AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Mai/Juni 2018 | Seite 1

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

INHALT

Neuregelung des § 203 StGB – Alles neu, alles gut?

Eine der letzten Amtshandlungen vor Ende der Legislaturperiode 2017 war die Neuregelung des § 203 StGB. Dieser Paragraph regelt die Strafbarkeit von Berufsgeheimnisträgern bei unbefugter Offenbarung anvertrauter Geheimnisse.

Dr. Sebastian Ertel

Diese Regelung dient dem besonderen Schutz der Vertrauensbeziehung zwischen Geheimnisinhaber und Berufsgeheimnisträger ...

... und stellte Letztere regelmäßig vor Probleme, wenn aus personellen, fachlichen oder ökonomischen Gründen auf die Kompetenzen externer Dienstleister zurückgegriffen werden soll.

In der Realität ist eine Gesundheitseinrichtung ohne externe Dienstleister kaum noch vorstellbar. Zu komplex sind bestimmte Prozesse geworden und erfordern ein Höchstmaß an informationstechnischem Know-How.

Durch den neu geschaffenen § 203 Abs. 3 StGB machen sich die Angehörigen eines medizinischen Heilberufes nicht strafbar, wenn geheim zu haltende Daten gegenüber sonstigen Personen offenbart werden, die an der beruflichen oder dienstlichen Tätigkeit des Berufsgeheimnisträgers mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist.

Alles gut?

Leider nein. Bereits im Vorfeld der Änderung des § 203 StGB machten die Datenschutzbehörden deutlich, dass sie mit der Neuregelung nicht glücklich sind. Nach ihrer Auffassung [ist es] „weder mit dem Schutzzweck von § 203 StGB vereinbar noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen.“ [1)]

Was bedeutet das?

Soll ein Dienstleister eigenverantwortlich eine Datenverarbeitung durchführen, bedarf es trotz geändertem § 203 StGB einer datenschutzrechtlichen Einwilligung. Dementsprechend wird zunehmend die Auffassung vertreten, dass eine Einbindung eines Dienstleisters ohne Einwilligung des Geheimnisträgers einen datenschutzrechtlichen Verstoß darstellt, unabhängig von der konkreten Ausgestaltung der Dienstleistung. [2)]

Die Darstellung ist grundsätzlich richtig. Soll der externe Dienstleister eigenverantwortlich, mithin weisungsfrei, die Datenverarbeitung durchführen, greift der datenschutzrechtliche Grundsatz des Verbots der Datenverarbeitung mit Erlaubnisvorbehalt. Dieser besagt, dass eine Datenverarbeitung bzw. eine Datenübermittlung nur dann zulässig ist, wenn eine gesetzliche oder vertragliche Grundlage besteht oder der Betroffene in die Datenverarbeitung eingewilligt hat.

Allerdings wird häufig verkannt bzw. nicht erwähnt, dass im Datenschutzrecht noch die Figur der Auftrags(-daten)verarbeitung existiert. Diese ist dadurch geprägt, dass der Dienstleister streng weisungsgebunden ist und ohne mit den Daten bzw. der Datenverarbeitung eigene Interessen zu verfolgen seine Dienstleistung erbringt. In diesem Fall verbleibt die Verantwortlichkeit für die Datenverarbeitung beim Auftraggeber. Der Dienstleister wird, bildlich gesprochen, wie eine Fachabteilung des Auftraggebers angesehen. Die Auftragsverarbeitung prägend ist, dass die Bereitstellung der Daten gerade nicht im Rahmen der Datenübermittlung erfolgt. Es bedarf daher bei der Auftragsverarbeitung weder einer gesetzlichen Grundlage noch einer datenschutzrechtlichen Einwilligung des Betroffenen. Der Dienstleister muss mittels eines umfangreichen Vertrages zur Auftragsverarbeitung an den Auftraggeber „gekettet“ werden.

Erbringt der Dienstleister seine Arbeit daher in Form der Auftragsverarbeitung, dürfen die dem Berufsgeheimnis unterliegenden Daten vom Dienstleister verarbeitet werden, ohne dass es einer Einwilligung des Betroffenen bedarf und ohne dass eine Strafbarkeit nach § 203 StGB im Raum steht. Es müssen lediglich die Anforderungen der Auftragsverarbeitungen (§ 11 BDSG a.F., Art. 28 DSGVO) und des § 203 Abs. 3 StGB gewahrt werden. Dies wird auch von einigen Aufsichtsbehörden so dargestellt. [3)]

Alles gut?

