AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe August 2017 | Seite 1

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

INHALT

SEITE 1
Änderung des BSI-Gesetzes

SEITE 5
Öffnung des § 203 StGB für die Einbindung externer Dienstleister

SEITE 7
Neues Muster für den Vertrag zur Auftragsverarbeitung nach der DS-GVO

Änderung des BSI-Gesetzes und der BSI-Kritisverordnung – Schwellenwerte für Gesundheitseinrichtungen stehen fest

Das BSI-Gesetz wurde vor etwa zwei Jahren durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) geändert. Diese Änderungen führten dazu, dass Betreibern Kritischer Infrastrukturen weitreichende Pflichten auferlegt wurden.

Sven Venzke-Caprarese

Lange Zeit war für den Gesundheitssektor unklar, wann eine Gesundheitseinrichtung zu den Betreibern Kritischer Infrastrukturen zählt. Dies ändert nun die Erste Verordnung zur Änderung der BSI-Kritisverordnung, welche zum 30.06.2017 in Kraft getreten ist. Parallel wurde auch das BSI-Gesetz weiter angepasst, um die EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) umzusetzen.

Der zweite Korb der BSI-Kritisverordnung ist wirksam

Betreiber von Gesundheitseinrichtungen konnten in der Vergangenheit angesichts des BSI-Gesetzes relativ entspannt bleiben. Zwar regelte dieses bestimmte Pflichten für die Betreiber Kritischer Infrastrukturen in den Sektoren:

- Energie,
- Wasser,
- Ernährung,
- Informationstechnik und Telekommunikation,
- Gesundheit,
- Finanz- und Versicherungswesen

sowie

- Transport und Verkehr.

Allerdings fehlten bislang Regelungen, wann Unternehmen der drei letztgenannten Sektoren als Betreiber Kritischer Infrastrukturen anzusehen sind. Dies liegt daran, dass von vornherein geplant war, die entsprechenden Bestimmungen in zwei zeitversetzten Körben durch die BSI-Kritisverordnung zu regeln. Im ersten Korb wurden mit Wirkung zum 03.05.2016 die Schwellenwerte für die Sektoren

- Energie,
- Wasser,
- Ernährung sowie
- Informationstechnik und Telekommunikation

geregelt.

Mit Wirkung zum 30.06.2017 regelt nun der zweite Korb (Erste Verordnung zur Änderung der BSI Kritisverordnung) die Schwellenwerte für die Sektoren

- Gesundheit,
- Finanz- und Versicherungswesen sowie
- Transport und Verkehr.

Schwellenwerte für Gesundheitseinrichtungen

Die aktuellen Schwellenwerte, die bestimmen, wann eine Gesundheitseinrichtung als Betreiber Kritischer Infrastrukturen zu sehen ist und somit die erweiterten Pflichten nach dem BSI-Gesetz einzuhalten hat, finden sich in Anhang 5 Teil 3 der BSI-Kritisverordnung:

- Krankenhäuser gelten demnach ab 30.000 vollstationären Krankenhausfällen pro Jahr als Kritische Infrastruktur;
- Apotheken gelten ab 4,65 Millionen abgegebenen Packungen pro Jahr als Betreiber einer Kritischen Infrastruktur;
- Für Labore gilt ein Schwellenwert von 1,5 Millionen Aufträgen pro Jahr.

Anhang 5 Teil 3 der BSI-Kritisverordnung enthält darüber hinaus weitere Schwellenwerte, u. a. für Produktionsstätten und Abgabestellen verschreibungspflichtiger Arzneimittel sowie von Blut- und Plasmakonzentraten.

Was der zweite Korb für Gesundheitseinrichtungen bedeutet

Gesundheitseinrichtungen sollten unverzüglich überprüfen, ob sie als Betreiber Kritischer Infrastrukturen anzusehen sind. Denn mit dem nun in Kraft getretenen zweiten Korb beginnen die Umsetzungsfristen (auch) im Bereich Gesundheit zu laufen.

Umsetzungsfrist: Sechs Monate

Gesundheitseinrichtungen haben nach § 8b BSI-Gesetz vom 30.06.2017 an sechs Monate Zeit, um folgende Pflichten zu erfüllen:

- Einrichtung einer Kontaktstelle, über welche die Gesundheitseinrichtung als Betreiber einer Kritischen Infrastruktur jederzeit erreichbar ist und Meldung dieser Kontaktstelle an das BSI;
- Meldungen von bestimmten Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit an das BSI.

