicher Sicht besonders gut abgeschnitten haben.

Klinik-Website und HTTPS-Verschlüsselung

Im Gegensatz zum Datenschutz-Check des Vorjahres ist die Zahl der Klinik-Websites, die auf eine verschlüsselte Datenübertragung per HTTPS setzen, deutlich gestiegen:

- Sechs der zehn geprüften Top 10 Klinik-Websites verschlüsselten alle Übertragungen durchgängig per HTTPS. Eine der geprüften Klinik-Websites nutzte verschlüsselte Übertragungen per HTTPS immerhin noch auf allen Seiten, welche die Eingabe personenbezogener Daten ermöglichten. Zum Vergleich: In unserem letzten Datenschutz-Check verwendeten gerade einmal zwei von

zehn Klinik-Websites verschlüsselte Datenübertragungen per HTTPS – auf den ersten Blick also eine deutliche Steigerung von Datenschutz und Datensicherheit.

- Drei der zehn geprüften Websites unterstützten jedoch keinen Aufruf per HTTPS. Gleichzeitig enthielten diese Klinik-Websites Eingabeformulare, über die Websitebesucher personenbezogene Daten eingeben konnten. Als besonders kritisch fiel dabei eine Website auf, die Ärzte auf einer unverschlüsselten Formulareingabeseite aufforderte, Patientendaten einzugeben. Das entsprechende Eingabeformular enthielt dabei u. a. Felder für den Namen des Patienten, Diagnose, Nebendiagnose, Diagnostik-Staging, Verlauf, Medikamente, Tumormarker und Medikation. Zwar ist es durchaus möglich, die Inhalte von unverschlüsselt ausgelieferten Eingabeformularen verschlüsselt zu übertragen (indem z. B. als Zieladresse für die zu übermittelnden Formulardaten eine HTTPS-Adresse verwendet wird). Im vorliegenden Fall fanden sich hierfür im Quelltext der Website jedoch keine Anhaltspunkte. Im Gegenteil: Eine Analyse des Quelltextes ergab, dass diese sensiblen Formularinhalte unverschlüsselt übertragen worden wären.

Im Ergebnis erfüllten sieben der geprüften Websites die Anforderungen unseres Datenschutz-Checks. Drei der Top 10 Klinik-Websites schieden jedoch bereits bei diesem ersten Prüfpunkt aus dem Rennen aus.

PRAXISTIPP: Eine unverschlüsselte Übertragung von personenbezogenen Daten ist nicht nur nicht mehr zeitgemäß. Eine solche Datenübertragung verstößt regelmäßig auch gegen die gesetzlichen Anforderungen aus § 13 Abs. 7 Telemediengesetz und § 9 Bundesdatenschutzgesetz. Betreiber von

Klinik-Websites sollten im Jahr 2017 darüber nachdenken, ihren kompletten Internetauftritt auf HTTPS umzustellen. Hierdurch können nicht nur Webformulare abgesichert werden. Darüber hinaus kann die Sicherheit der Kommunikation der gesamten Websiteinhalte mithilfe einer durchgängigen HTTPS-Verschlüsselung deutlich erhöht werden. In der Praxis sollte dabei auf Folgendes geachtet werden:

- Als Verschlüsselungsstandard sollte TLS 1.2 verwendet werden.
- Die Auslieferung über HTTPS sollte erzwungen werden (jeder HTTP-Aufruf sollte also auf HTTPS umgeleitet werden).

Impressum und Datenschutzerklärung

Alle geprüften Websites verfügten in der Desktop-Standardansicht über ein rechtskonform platziertes Impressum. Auch die nach § 13 TMG vorgeschriebene Datenschutzerklärung war auf allen Websites vorhanden, wobei drei Websites die Datenschutzerklärung nicht als separaten Punkt, sondern innerhalb des Impressums platzierten (was die Auffindbarkeit erschwerte).

