AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Februar 2018 | Seite 1

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

INHALT

Haftungsrisiken der DS-GVO erkennen und vermeiden

Viele Unternehmen blicken angespannt auf die Zeit nach dem 25. Mai 2018 und fürchten drakonische Strafen für Datenschutzverstöße. Insbesondere die mögliche Höhe von Bußgeldern treibt viele Verantwortliche an, das Thema Datenschutz neu zu gewichten.

Sven Venzke-Caprarese

Dabei wird deutlich, dass sich nicht nur der mögliche Umfang der Bußgelder massiv erhöhen wird, sondern auch die Anzahl der mit Bußgeldern bedrohten Tatbestände und die gesetzlichen Handlungsvorgaben für Aufsichtsbehörden. Darüber hinaus drohen Schadensersatzansprüche und berufsrechtliche Sanktionen bei Datenschutzverstößen.

1. Erweiterter Bußgeldrahmen

Nach Art. 83 Abs. 4 DS-GVO sind bei Datenschutzverstößen künftig Bußgelder in Höhe von bis zu 10 Millionen Euro oder 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres möglich. Dieser Bußgeldrahmen wird durch Art. 83 Abs. 5 DS-GVO sogar noch einmal verdoppelt. Bestimmte Tatbestände können mit Bußgeldern in Höhe von bis zu 20 Millionen Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden. Damit wird deutlich, dass die mögliche Höhe eines Bußgeldes nach der DS-GVO den bisherigen Bußgeldrahmen des BDSG a. F. um ein Vielfaches übersteigt. Denn nach § 43 Abs. 3 BDSG waren bisher „nur“ Geldbußen in Höhe von bis zu 300.000 Euro denkbar, die in bestimmten Fällen zwar noch erhöht werden konnten, jedoch selbst dann nicht den Maximalrahmen der DS-GVO erreicht hätten.

Die mögliche Höhe der Geldbußen ist jedoch nicht der einzige Umstand, der dazu führt, dass sich der Bußgeldrahmen erweitert. Denn auch die Tatbestände, die nach der DS-GVO bußgeldbewehrt sind, unterscheiden sich teilweise erheblich von denen des bisherigen BDSG.

Beispiel 1: Verstoß gegen Informationspflichten

Bereits § 4 Abs. 3 BDSG a. F. regelte besondere Informationspflichten des Verantwortlichen bei erstmaliger Direkterhebung. Diese Informationspflichten werden durch Art. 13 DS-GVO nicht nur fortgeführt, sondern vom inhaltlichen Umfang auf eine ganz neue Stufe gehoben. Gesundheitseinrichtungen werden in Zukunft verpflichtet sein, Formulare, Erhebungsbögen, Behandlungsverträge etc. an die Informationspflichten des Art. 13 DS-GVO anzupassen.

Vergleicht man die möglichen Folgen von Verstößen gegen Informationspflichten bei erstmaliger Direkterhebung nach dem bisherigen BDSG und der DS-GVO so wird man überrascht feststellen: Ein Verstoß gegen die Informationspflichten des § 4 Abs. 3 BDSG a. F. ist bislang weitestgehend sanktionsfrei. Ein Verstoß gegen die Informationspflichten des Art. 13 DS-GVO wird hingegen künftig vom „großen" Bußgeldrahmen des Art. 83 Abs. 5 DS-GVO bedroht.

Dieses Beispiel zeigt deutlich, dass haftungsrechtlich bisher eher risikoarme Bereiche künftig sehr genau betrachtet werden müssen.

Nähere Details zur Umsetzung der Informationspflichten nach Art. 13 DS-GVO sowie ein Beispiel für einen Krankenhausbehandlungsvertrag, der um die entsprechenden Informationen nach Art. 13 DS-GVO ergänzt wurde, finden Sie im Fachbuch „Der NEUE Datenschutz im Gesundheitswesen", Kapitel 8/1 (Formulare, Verträge, Einwilligungserklärungen anpassen) AOK-Verlag GmbH, Remagen, ISBN 978-3-553-43100-2.