Neben der Einrichtung einer entsprechenden Kontaktstelle müssen Gesundheitseinrichtungen nun Prozesse implementieren, welche die unverzügliche Meldung der von § 8a Abs. 4 BSI-Gesetz benannten Störungen sicherstellt. Dies wird in der Praxis dazu führen, dass Verantwortlichkeiten und Meldeketten definiert werden müssen sowie Sensibilisierungs- und Schulungsmaßnahmen der beteiligten Personen (insbesondere auch der IT-Abteilung) durchgeführt werden sollten.

Umsetzungsfrist: Zwei Jahre

Gesundheitseinrichtungen haben nach § 8a BSI-Gesetz vom 30.06.2017 an zwei Jahre Zeit, um folgende Pflichten zu erfüllen:

- Es müssen angemessene technische und organisatorische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse getroffen werden, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind;
- Es muss mindestens alle zwei Jahre nachgewiesen werden, dass diese Anforderungen eingehalten werden. Dies kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen gegenüber dem BSI nachgewiesen werden. Die Gesetzesbegründung stellt insoweit klar, dass dabei auch auf bestehende Zertifizierungsstrukturen nach internationalen, europäischen oder nationalen Standards zurückgegriffen werden kann.

An dieser Stelle stellt sich nur für Gesundheitseinrichtungen die Frage, welche Vorkehrungen zu treffen sind.

Hinweise für die Praxis lassen sich aus einer Orientierungshilfe des BSI zu Nachweisen gemäß § 8a Abs. 3 BSI-Gesetz ableiten. Diese stellt klar, dass sich Betreiber kritischer Infrastrukturen zum Nachweis der Einhaltung der Anforderungen überprüfen lassen müssen und dem BSI entsprechende Nachweise vorzulegen haben.

Für die Prüfung setzt die Orientierungshilfe regelmäßig folgende Dokumente voraus: *„Konzept und Dokumentation des Risikomanagements inkl. Risikoanalyse; Beschreibung des Informationssicherheitsmanagementsystems (ISMS); Notfallkonzept und Beschreibung des Continuity Managements; Dokumente des Asset Managements; Dokumentation der Prozesse zur baulichen und physischen Sicherheit […]; Dokumentation der personellen und organisatorischen Sicherheit […]; Konzepte und Dokumentation zur Vorfallserkennung und -bearbeitung […]; Konzepte und Dokumentation von Überprüfungen […]; Richtlinien zur externen Informationsversorgung; Richtlinien zum Umgang mit Lieferanten und Dienstleistern […]; Sicherheitskonzept (inkl. Darstellung umgesetzter und geplanter Maßnahmen), insbesondere der branchenspezifischen Maßnahmen“.*

Auch die Orientierungshilfe des BSI zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Abs. 2 BSI-Gesetz stellt klar, dass die Einführung eines Informationssicherheitsmanagementsystems erforderlich ist. Dies kann nach der Orientierungshilfe *„beispielsweise durch die Einführung und den Betrieb eines ISMS auf Grundlage des BSI-IT-Grundschutz oder ISO/IEC 27001 erfolgen“* (vgl. Ziffer 5.1 der Orientierungshilfe). Darüber hinaus erwähnt auch die Orientierungshilfe die Einführung eines Continuity Managements *(„Aufrechterhaltung und Sicherung der Mindestqualität der kritischen Dienstleistung“)* sowie eines Asset Managements *(„Identifikation, Klassifizierung und Inventarisierung der für die kritische Dienstleistung maßgeblichen informationstechnischen Prozesse, Systeme und Komponenten“)*. Im Anhang der Orientierungshilfe werden zudem die relevantesten Bedrohungskategorien, Schwachstellenkategorien und Maßnahmen der technischen Informationssicherheit aufgelistet.

Die Anforderungen, die Betreiber kritischer Infrastrukturen einzuhalten haben, sind demnach als hoch einzustufen. Eine Gesundheitseinrichtung, die feststellt, dass sie als Betreiber. einer Kritischen Infrastruktur anzusehen ist und die bislang weder ein Informationssicherheitsmanagement eingeführt hat noch über einen Großteil der genannten Dokumente verfügt, sollte unverzüglich damit beginnen, die verbleibenden zwei Jahre zu nutzen, um sich entsprechend aufzustellen.

Weitere Änderungen des BSI-Gesetzes

Neben der BSI-Kritisverordnung wurde mit Wirkung zum 30.06.2017 auch das BSI-Gesetz weiter angepasst.