Wie bereits im letzten Datenschutz-Check wirkte sich auch dieses Jahr eine häufige Fehlerquelle praktisch aus: Das responsive Design (also die spezielle Ansicht für Smartphones) führte auf einer Website dazu, dass weder das Impressum noch die Datenschutzerklärung auffindbar waren. An dieser Stelle schied auch in diesem Jahr eine weitere Website unseres Datenschutz-Checks aus. Sechs blieben im Rennen.

Google Analytics, Piwik und mehr

Acht der zehn überprüften Websites verwendeten Webtracker, darunter auch häufig Google Analytics und

Piwik. Wie bereits im letzten Datenschutz-Check zeigten sich auch dieses Mal bei der datenschutzkonformen Implementierung dieser Analysetools erhebliche Defizite:

- Eine Website nutzte Piwik, ohne darauf in der Datenschutzerklärung hinzuweisen oder eine Möglichkeit zum Widerspruch zu bieten. Diese Website war jedoch ohnehin bereits im Rahmen der vorherigen Prüfpunkte des Datenschutz-Checks ausgeschieden.
- Vier Websites wiesen Defizite in der Implementierung von Google Analytics auf. Teilweise wurde die vom Hamburgischen Datenschutzbeauftragten vorgeschriebene Widerspruchsmöglichkeit per Google-Opt-Out-Cookie nicht angeboten, was dazu führt, dass Nutzer von Smartphones dem Tracking nicht widersprechen können. Darüber hinaus wurde häufig vergessen, im Quelltext der Website die Anonymisierung der IP-Adresse zu aktivieren, obwohl dies in der Datenschutzerklärung noch entsprechend erwähnt wurde. Eine dieser vier Websites mit Implementierungsdefiziten bei Google Analytics war bereits im Vorfeld ausgeschieden, so dass an dieser Stelle „nur“ drei weitere Websites aus dem Rennen genommen werden mussten.
- Im Gegensatz zum vorherigen Datenschutz-Check konnte dieses Jahr auf vielen Websites die Verwendung von zusätzlichen Trackingtechnologien festgestellt werden, die vermutlich Werbezwecken dienen. Hervorzuheben ist, dass drei der überprüften Websites bei Aufruf eine Verbindung zum Google-DoubleClick-Netzwerk aufbauten. Auf mindestens einer dieser Websites schienen insofern Remarketingzwecke verfolgt zu werden. Keine der Websites erläuterte die Verbindung zum DoubleClick-Netzwerk in der Datenschutzerklärung. Zwei Websites nutzten darüber hinaus weitere Trackingtechnologien, die nicht in der Datenschutzerklärung erwähnt wurden. Alle Websites, die Trackingtechnologien zu Werbezwecken nutzten, waren jedoch bereits bei einem der vorhergehenden Prüfpunkte ausgeschieden.

Zwischenfazit

Drei von zehn Websites schieden bereits wegen fehlender HTTPS-Verschlüsselung aus. Eine Website schied wegen fehlender Datenschutzerklärung im responsiven Design aus. Drei weitere Websites schieden wegen fehlerhafter Implementierung von Google Analytics aus. Somit haben drei Klinikwebseiten bisher alles richtig gemacht.

Social Plugins

Auf keiner der verbleibenden Websites konnte die unmittelbare Einbindung von Social Plugins festgestellt werden. Eine Website nutzte Social Plugins und verwendete hierzu die von den Aufsichtsbehörden anerkannte Shariff-Lösung.

Externe Schrift- und Scriptbibliotheken

Insgesamt neun der überprüften Websites, darunter auch die drei verbleibenden, nutzten externe Schrift- oder Scriptbibliotheken. Häufig anzutreffen waren an dieser Stelle Verbindungsaufnahmen zum Nachladen der entsprechenden Dateien von Google-Servern.

