Handwerkliche Fehler im § 75b SGB V als Grundlage der KBV-Richtlinie über die Anforderungen zur Gewährleistung der IT-Sicherheit – Auswirkungen für medizinische Labore

Andreas Becker, Edgar Gärtner

Handwerkliche Fehler des Gesetzgebers bei der Abfassung des § 75 b SGB V führen aktuell zu einem rechtsunsicheren Zustand vor allem für freie medizinische Labore.

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) definiert die Informationssicherheitsanforderungen u. a. an Krankenhäuser und medizinische Labore, die bestimmte Kriterien erfüllen, die in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) festgelegt sind.

Krankenhäuser und medizinische Labore, die die Kriterien der BSI-KritisV erfüllen, werden als *Betreiber Kritischer Infrastrukturen* (KRITIS-Betreiber) bezeichnet und sind nach § 8a Abs. 1 S. 1 BSIG *„verpflichtet, […] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."*

Darüber hinaus müssen die KRITIS-Betreiber *„mindestens alle zwei Jahre die Erfüllung der Anforderungen nach* [§ 8a] *Absatz 1* [BSIG] *auf geeignete Weise"* nachweisen (§ 8a Abs. 3 S. 1 BSIG).

Erwähnenswert ist auch, dass das BSIG in § 14 Bußgelder von bis zu 100.000 Euro für bestimmtes ordnungswidriges Verhalten vorsieht.

2 Die Ausgangslage für Krankenhäuser

Zum Verständnis der im Titel dieses Aufsatzes aufgeführten Problemstellung wird zunächst auf Krankenhäuser eingegangen[1].

1. KRITIS-Krankenhäuser

Unterliegt ein Krankenhaus als KRITIS-Betreiber den Pflichten aus § 8a Abs. 1 und 3 BSIG, so unterliegen alle Organisationseinheiten des Krankenhauses – sofern sie unmittelbar oder mittelbar für die stationäre Patientenversorgung relevant sind – diesen Pflichten. Im Rahmen der Erfüllung des § 8 a Abs. 1 und 3 BSIG wird der KRITIS-Betreiber – und nachfolgend auch die prüfende Stelle nach § 8a Abs. 3 Satz 2 BSIG – alle relevanten Organisationseinheiten angemessen berücksichtigen.

2. Nicht-KRITS-Krankenhäuser

Für alle Krankenhäuser, die nicht gemäß BSI-KritisV als KRITIS-Betreiber gelten, gilt ab 01.01.2022 das Regularium des (neu geschaffenen) § 75 c SGB V. Nicht der KritisV unterfallen – grob zusammengefasst – solche Krankenhäuser, die den derzeitigen Schwellenwert von 30.000 vollstationären Fällen pro Jahr nicht erreichen.

Auch der neue § 75c SGB V sieht Verpflichtungen zur IT-Sicherheit vor, die im Prinzip denen des § 8a Abs. 1 S. 1 BSIG entsprechen.

Interessanterweise gilt dieser Paragraf nicht für solche Krankenhäuser, die als KRITIS-Betreiber die Anforderungen aus dem BSIG zu erfüllen haben, denn: *„Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben."* (§ 75c Abs. 3 SGB V)

[1] Dazu ausführlich: Becker A. Anforderungen an die Informationssicherheit in deutschen Krankenhäusern (Teil I). Journal für Medizin- und Gesundheitsrecht. 1/2021: 39-48. Teil 2 zur Veröffentlichung angenommen in Heft 2/2021.

Der Gesetzgeber hat also gezeigt, dass die Vermeidung von redundanten und somit unverhältnismäßigen Anforderungen – zumindest für Krankenhäuser – gelingen kann.

Begründet wurde dies wie folgt: *„[…] dient der Klarstellung, dass keine doppelte Regulierung der IT-Sicherheit erfolgt. Die Anforderungen an die IT-Sicherheit der Krankenhäuser ist von den Anforderungen an die IT-Sicherheit der (Zahn-)Arztpraxen entkoppelt, auch wenn in den Krankenhäusern ambulante bzw. vertrags(zahn)ärztliche Versorgung stattfindet. Die Informationsinfrastrukturen in den Krankenhäusern sollen nicht wahlweise zwei verschiedenen und nicht zwingend deckungsgleichen IT-Sicherheitsregimen – dem des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und dem des § 75b – unterworfen werden."* (BT-Dr. 19/20708 vom 1.7.2020, 167)

An dieser Stelle kann man deshalb von einem Vorrang der IT-Sicherheitsanforderungen des BSIG gegenüber denen des § 75c SGB V sprechen.