Beispiel 2: Technische und organisatorische Maßnahmen

Bereits in der Vergangenheit war es wichtig, angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen. Eine entsprechende Verpflichtung ergab sich aus § 9 BDSG a. F. sowie der dazugehörigen Anlage. Ein Verstoß gegen § 9 BDSG a. F. war in der Praxis jedoch nicht unmittelbar bußgeldbewehrt und § 9 BDSG a. F. wurde nicht in den entsprechenden Bußgeldvorschriften des § 43 BDSG a. F. aufgeführt. Dies ändert die DS-GVO.

So regelt Art. 32 DS-GVO eine ganze Reihe von technischen und organisatorischen Sicherheitsmaßnahmen, die Verantwortliche und Auftragsverarbeiter treffen müssen. Ein Verstoß gegen diese Vorgaben ist nach Art. 83 Abs. 4 lit. a DS-GVO bußgeldbewehrt.

Gesundheitseinrichtungen sollten daher, sofern noch nicht geschehen, künftig noch höheren Wert auf die Sicherheit der Verarbeitung, deren Dokumentation und regelmäßige Überprüfung legen.

Beispiel 3: Melde- und Benachrichtigungspflichten

Die DS-GVO regelt insbesondere die Meldepflichten gegenüber Aufsichtsbehörden im Falle von Datenpannen von Grund auf neu. Art. 33 DS-GVO bestimmt insofern nicht nur sehr knappe Reaktionsfristen, sondern kennt kaum noch Fälle von Datenpannen, in denen keine Meldung zu erfolgen hat. In bestimmten Fällen sind darüber hinaus nach Art. 34 DS-GVO auch die betroffenen Personen zu benachrichtigen. Verstöße gegen diese Vorgaben sind nach Art. 83 Abs. 4 lit. a DS-GVO bußgeldbewehrt.

Gesundheitseinrichtungen benötigen daher Prozesse, die Datenpannen zum einen vermeiden und zum anderen die Einhaltung der Meldefristen gewährleisten, sollte eine Datenpanne dennoch eintreten. Einen Prozess zur Meldung von Datenpannen finden Sie im Fachbuch „Der NEUE Datenschutz im Gesundheitswesen", Kapitel B/7 (Melde- und Benachrichtigungspflichten).

Bußgeld oder nicht – künftig keine Frage mehr?

Der Bußgeldrahmen, der in Art. 83 DS-GVO geregelt wird, bedeutet zwar nicht, dass jeder Verstoß gegen datenschutzrechtliche Vorschriften künftig

massive Strafen nach sich ziehen wird. Denn auch die Aufsichtsbehörden werden nach wie vor einen erheblichen Ermessensspielraum bei der Höhe des Bußgeldes haben und dürfen die Verhältnismäßigkeit und Verfahrensfairness nicht außer Acht lassen. Die Kriterien für die Bemessung eines Bußgeldes im Einzelnen ergeben sich aus Art. 83 Abs. 2 S. 2 DS-GVO.

Andererseits muss an dieser Stelle auch darauf hingewiesen werden, dass derzeit in der Kommentierung und Fachliteratur ein Meinungsstreit darüber entbrannt ist, ob Aufsichtsbehörden künftig hinsichtlich der Frage ob ein Bußgeld verhängt wird, noch einen Ermessensspielraum haben werden oder nicht.

Zum Teil wird angenommen, dass die DS-GVO eine Abkehr vom Opportunitätsprinzip regle und „mit wenigen Ausnahmen eine Pflicht zur Verhängung von Geldbußen“ auferlege (Bergt in Kühling/Buchner, Datenschutz-Grundverordnung 1. Auflage 2017, Art. 83 Rn. 2, 30 ff.)