Die Einbindung externer Schrift- und Scriptbibliotheken führt dazu, dass jeder Websiteaufruf automatisch auch eine Verbindung zum Anbieter der entsprechenden Dateien auslöst. Ob und ggf. zu welchen Zwecken Betreiber von entsprechenden Schrift- bzw. Scriptbibliotheken diese Daten nutzen, ist unklar. Die Möglichkeiten, die hier zumindest theoretisch bestehen, sind immens. Zwar steht die Einbin-

dung von externen Schrift- und Scriptbibliotheken noch nicht im Fokus von Aufsichtsbehörden. Genau genommen könnte aber die Kritik, die seit Jahren in Bezug auf die unmittelbare Einbindung von Social Plugins vorgebracht wird, auch auf diesen Sachverhalt übertragen werden.

Da jede der drei verbleibenden Websites an dieser Stelle externe Bibliotheken nutzte, konnte sich keine Website an dieser Stelle von den anderen absetzen.

IP-Adresse

Bei den verbleibenden drei Websites prüften wir daher die Inhalte der Datenschutzerklärung etwas näher und legten einen Schwerpunkt auf die Darstellung der Verarbeitung der IP-Adresse:

- Die erste Datenschutzerklärung, die wir prüften, stellte dar, dass die IP-Adressen der Besucher nach Beendigung des Websitebesuchs anonymisiert werden.
- Die zweite Datenschutzerklärung traf keine näheren Aussagen zum Umgang mit IP-Adressen der Besucher.
- Die dritte Website informierte über eine Datenspeicherung der IP-Adressen zu Sicherheitszwecken für die Dauer von sechs Monaten. Selbst unter Berücksichtigung der aktuellen Diskussion zur Speicherung von IP-Adressen (vgl. unseren Dezember-Newsletter) erschien uns dieser Zeitraum als deutlich zu lang. Eine weitere Website schied somit auf der Zielgeraden aus.

Videoplayer

Auf den beiden verbleibenden Websites waren jeweils Videos abrufbar. Eine Website bot hierfür eine datenschutzrechtlich unbedenkliche Lösung an und spielte die Videos in einem eigenen Videoplayer ab. Die zweite Website verwendete eingebettete YouTube-Videos, ohne den erweiterten Datenschutz-Modus zu aktivieren. Da dies auch die Website war, die keine Aussagen zu dem Umgang mit den IP-Adressen der Besucher machte, verfestigte sich der zweite Platz.

Die ersten beiden Plätze

In unserem Datenschutz-Check, belegte Platz 1 die Website des Universitätsklinikums Hamburg- Eppendorf (https://www.uke.de).

Knapp dahinter folgt die Website der Martini-Klinik am UKE (https://www.martini-klinik.de).

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.

Vertiefungshinweise im Handbuch DSiGW:

Datenschutz im Gesundheitswesen (AOK Verlag GmbH), Kapitel C/12 (Der Internetauftritt).

Videoüberwachung

Gerade in großen Gesundheitseinrichtungen ist der Einsatz von Videoüberwachungstechnik ein wichtiger Faktor, um trotz personeller Unterbesetzung wichtige Aufgaben wahrnehmen zu können. Dabei deckt der medizinische Kernbereich nur einen Teil ab. Vor allem bei der Überwachung von schwer zugänglichen Räumlichkeiten, denen ein besonderes Gefährdungspotential immanent ist, erfolgt zunehmend der Rückgriff auf Kameras.

Dr. Sebastian Ertel

Rechtliche Anforderungen

Aufgrund des datenschutzrechtlichen Grundsatzes des Verbots der Datenverarbeitung mit Erlaubnisvorbehalt ist der Einsatz einer Videoüberwachung nur zulässig, wenn diese durch eine entsprechende gesetzliche Grundlage legitimiert ist. Maßgeblich für die Ermittlung der richtigen Rechtsgrundlage ist zunächst, ob der Einsatz der Videoüberwachung in einem öffentlich zugänglichen oder in einem nicht öffentlich zugänglichen Raum stattfinden soll.