Obwohl die datenschutzrechtliche Thematik ausdiskutiert erscheint, ist das Thema wohl noch nicht abgeschlossen. Als nächstes Hindernis soll nunmehr die Berufsordnung der Ärzte wirken. Nach dieser sind Ärzte und Ärztinnen zur Offenbarung von Berufsgeheimnissen nur dann befugt, wenn sie von der Schweigepflicht entbunden worden sind oder eine gesetzliche Regelung die Offenbarung erlaubt.

Also keine Strafbarkeit, kein Datenschutzverstoß, aber eine Verletzung der Berufsordnung?

Auf Rückfrage wurde seitens der Bundesärztekammer erklärt, dass sich derzeit mit der Thematik auseinandergesetzt wird. Die Herausforderung bestünde darin, eine ausgewogene und alle Interessen berücksichtigende Regelung zu schaffen. Mit einer entsprechenden Aussage sei Mitte des Jahres zu rechnen.

Und nun?

Die Einbindung externer IT-Dienstleister wird in vielen Fällen auch weiterhin unumgänglich sein, um die Heilbehandlung des Patienten adäquat zu gewährleisten – nicht auszudenken, welche Folgen Softwareprobleme in Folge mangelnden Supports haben könnten. Strafrechtlich und datenschutzrechtlich ist dies bei Beachtung der entsprechenden Voraussetzungen unproblematisch. Hinsichtlich der Berufsordnung besteht ein Restrisiko. In diesem Zusammenhang ist auch zu berücksichtigen, dass kein Fall publik geworden ist, in dem entsprechende berufsrechtliche Sanktionen verhängt worden sind.

1) Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 15.3.2017.

2) Vergl. Dr. Eugen Ehmann, Externe Dienstleister und ärztliche Schweigepflicht – so wird es nichts werden!, ZD 2017, 201.

3) Berliner Beauftragte für Datenschutz und Informationsfreiheit, Tätigkeitsbericht 2017, Punkt 7.6.

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

Deutschlands beste Klinik-Websites: Dritter Datenschutz-Check

Wie bereits in den letzten Jahren wurden auch Anfang dieses Jahres die Gewinner des Awards für „Deutschlands Beste Klinik-Website“ unter der Schirmherrschaft von Novartis gekürt. Auch dieses Jahr haben wir die zehn erstplatzierten Websites im Anschluss einem Datenschutz-Check und einem weiteren kleinen Wettbewerb unterzogen.

Sven Venzke-Caprarese

1. Verschlüsselte Kommunikation

Im ersten Schritt haben wir bei allen Websites geprüft, ob diese verschlüsselt über https aufgerufen werden können oder teilweise noch unverschlüsselte Datenübertragungen per http unterstützen. Von den zehn geprüften Klinik-Websites konnten sechs Websites ausschließlich per https aufgerufen werden. Versuche, die Websites mittels http aufzurufen, führten zu einer Umleitung auf die entsprechende Website per https. Datenschutzrechtlich machten diese sechs Websites also alles richtig.

Zwei der verbleibenden vier Websites unterstützen zwar https, konnten jedoch auch via http aufgerufen werden. Beide Websites haben wir uns näher angesehen. Auf einer der beiden Websites wäre es möglich gewesen, Terminanfragen unter Angabe von u. a. Name, Krankenkasse, Körpergewicht und gewünschter Untersuchung unverschlüsselt per Kontaktformular zu übermitteln. Auch auf der anderen Website fanden wir ein unverschlüsseltes Kontaktformular, welches u. a. Name, Krankenkasse, Ort von Gelenkbeschwerden, Vordiagnosen zur Notwendigkeit eines künstlichen Gelenks etc. abfragte. Beide Klinik-Websites scheiterten damit bereits in der ersten Runde unseres Datenschutz-Wettbewerbs.