Im Gegensatz dazu wird vertreten, dass das Opportunitätsprinzip weiterhin gelte und Aufsichtsbehörden nicht der Pflicht erliegen würden, einen Verstoß gegen die DS-GVO mit einer Geldbuße zu ahnden (Frenzel in Paal/Pauly, DS-GVO BDSG 2. Auflage 2018, Art. 83 Rn. 8 ff.). Demnach könnten Aufsichtsbehörden – je nach Einzelfall – auch mit Hinweisen und Verwarnungen (vgl. Art. 58 DS-GVO) als Vorstufe von Geldbußen arbeiten.

2. Schadensersatzansprüche nach DS-GVO

Gemäß Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Sofern von der betroffenen Person ein Verstoß gegen die DS-GVO behauptet wird, müssen der in Anspruch genommene Verantwortliche bzw. der Auftragsverarbeiter nachweisen, dass die Verarbeitungstätigkeiten im Einklang mit der DS-GVO stattgefunden haben. Spätestens hier zeigt sich, wie wichtig die Dokumentation von Maßnahmen, die Umsetzung der Vorgaben zur Rechenschaftspflicht und nicht zuletzt die sorgfältige Führung des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO werden.

3. Schadensersatzansprüche nach BGB in Verbindung mit der DS-GVO

Wie bisher, wird es Betroffenen darüber hinaus möglich bleiben, Schadensersatzansprüche nach BGB geltend zu machen. In Betracht kommen hier insbesondere Unterlassungsansprüche nach §§ 823, 1004 BGB, aber (und das ist neu) auch Schadensersatzansprüche nach § 823 Abs. 2 BGB i. V. m. der DS-GVO.

Fazit

Die DS-GVO wird ab dem 25. Mai 2018 die Höhe der möglichen Bußgelder erheblich erweitern. Darüber hinaus werden auch mehr Tatbestände als bisher von möglichen Bußgeldern erfasst. Die Situation wird noch dadurch verschärft, dass derzeit unklar ist, ob sich Aufsichtsbehörden weiterhin vom Opportunitätsprinzip leiten lassen dürfen und zugunsten von Hinweisen und Verwarnungen im Einzelfall auf Bußgelder verzichten können oder ob das Legalitätsprinzip gilt und eine Pflicht zur Verhängung von Bußgeldern besteht. Die strengen Regelungen zu Schadensersatzansprüchen nach der DS-GVO und die mit der DS-GVO einhergehende Beweislastverschiebung machen die Situation für Gesundheitseinrichtungen nicht einfacher.

Gesundheitseinrichtungen sollten das Thema Datenschutz nicht zuletzt aus diesen Gründen in Zukunft noch organisierter und nachhaltiger als bisher angehen.

Einen Überblick über die wichtigsten Punkte zur Vorbereitung auf und zur Umsetzung der DS-GVO gibt unser Fachbuch „Der NEUE Datenschutz im Gesundheitswesen“. Im Kapitel B (Datenschutzorganisation) erhalten Sie viele Hinweise, wie Sie die Zeit bis zum 25. Mai 2018 für den Aufbau einer Datenschutzorganisation innerhalb Ihrer Gesundheitseinrichtung noch nutzen können. Weitere Informationen zu den möglichen Sanktionen finden Sie im Kapitel A/5 (Sanktionen).

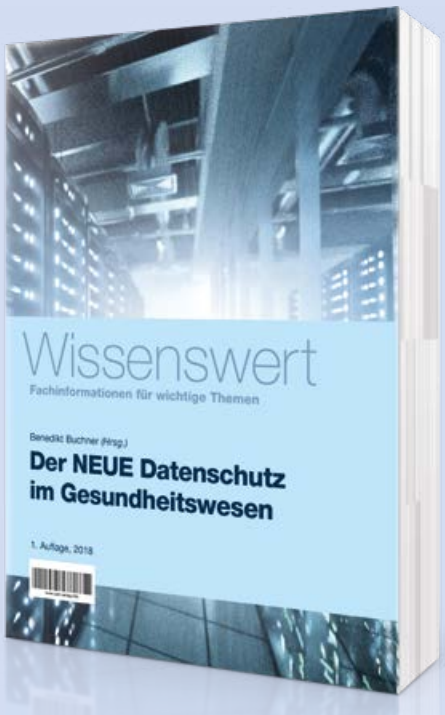
Der NEUE Datenschutz im Gesundheitswesen