Öffentlich zugänglich

Öffentlich zugänglich sind Räume, die ihrem Zweck nach dazu dienen, von unbestimmt vielen Personen betreten zu werden, ohne dass Zugangsbarrieren überwunden werden müssen.

Aktueller Stand zur Anpassung des BDSG

Im Januar-Newsletter hatten wir über die Anpassung der nationalen Gesetze im Zuge der Einführung der DS-GVO berichtet. In Bezug auf das Gesetz zur Anpassung des Datenschutzrechts (BDSG neu) existiert seit Anfang Februar 2017 ein offizieller Gesetzesentwurf der Bundesregierung. Eine erste Beratung im Bundestag (Bundestagsdrucksache 18/11325) fand am 9.3.2017 statt. Als Ergebnis dieser 1. Lesung wurde die Überweisung des Gesetzesentwurfs in die zuständigen Ausschüsse des Bundestags beschlossen. Einen Tag später wurde der Gesetzesentwurf im Bundesrat (Bundestagsdrucksache 110/17) am 10.3.2017 beraten und die Stellungnahme des Bunderats zum Gesetzesentwurf beschlossen.

Es ist davon auszugehen, dass der bisherige Gesetzesentwurf der Bundesregierung, der sich nun in den Ausschüssen des Bundestags befindet, noch erhebliche Änderungen erfahren wird, da die Stellungnahme des Bundesrats viele Änderungsvorschläge im Detail enthält. Ein Termin für die 2. und 3. Lesung im Bundestag steht noch nicht fest, kann jedoch frühestens für Ende April erwartet werden. Die dann gültige Fassung könnte im zweiten Durchgang somit frühestens ab Mai wieder durch den Bundesrat beraten werden (z. B. in der 957. Plenarsitzung am 12.5.2017). Da es sich um ein Zustimmungsgesetz handelt, hat der Bundesrat dann die Möglichkeit, dem Gesetz zuzustimmen, die Zustimmung zu verweigern oder den Vermittlungsausschuss anzurufen.

Die Videoüberwachung im öffentlich zugänglichen Raum ist durch § 6b BDSG geregelt. Diese ist zulässig, zur

- Aufgabenerfüllung öffentlicher Stellen,
- Wahrnehmung des Hausrechts oder
- Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.

Darüber hinaus dürfen keine schutzwürdigen Interessen der Betroffenen überwiegen. Entsprechende Regelungen finden sich in den Landesdatenschutzgesetzen sowie im Datenschutzgesetz der Evangelischen (§ 7a DSG-EKD) und der Katholischen (§ 5a KDO) Kirche.

Gliederung Vorabkontrolle

- Einführung und Ergebnis
- Datenverarbeitende Stelle
- Zweck und Umfang der Videoüberwachung
- Eingesetzte Technik und Qualität der Aufzeichnung
- Rechtsgrundlage der Videoüberwachung
- Kreis der Betroffenen
- Kreis der zugangsberechtigten Personen
- Art der Überwachung
- Abwägung der gegenläufigen Interessen
- Technische und organisatorische Sicherheitsmaßnahmen
- Beteiligung der Mitarbeitervertretung
- Dauer der Überwachung

Nicht öffentlich zugänglich

Nicht öffentlich zugänglich sind Bereiche, die für die Allgemeinheit unzugänglich sind. Hierzu gehören Gelände oder Gebäude, die nur mit individueller Erlaubnis (z. B. durch Benutzung eines zuvor ausgegebenen Schlüssels, nach Betätigen eines Türöffners durch den Pförtner oder nach Kontrolle durch den Wachdienst) betreten werden können.

Die Videoüberwachung nicht öffentlich zugänglicher Bereiche ist nicht gesetzlich geregelt. Hier ist ein Rückgriff auf die allgemeinen Regelungen, insbesondere §§ 28, 32 BDSG, zu nehmen. Entsprechende Normen finden sich in den Landesdatenschutzgesetzen sowie im Datenschutzgesetz der Evangelischen (§§ 4, 5, 24 DSG-EKD) und der Katholischen (§§ 9, 10, 10a KDO) Kirche.