Für Gesundheitseinrichtungen als Betreiber Kritischer Infrastrukturen sind insbesondere folgende Änderungen relevant:

- § 8a Abs. 4 BSI-Gesetz regelt nunmehr ein Überprüfungs- und Betretungsrecht des BSI hinsichtlich der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten.
- Zudem müssen auf Anforderung die relevanten Dokumente gegenüber dem BSI offengelegt werden.

Fazit

Seit dem 30.06.2017 stehen die Schwellenwerte fest, mit deren Hilfe Gesundheitseinrichtungen bestimmen können, ob sie die erweiterten Pflichten nach dem BSI-Gesetz einhalten müssen. Zeitgleich beginnen die Umsetzungsfristen zu laufen, weshalb die betroffenen Gesundheitseinrichtungen unverzüglich die künftige Umsetzung der entsprechenden Maßnahmen planen sollten.

Hinweise im Buch

Vertiefungshinweise im Handbuch DSiGW:
Datenschutz im Gesundheitswesen (AOK Verlag GmbH), Kapitel D/7 (Das neue IT-Sicherheitsgesetz))

Öffnung des § 203 StGB für die Einbindung externer Dienstleister

Gegenwärtige Rechtslage

Überlegungen, Datenverarbeitungen bei Stellen außerhalb der Gesundheitseinrichtung auszulagern, scheiterten bislang häufig an der Geheimhaltungspflicht der Berufsgeheimnisträger und dem Straftatbestand des § 203 StGB.

Nur vereinzelt bestehen Regelungen, die eine Auslagerung der Datenverarbeitung in bestimmten Konstellationen erlauben und überwiegend als Offenbarungsbefugnis im Sinne des § 203 StGB verstanden werden. Wie unterschiedlich die landesspezifischen Regelungen sein können, soll anhand der entsprechenden Vorgaben aus dem Bayerischen Krankenhausgesetz (BayKrG) und dem Gesundheitsdatenschutzgesetz Nordrhein-Westfalen verdeutlicht werden.

Art. 27 Abs. 4 Satz 5 und 6 BayKrG

Das Krankenhaus kann sich zur Verarbeitung und Mikroverfilmung von Patientendaten anderer Personen oder Stellen bedienen, wenn es sicherstellt, dass beim Auftragnehmer die besonderen Schutzmaßnahmen nach Abs. 6 eingehalten werden, und solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden. Zur Verarbeitung oder Mikroverfilmung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, darf sich das Krankenhaus jedoch nur anderer Krankenhäuser bedienen.

§ 7 GDSG NRW

(1) Patientendaten sind grundsätzlich in der Einrichtung oder öffentlichen Stelle zu verarbeiten; eine Verarbeitung im Auftrag ist nur nach Maßgabe der Absätze 2 bis 4 zulässig.

(2) Die Verarbeitung von Patientendaten im Auftrag ist nur zulässig, wenn sonst Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger vorgenommen werden können.

In verschiedenen Bundesländern, beispielsweise Schleswig-Holstein oder Niedersachsen, bestehen keine gesetzlichen Regelungen zur Verarbeitung von Patientendaten im Allgemeinen bzw. deren Verarbeitung durch externe Dienstleister.

Neben der Problematik der uneinheitlichen Regelungen können insoweit auch Standortnachteile entstehen, wenn eine Einrichtung die Datenverarbeitung kostengünstig auslagern kann, während eine vergleichbare Einrichtung in einem anderen Bundesland diese kostenintensiv selbst vornehmen muss.

Nach der gegenwärtigen Konzeption des § 203 StGB dürfen Dritte nur dann Zugriff auf die geschützten Daten und Informationen nehmen, wenn diese Dritten als berufsmäßig tätige Gehilfen handeln oder bei dem Berufsgeheimnisträger zur Vorbereitung auf den Beruf tätig sind. Erforderlich ist demnach ein Über-Unterordnungsverhältnis zwischen Berufsgeheimnisträger und Dritten und daraus herleitend ein entsprechendes Weisungsrecht.

Ein solches besteht grundsätzlich nur innerhalb einer arbeitsvertraglichen Beziehung, nicht aber bei einer Einbindung eines unabhängigen externen Dienstleisters. Die verbleibende Möglichkeit der Entbindung von der Schweigepflicht ist in vielen Konstellationen nicht praktikabel:

- Wie soll mit dem Widerruf der Entbindungserklärung bei komplexen EDV-gestützten Datenverarbeitungen umgegangen werden?
- Wie soll eine Entbindungserklärung eingeholt werden, wenn die Datenverarbeitung ausgelagert werden soll und der betroffene Patient nicht mehr erreichbar oder gegebenenfalls bereits verstorben ist.