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

Entlassungsmanagement

Seit dem 1.10.2017 sind Krankenhäuser verpflichtet, ein Entlassungsmanagement vorzuhalten. Durch dieses ist der reibungslose Übergang der im Krankenhaus behandelten Patienten in die sich anschließenden Versorgungsbereiche zu gewährleisten.

Dr. Sebastian Ertel

Durch die Gesundheitseinrichtung müssen geeignete Maßnahmen getroffen werden, um den jeweiligen Bedarf des Patienten rechtzeitig zu identifizieren und den Entlassungsprozess interessengerecht zu gestalten.

Gesetzliche Regelung

Geregelt ist das Entlassungsmanagement in § 39 Abs. 1a SGB V. Dieser sah vor, dass die Deutsche Krankenhausgesellschaft (DKG), die Kassenärztliche Bundesvereinigung (KBV) und der GKV-Spitzenverband bis zum 31.12.2015 einen Rahmenvertrag über das Entlassungsmanagement abschließen. Diese Frist konnte nicht eingehalten werden. Daraufhin hatte das Bundesschiedsamt am 13.10.2016 über den Rahmenvertrag entschieden und die essentiellen Vertragsinhalte festgesetzt. Gegen den Schiedsspruch klagte die DKG, nahm die Klage, nachdem sich die Parteien auf eine Änderungsvereinbarung einigten, allerdings zurück.

Was wird geregelt?

Letztlich sind alle Punkte zu regeln, die zur bestmöglichen Versorgung des Patienten führen. Hierzu können insbesondere gehören:

- Nach- oder Weiterbehandlung durch Haus- oder Facharzt
- Einbindung von Pflege- oder Rehabilitationsdiensten (z. B. Krankengymnastik)
- Unterbringung in einem Alten- oder Pflegeheim
- Bereitstellung von Medikamenten

Hierzu ist es zwangsnotwendig, dass die Gesundheitseinrichtungen rechtzeitig prüfen, ob und in welcher konkreten Form der zu entlassende Patient nach seiner Behandlung weiterer Unterstützung bedarf. Die frühzeitige Prüfung ist auch erforderlich, damit die notwendigen Anträge gestellt oder Genehmigungen eingeholt werden können.

Wer wird beteiligt?

Je nachdem, wie sich die Anschlussversorgung ausgestaltet, sind verschiedene Personen und Institutionen zu kontaktieren, beispielsweise:

- Angehöriger oder Betreuer
- Weiterbehandelnde Ärzte
- Rehabilitationseinrichtungen (z. B. Physio- oder Ergotherapie)
- Alten- oder Pflegeheim
- Ambulante Pflege

Und der Datenschutz?

Der Rahmenvertrag sieht in § 7 Abs. 1 vor, dass das Krankenhaus vorab schriftlich über Inhalte und Ziele des Entlassungsmanagements informiert. Zudem hat es, sofern erforderlich, die schriftliche Einwilligung des Patienten für die Durchführung des Entlassungsmanagements einzuholen. Zu verwenden sind hierzu Formulare, die dem Rahmenvertrag als Anlage 1a und 1b angehängt sind. Diese regeln u. a. folgende Punkte:

- **Krankenkasse**
  Soll die Krankenkasse beim Entlassungsmanagement unterstützen, sind mit Einwilligung des Patienten die erforderlichen Informationen aus dem Entlassplan zu übersenden (§ 3 Abs. 5 Rahmenvertrag)