Vorabkontrolle

Vor der Einführung der Videoüberwachung ist das Verfahren einer Vorabkontrolle zu unterziehen, wenn der Einsatz besondere Risiken für die Rechte und Freiheiten der Betroffenen bedeutet. Die Vorabkontrolle, die unter der DSGVO Datenschutz-Folgenabschätzung heißen wird, dient der Prüfung, ob das geplante Vorhaben überhaupt rechtskonform realisiert werden kann bzw. welche Maßnahmen technischer und organisatorischer Art getroffen werden müssen.

Neben dem Schwerpunkt der rechtlichen Bewertung, unter Berücksichtigung der Notwendig- und Verhältnismäßigkeit sowie der Risiken für die Rechte und Freiheiten der betroffenen Personen, umfasst die Vorabkontrolle eine systematische Beschreibung der geplanten Datenverarbeitungsvorgänge, der Verarbeitungszwecke sowie ggfls. weiterer Interessen der verantwortlichen Stelle.

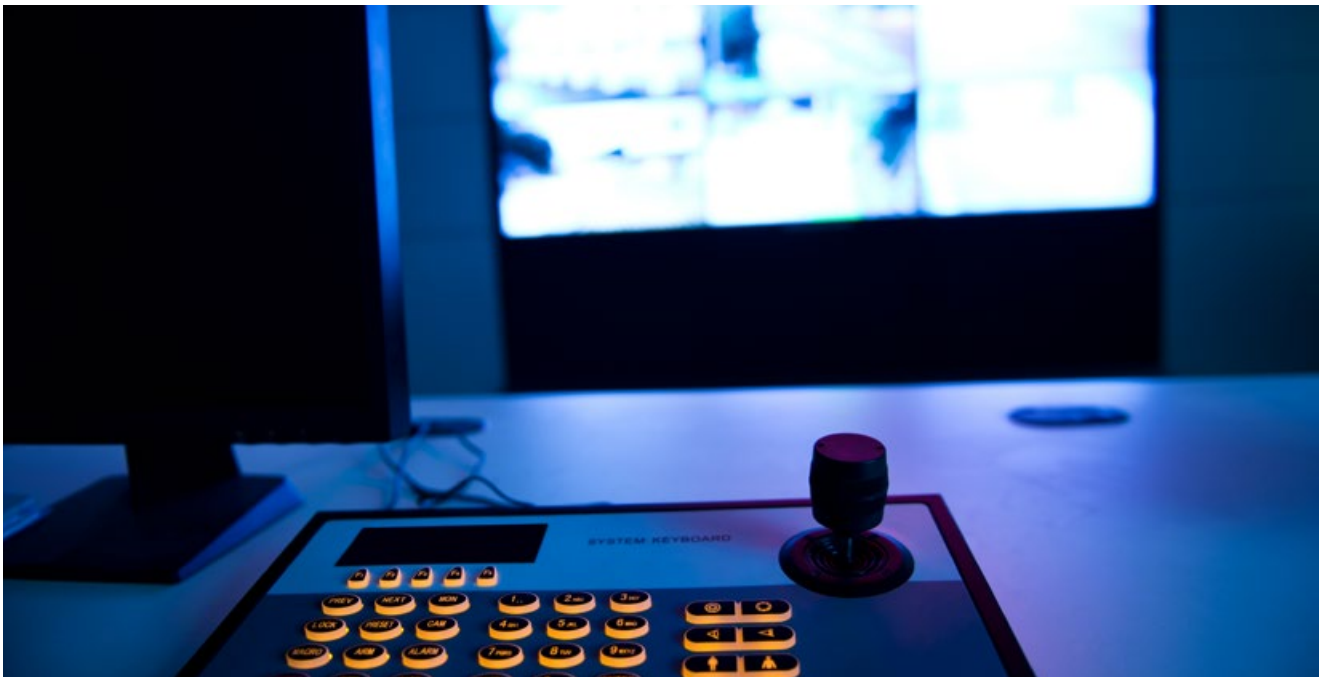
Darüber hinaus sind die Maßnahmen zu definieren, die den identifizierten Risiken entgegengestellt werden. Hierzu gehören insbesondere die Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird.