Auch die zwei weiteren Websites, die keinerlei https-Unterstützung boten, nahmen wir etwas detaillierter in den Blick. Hier waren auf einer Website ebenfalls unverschlüsselte Kontaktformulare aufzufinden, etwa allgemeine Kontaktformulare und Formulare zu Lob und Tadel. Auch diese Website schied an dieser Stelle aus unserem Wettbewerb aus. Die verbleibende Website bot zwar kein https an. Allerdings waren auch keine personenbezogenen Kontaktformulare etc. in die Website eingebunden. Ein eigener Karrierebereich war vorhanden - dieser leitete jedoch auf eine neue Seite weiter, die https-verschlüsselt ausgeliefert wurde. Zu einer Schwachstelle führte die fehlende https-Verschlüsselung jedoch: Die Login-Seite des von der Klinik-Website verwendeten Content Management Systems war ebenfalls unverschlüsselt. Im Hinblick auf die Anmeldung von Administratoren oder

Redakteuren kann dies ein Sicherheitsrisiko darstellen. An dieser Stelle behielten wir die Website zwar noch im Wettbewerb, allerdings vermerkten wir einen Abzug in der „B-Note“.

Praxistipp:

Die Einstellung, dass Websites nur mittels https aufgerufen werden können, sollte eigentlich jeder Websitebetreiber vornehmen. Andernfalls droht ein Verstoß gegen § 13 Abs. 7 TMG, gegen § 9 BDSG bzw. Art. 32 DSGVO und schlimmstenfalls gegen § 203 StGB.

2. Trackingtools

Acht der zehn überprüften Websites nutzten Tracking Tools zur Zählung der Websitebesucher. Fünf Seiten verwendeten Google Analytics. Drei Seiten verwendeten Matomo (vormals Piwik).

Wir sahen uns zuerst die fünf Websites an, die Google Analytics einsetzten. Als Prüfungsmaßstab legten wir die Orientierungshilfe der Hamburger Aufsichtsbehörde zum beanstandungsfreien Betrieb an. Es zeichnete sich jedoch insgesamt kein gutes Bild ab:

- Drei der fünf Websites erwähnten Google Analytics überhaupt nicht in der Datenschutzerklärung. Somit fehlten auch jede Opt-Out Möglichkeit. Eine der betroffenen Websites war bereits im Vorfeld ausgeschieden. Die beiden weiteren Websites schieden nun aus.
- Die verbleibenden zwei der fünf Websites, die Google Analytics verwendeten, informierten zwar über den entsprechenden Einsatz in der Datenschutzerklärung. Allerdings fehlte die Möglichkeit, per Opt-Out-Cookie dem Tracking zu widersprechen, was insbesondere für Nutzer von Mobilgeräten wichtig ist. Als weiterer Ausschlussgrund kam auf beiden Seiten hinzu, dass eine Analyse des Quelltextes zeigte, dass die Anonymisierung der IP-Adresse bei Google Analytics nicht aktiviert war. Auch diese beiden Websites schieden nun aus dem Wettbewerb aus.

Im Anschluss prüften wir die drei Websites, die als Trackingtool Matomo nutzten:

- Auf einer Seite war bereits die Auffindbarkeit der Datenschutzerklärung schwierig, da diese einfach im Impressum untergebracht war. Matomo wurde dort zudem nicht erwähnt und somit fehlte auch hier die notwendige Opt-Out-Möglichkeit. Die Website schied somit aus dem Wettbewerb aus.
- Eine Seite erwähnte zwar den Einsatz vom Matomo in der Datenschutzerklärung, verwies jedoch als Opt-Out-Möglichkeit nur darauf, JavaScript und die Speicherung von Cookies zu deaktivieren. Angesichts der guten Opt-Out-Möglichkeiten, die Matomo von Haus aus mit sich bringt, hätte dieser Umstand zum Ausscheiden der Website geführt. Sie war jedoch bereits in der ersten Runde ausgeschieden.
- Die dritte Seite erwähnte den Einsatz von Matomo und verwies auch auf die Möglichkeit, dem Tracking durch Opt-Out-Cookie zu widersprechen. Dies ist an sich auch die richtige Vorgehensweise. Allerdings wurde an der entsprechenden Stelle in der Datenschutzerklärung vergessen, die Funktion zum Setzen des Opt-Out-Cookies auch tatsächlich einzubinden. Somit war kein Opt-Out vorhanden. Die Website schied daher aus.