Privilegierte Tätigkeiten

Diese Aspekte flossen in einen Gesetzentwurf der Bundesregierung zur Änderung des § 203 StGB ein. Durch diesen sollen unterstützende Verarbeitungen von Informationen und Daten, die unter dem Schutz der Verschwiegenheit des Berufsgeheimnisträgers stehen, unter bestimmten Voraussetzungen auf externe Stellen, § 203 StGB spricht von den mitwirkenden Personen, ausgelagert werden können. Hierzu zählen nach dem Gesetzesentwurf insbesondere

- Schreibarbeiten,
- Rechnungswesen,
- Annahme von Telefonanrufen,
- Aktenarchivierung und -vernichtung,
- Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art, beispielsweise auch von entsprechend ausgestatteten medizinischen Geräten,
- Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten und die
- Mitwirkung an der Erfüllung von Buchführungs- und steuerrechtlichen Pflichten des Berufsgeheimnisträgers.

Einbeziehung Externer

Als Basis für die Beauftragung einer mitwirkenden Person mit einer der vorgenannten oder einer vergleichbaren Tätigkeit soll nach dem Gesetzesentwurf

- diese in die berufliche Tätigkeit der schweigepflichtigen Person einbezogen sein und
- die Einbeziehung im Einvernehmen mit der schweigepflichtigen Person, gerade auch in mehrstufigen Auftragsverhältnissen, geschehen.

Zulässig wäre unter diesen Voraussetzungen auch eine Beauftragung von Subunternehmern, sofern dies im Einvernehmen mit dem Berufsgeheimnisträger erfolgt und eine lückenlose Vertragskette zwischen dem Berufsgeheimnisträger und der letztlich tätig werdenden Person besteht. Dabei muss zwischen dem Berufsgeheimnisträger und der letztlich tätigen Person keine unmittelbare vertragliche Beziehung bestehen. Maßgeblich ist einzig die bereits erwähnte Vertragskette.

Kann eine mitwirkende Person mit der unterstützenden Verarbeitung betraut werden, dürfen nur die Daten offenbart werden, die für die Verarbeitung erforderlich sind. Offenbart die mitwirkende Person die anvertrauten Informationen unbefugt einem Dritten, macht sich diese nach der Neukonzeption des § 203 Abs. 4 StGB ihrerseits strafbar.

Dem Berufsgeheimnisträger obliegt diesbezüglich die Verpflichtung, die mitwirkenden Personen angemessen zur Vertraulichkeit zu verpflichten. Unterlässt er dies, kann hieraus ebenfalls eine Strafbarkeit begründet werden.

Stand des Verfahrens

Der Gesetzesentwurf befindet sich derzeit in den Ausschüssen, da einige Detailfragen noch zu erörtern sind. Hierzu zählt beispielsweise die Frage, ob sich die mitwirkende Person ebenso wie der Berufsgehilfe auf ein strafprozessuales Zeugnisverweigerungsrecht berufen kann. Das Gesetzgebungsverfahren sollte bis zur Bundestagswahl im September abgeschlossen werden. Wegen der sachlichen Diskontinuität würden sämtliche Ausarbeitungen mit Ende der Legislaturperiode verfallen und müssten neu auf den Weg gebracht werden.

Kurznotiz:

Neues Muster für den Vertrag zur Auftragsverarbeitung nach der DS-GVO

Im Rahmen der Zusammenarbeit mehrerer Verbände, unter anderem dem Berufsverband der Datenschutzbeauftragten Deutschlands e. V., dem Bundesverband Gesundheits-IT e. V und der Deutsche Krankenhausgesellschaft e. V. wurde ein neuer Mustervertrag für die Auftragsverarbeitung im Gesundheitswesen erstellt. Dieser ist an die Neuerungen der DS-GVO angepasst. Das Papier zeichnet sich dadurch aus, dass die Thematik der Auftragsverarbeitung detailliert erklärt wird und die einzelnen Paragrafen des Mustervertrages kommentiert und mit umfangreichen Literaturhinweisen untermauert sind. Neben dem Muster für Neuverträge wurde ein Arbeitspapier für den Umgang mit Altverträgen erarbeitet. Die Dokumente können im WORD- und PDF-Format beispielsweise unter https://www.bvdnet.de/arbeitskreis-medizin/ abgerufen werden.

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.

© 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: www.istock.com