Die Durchführung einer Vorabkontrolle ist verpflichtend und elementrare Zulässigkeitsvoraussetzung für die Videoüberwachung.

Weitere Anforderungen

Hinweispflichten

Eine stattfindende Videoüberwachung muss hinreichend erkennbar sein. Dies erfolgt in der Regel durch die Verwendung eines entsprechenden Hinweisschildes nach DIN 33450. Dieses muss so angebracht sein, dass es dem Betroffenen unmittelbar zur Kenntnis gelangt, beispielsweise auf



Augenhöhe. Zudem muss ein Schild an jedem Zugang angebracht werden, über den man in den überwachten Bereich gelangen kann. Darüber hinaus muss das Schild Informationen zur verantwortlichen Stelle enthalten, sofern diese nicht eindeutig erkennbar ist. Die Erkennbarkeit der verantwortlichen Stelle ist in einem Medizinischen Versorgungszentrum regelmäßig unklar. In diesem Fall sind Name und Kontaktdaten (mindestens E-Mail oder Telefonnummer) zu benennen.

Speicherdauer

Sofern eine Speicherung der Videodaten erfolgt, stellt sich die Frage der zulässigen Speicherdauer. Nachdem die Aufsichtsbehörden früher von einer grundsätzlichen Speicherhöchstdauer von 72 Stunden ausgingen, wird nunmehr unter Verweis auf die Bundestagsdrucksache 14/5793 (Beschlussempfehlung zum Gesetzentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes 2001) die Maximaldauer mit 48 Stunden beziffert. Durch Betriebs- oder Dienstvereinbarungen kann diese Frist individuell und in einem angemessenen Umfang verlängert werden. Nach § 7a Abs. 5 S. 1 DSG-EKD wird die grundsätzliche Speicherdauer mit einer Woche definiert.

Von diesen Speicherfristen unberührt bleiben die Aufzeichnungen, die über den Zeitraum hinaus, etwa zur Aufklärung einer Straftat, benötigt werden. Diese sind entsprechend rechtzeitig zu sichern.

Verfahrensverzeichnis

Der Einsatz der Videoüberwachung ist in das Verfahrensverzeichnis aufzunehmen und so zu beschreiben, dass der Betroffene über die verschiedenen Datenverarbeitungen hinreichend informiert wird, aber andererseits nicht so viele Informationen erhält, dass er diese zur Umgehung des Systems nutzen kann. Die Evangelische Kirche sieht in § 7a Abs. 7 DSG-EKD das Führen eines separaten Verfahrensverzeichnisses für die Videoüberwachung vor, das zur Einsichtnahme von jedermann vorgehalten werden muss.

Abwägung

Im Rahmen der Zulässigkeitsprüfung einer Videoüberwachung sind die Interessen der verantwortlichen Stelle an der Einführung gegenüber den Interessen der Betroffenen abzuwägen. Von der Ausgangslage her überwiegt zunächst grundsätzlich das Interesse der Betroffenen, die Videoüberwachung nicht einzuführen. Durch verschiedene Maßnahmen kann dieser Grundsatz zugunsten der verantwortlichen Stelle verschoben werden.

Erfasste Bereiche

Eine Videoüberwachung ist unzulässig, wenn die **Intimsphäre** der Betroffenen berührt ist. Das ist beispielsweise bei der Erfassung von Umkleiden, Waschräumen, Toiletten und Sozialräumen der Fall. Zum Teil darf auch der Zugang zu diesen Räumen nicht überwacht werden (Möglichkeit der unzulässigen Verhaltens- und Leistungskontrolle). In diesem Zusammenhang: Unzulässig ist die Erfassung des Raumgespräches. Das Mithören kann den Straftatbestand des § 201 StGB (Verletzung der Vertraulichkeit des Wortes) erfüllen.