Im Ergebnis überstanden die zweite Runde lediglich die beiden Websites, die völlig auf den Einsatz von Trackingtools verzichteten. Einer dieser beiden Websites war jedoch in Runde eins bereits wegen fehlender https-Verschlüsselung trotz Übertragung personenbezogener Daten ausgeschieden. Somit verblieb nur noch eine Website im Wettbewerb – hierbei handelte es sich um die Website, die Runde eins gerade noch mit einem Abzug in der „B-Note“ überstanden hatte.

3. Die Datenschutzerklärung

In der letzten Runde sahen wir uns die verbleibende Seite noch etwas genauer

an. Bei Aufruf begrüßte uns ein Cookie-Banner und wir wurden über die Verwendung von Cookies informiert, die der Personalisierung der Seite, der Websiteanalyse und der Einbindung von Funktionen sozialer Medien dienen sollte. Keines der genannten Szenarien konnten wir allerdings auf der Seite nachvollziehen – nicht einmal die Verwendung von Cookies. Wir vermerkten einen weiteren Abzug in der „B-Note“ wegen der fehlerhaften Information. Das gleiche Bild zeigte sich in der Datenschutzerklärung. Diese war zwar sowohl in der Desktop- als auch in der mobilen Version gut auffindbar. Inhaltlich informierte die Datenschutzerklärung aber über die Nutzung von Social Plugins von Facebook, Google+ und Twitter. Eine entsprechende Nutzung von Social Plugins konnten wir auf der Website nicht feststellen. Wir nahmen an dieser Stelle den dritten Abzug in der „B-Note“ vor. Schließlich informierte die Datenschutzerklärung über die vollständige Speicherung der IP-Adresse ohne weitere Angabe der Dauer. Neben Sicherheitszwecken wurde in diesem Rahmen auch die Auswertung der Protokolldaten zur „Optimierung des Angebotes“ angegeben. An dieser Stelle schied die letzte verbleibende Website aus dem Wettbewerb aus.

4. Fazit

Die diesjährige Betrachtung der Websites zeigt einmal mehr, wie schwer es offenbar selbst für überdurchschnittlich professionelle Websitebetreiber ist, die datenschutzrechtlichen Basisvorgaben in der Praxis zu beachten. Bereits bei unserem ersten Websitecheck im Jahr 2016 zeichnete sich kein gutes Bild ab. Der Websitecheck im Jahr 2017 bot hingegen ein wenig Hoffnung, da immerhin zwei Websites den Websitecheck überstanden und als Gewinner gekürt werden konnten. Im Jahr 2018 – kurz vor Einführung der Datenschutzgrundverordnung – bleibt das Treppchen jedoch wieder leer.

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.

Kurznotiz:

Meldung der Kontaktdaten des Datenschutzbeauftragten an die Aufsichtsbehörde – unabhängig davon, ob es sich um eine weltliche, katholische oder evangelische Einrichtung handelt.

Ab dem 24.5 bzw. 25.5. muss jede Einrichtung die neuen Datenschutzbestimmungen beachten.
Die Einrichtung trifft auch die Pflicht, ihren Datenschutzbeauftragten an die für sie zuständige Aufsichtsbehörde zu melden (z. B. gem. Art. 37 Abs. 7 DSGVO). Auf welchem Weg diese Meldung erfolgen muss, ist gesetzlich nicht festgelegt. Um den bürokratischen Aufwand möglichst gering zu halten, gehen die Aufsichtsbehörden teilweise dazu über, auf ihren Webseiten Meldeformulare zu integrierenv. Vereinzelt, beispielsweise bei der LfDI Nordrhein-Westfalen, kann ein solches schon aufgerufen (aber noch nicht genutzt) werden. Teilweise äußern Aufsichtsbehörden auf Rückfragen aber auch, dass keine Webformulare zur Verfügung gestellt werden.

Melden Sie im Zweifel daher bereits jetzt. Sorgen Sie auch dafür, dass die Meldung von Ihrer Einrichtung dokumentiert wird, um diese später im Zweifel beweisen zu können. Hierfür kommt z. B. ein Faxsendebericht, eine Kopie der E-Mail oder ein Einschreiben per Rückschein in Betracht.

© 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 | 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: Seite 1: iStock.com/metamorworks; Seite 2: iStock.com/ByoungJoo; Seite 5: iStock.com/ipopba; Seite 6: iStock.com/Bet_Noire