- **Entlassbrief an Anschlussarzt**
  Der die Anschlussversorgung durchführende Arzt erhält, bei Einwilligung des Patienten, einen (vorläufigen) Entlassbrief. Sofern weiterbehandelnder und einweisender Arzt personenverschieden sind, erhält der einweisende Arzt, bei Einwilligung des Patienten, ebenfalls den Entlassbrief. Werden pflegerische Leistungserbringer in die weitere Betreuung einbezogen, erhalten diese, bei entsprechender Einwilligung, die für die pflegerische Versorgung erforderlichen Daten. Erfolgt die weitere Betreuung des Patienten in Form einer stationären Heilbehandlung oder Pflege, erhalten den Entlassbrief, bei Einwilligung des Patienten, sowohl die stationäre Einrichtung als auch der Hausarzt bzw. der einweisende oder weiterbehandelnde Vertragsarzt (§ 3 Abs. 7 Rahmenvertrag).

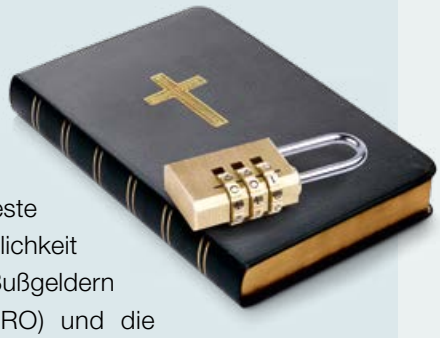
Alles gut?

Anlage 1b - die Einwilligungserklärung - des Rahmenvertrages muss verpflichtend verwendet werden. Dabei hat der Patient lediglich die Wahl zur Einbindung der Krankenkasse und in die Durchführung des Entlassungsmanagements allgemein. Er hat jedoch keine Entscheidungsmöglichkeiten hinsichtlich einzelner Datenweitergaben, obwohl § 3 Abs. 7 Rahmenvertrag eine differenzierte Darstellung der potentiellen Empfänger vornimmt. Nach dem gegenwärtigen Muster kann der Patient nicht entscheiden, dass der einweisende Arzt, der bei der nachgelagerten Behandlung nicht mehr beteiligt ist, keinen Entlassbrief erhält.

Es bleibt daher abzuwarten, ob hier noch eine Anpassung der Formulare erfolgt.

Kurznotiz:

Neuer Datenschutz in der Kirche



Die Europäische Datenschutzgrundverordnung (DS-GVO) regelt in Art. 91, dass Religionsgemeinschaften den Datenschutz in ihrem Bereich weiterhin regeln dürfen, wenn zum 25.5.2018 (Beginn der Anwendbarkeit der DS-GVO) adäquate kirchliche Regelungen bestehen. Sowohl die Katholische Kirche als auch die Evangelische Kirche haben Ende 2017 entsprechende Gesetze geschaffen. Die Katholische Kirche hat mit dem Kirchlichen Datenschutzgesetz (KDG) ein neues Gesetz erlassen. Die Evangelische Kirche hat ihr Datenschutzgesetz (DSG) komplett überarbeitet. In vielen Bereichen erfolgten starke Anpassungen an die Regelungen der DS-GVO. Verschiedene Aspekte wurden kirchenspezifisch geregelt.

Die wohl relevanteste Neuerung ist die Möglichkeit der Verhängung von Bußgeldern (bis zu 500.000 EURO) und die Schaffung eines Rechtsweges zu kirchlichen Datenschutzgerichten, um die Bußgeldbescheide gerichtlich überprüfen zu lassen. Das KDG und das DSG werden zum 24.5.2018 (also einen Tag vor dem Anwendungsbeginn der DS-GVO) in Kraft treten, damit den Anforderungen des Art. 91 DS-GVO entsprochen wird.

Im nächsten Newsletter werden die Besonderheiten der kirchlichen Datenschutzgesetze dargestellt.

© 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

Bildnachweise: iStock.com