Dauer der Überwachung

Ebenfalls relevant ist der Zeitraum der Überwachung. Erfolgt diese nur außerhalb der üblichen Geschäftszeiten/des üblichen Publikumsverkehrs, ist die Eingriffsintensität wesentlich geringer als bei einer 24–Stunden-Überwachung.

Livebild/ Aufzeichnung

Ein weiterer Abwägungsaspekt betrifft die Darstellung des erzeugten Bildes: Erfolgt diese lediglich als Livebild, auf welches unter Umständen nur bei Bedarf zugegriffen wird oder werden die Daten aufgezeichnet? Die Intensität des Eingriffs in die Rechte der Betroffenen ist bei einem Livebild wesentlich geringer als bei einer Speicherung. So ist die Überwachung des OP-Aufwachraums als Livebild ohne Speicherung regelmäßig zulässig (22. Tätigkeitsbericht LfD Bayern, Ziffer 13.2.2), die Überwachung eines Krankenhausaufzuges als Livebild nur bei konkreten Anlässen (technischer Defekt), nicht aber permanent (24. Tätigkeitsbericht LfD Bayern, Ziffer 7.3).

Technisch-organisatorische Maßnahmen

Darüber hinaus muss durch technisch-organisatorische Maßnahmen der Schutz der Daten vor unbefugter Kenntnisnahme gewährleistet werden.

Zutritts- und Zugangskontrolle

Der Zugang zu Livemonitoren, zu den Videoservern und sonstigen Datenträgern muss genau definiert sein. Die Monitore sind so aufzustellen bzw. auszustatten (Sichtschutzfolie), dass Unbefugte diese nicht einsehen können. Server bzw. Datenträger sind so aufzustellen, dass der Zugang nur einem begrenzten und zuvor definierten Personenkreis möglich ist. Die Speichermedien sollten verschlüsselt sein. Der Zugriff auf die gespeicherten Daten ist durch eine Benutzerkennung mit Passwort abzusichern. Die Anbindung der Kameras an das Unternehmensnetz muss hinreichend abgesichert sein.

Zugriffskontrolle

Der Zugriff auf die Videodaten muss so eingeschränkt sein, dass sich dies auf die Erfüllung der jeweiligen Aufgaben beschränkt. Ferner ist sicherzustellen, dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können. Der Zugriff auf das Videomaterial sollte ausschließlich nach dem 4-Augen-Prinzip, beispielsweise mit einem geteilten Passwort (je zur Hälfte im Besitz des Arbeitgebers und der Mitarbeitervertretung), erfolgen.

Weitergabekontrolle

Eine Datenweitergabe ist auszuschließen. Sofern im konkreten Einzelfall Daten an Strafverfolgungsbehörden oder Versicherer weitergegeben werden sollen, sollte dies mittels verschlüsseltem Datenträger (CD, DVD, USB-Stick) realisiert werden. Eine Weitergabe per unverschlüsselter Mail oder FTP sollte unterbunden werden.

Eingabekontrolle

Zugriffe auf das gespeicherte Datenmaterial sollten unter Angabe des Zwecks dokumentiert werden.

Exkurs: Kameraattrappe

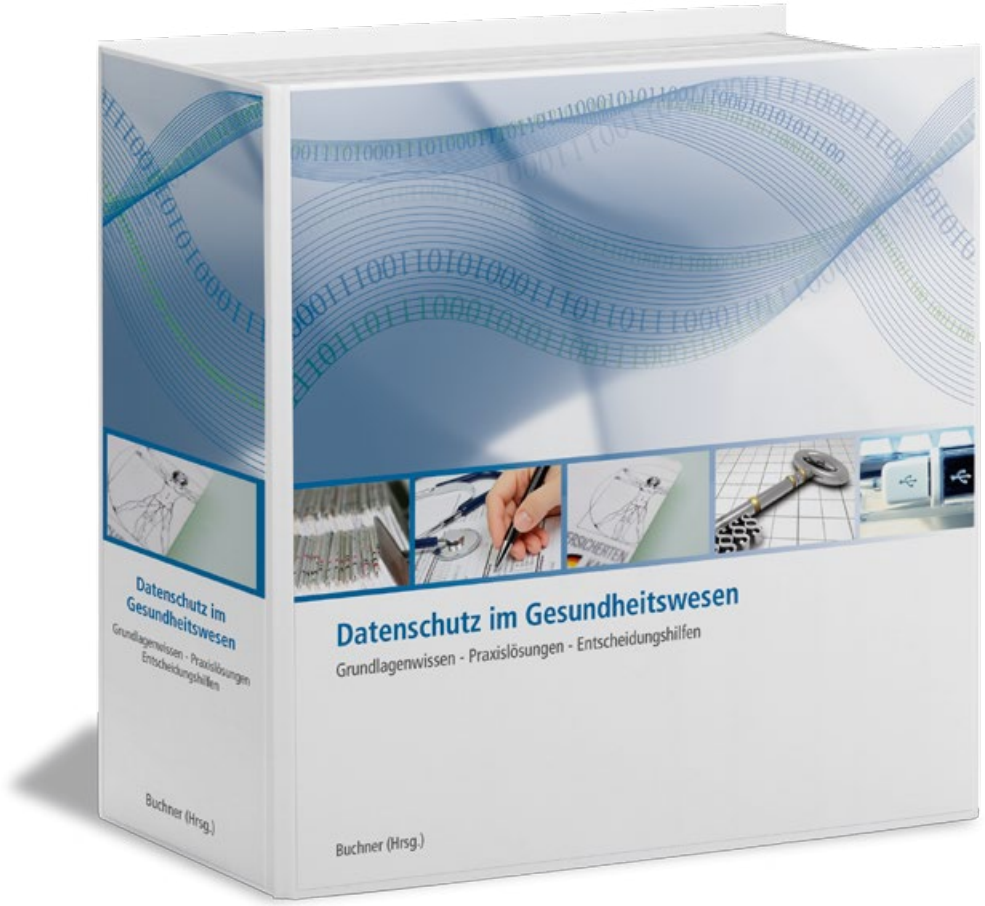
Häufig werden Kameraattrappen eingesetzt, um unter dem Aspekt der Abschreckung die Begehung von Straftaten zu verhindern. Da diese Attrappen keine (personenbezogenen) Daten erzeugen, ist Datenschutzrecht eigentlich nicht einschlägig.

Die Aufsichtsbehörden bewerten den Einsatz einer Kameraattrappe im Lichte des Volkszählungsurteils von 1984 und sehen wegen des psychischen Überwachungsdrucks, der durch die Attrappe ausgelöst wird, einen Grundrechtseingriff, der einer gesetzlichen Grundlage bedarf (30. Tätigkeitsbericht LfD Baden-Württemberg, Ziffer 2.1). Im Evangelischen Datenschutzrecht ist der Einsatz von Kameraattrappen explizit geregelt (§ 7a Abs. 9 DSG-EKD).

Im Ergebnis sind Kameraattrappen wie echte Kameras zu bewerten, sodass für diese dieselben Anforderungen, aufgrund des fehlenden Datenmaterials in abgeschwächter Form, bestehen.

Gliederung Verfahrensbeschreibung Videoüberwachung

- Einführung und Ergebnis
- Einführung
- Datenverarbeitende Stelle
- Zweck der Videoüberwachung
- Rechtsgrundlage der Videoüberwachung
- Kreis der Betroffenen
- Kreis der zugangs-, zutritts- und zugriffberechtigten Personen
- Abwägung
- Art der Überwachung



Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.500 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 79,90 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.