3 Die Ausgangslage für medizinische Labore

Vor der Einführung des § 75b SGB V konnten auch medizinische Labore (nachfolgend nur: Labore) hinsichtlich der IT-Sicherheit in zwei Gruppen unterteilt werden.

1. KRITIS-Labore

Labore, die in eigenständiger Rechtsform tätig sind (nachfolgend zur Abgrenzung *freie Labore* genannt) und beispielsweise jährlich mindestens 1.500.000 Aufträge in der Analytik bearbeiten, fallen unter die Anforderungen des § 8a Abs. 1 BSIG und müssen – wie die KRITIS-Krankenhäuser – *„mindestens alle zwei Jahre die Erfüllung der Anforderungen nach* [§ 8a] *Absatz 1* [BSIG] *auf geeignete Weise"* nachweisen (§ 8a Abs. 3 S. 1 BSIG).

2. Labore als Organisationseinheit eines KRITIS-Krankenhauses

Wie bereits oben erläutert, resultieren für ein Labor als Organisationseinheit eines Krankenhauses, welches als KRITIS-Betreiber den Pflichten aus § 8a Abs. 1 und 3 BSIG unterliegt, keine gesonderten Verpflichtungen. Sie sind im Rahmen der (ggf. noch erforderlichen) Einführung oder Erweiterung

der IT-Sicherheitsmaßnahmen nach § 8a Abs. 1 BSIG angemessen zu berücksichtigen, so wie auch klinische Fachabteilungen, die Radiologie oder die Apotheke etc. Im Rahmen der Prüfung nach § 8a Abs. 3 S. 1 BSIG wird das Labor dann auch mitgeprüft.

Die Rechtslage ist also klar: soweit es um die Anwendbarkeit des Regulariums für die IT-Sicherheit geht, gilt das Regularium des KRITIS-Krankenhauses; eine eigene oder gesonderte Verpflichtung hat das in die Organisation des KRITIS-Krankenhauses eingebundene Labor nicht.

Bisher gab es für freie Labore, die nicht als Betreiber Kritischer Infrastrukturen galten, keine definierten Anforderungen an die IT-Sicherheit.

Das sollte sich mit dem § 75b SGB V und der Richtlinie der Kassenärztliche Bundesvereinigung (KBV) jedoch ändern.

4 Die Richtline der Kassenärztlichen Bundesvereinigung

Die Vertreterversammlung der Kassenärztliche Bundesvereinigung hat mit Beschluss vom 16. Dezember 2020 die *„Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“* in der vertragsärztlichen Versorgung beschlossen.

Die Richtlinie der KBV legt folglich die in einer vertragsärztlichen bzw. vertragspsychotherapeutischen Praxis erforderlichen Anforderungen an die IT-Sicherheit fest, die Anforderungen richten sich nach der Größe der Praxis und sind in fünf Anlagen zur Richtlinie definiert. Die Anforderungen der Richtlinie gelten ab den in den Anlagen angegebenen Zeitpunkten, beginnend mit dem 1.4.2021.

Der Anwendungsbereich der Richtlinie wird in § 75 b Abs. 4 SGB V geregelt: *„Die Richtlinie ist für die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich.“*

Bis hier kann festgestellt werden: die KBV-Richtlinie gilt zweifelsfrei verbindlich für freie Labore, die an der vertragsärztlichen Versorgung teilnehmen und gemäß BSI-KritisV nicht als KRITIS-Labore gelten.

Der geneigte Leser erwartet höchstwahrscheinlich nun, dass die Richtlinie im Gegenzug nicht für solche Labore gilt, die zwar auch an der vertragsärztlichen Versorgung teilnehmen, aber als KRITIS-Labore den Anforderungen des BSIG unterliegen.

Problematisch wird die Situation aber dadurch, dass eine entsprechende Ausnahmeregelung – analog zu der für Krankenhäuser in § 75c Abs. 3 SGB V – in § 75b SGB V nicht eingebracht wurde.

§ 75 b SGB V enthält also eine – auf Nachlässigkeit des Gesetzgebers zurückgehende – Unklarheit für solche freien Labore, die die Voraussetzungen der BSI-KritisV erfüllen.

5 § 75b SGB V – Gut gedacht ist nicht gleich gut gemacht

Der Auftrag der KBV zur Erstellung der IT-Sicherheits-Richtlinie basiert auf § 75b Abs. 1 SGB V, in den Abs. 2 und 4 werden Regelungsinhalte näher spezifiziert.

Während die Richtlinie gemäß § 75b Abs. 4 S. 1 SGB V *„für die an der vertragsärztlichen […] Versorgung teilnehmenden Leistungserbringer verbindlich.* ist, ist sie *nicht anzuwenden für die vertragsärztliche […] Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen getroffen werden. Angemessene Vorkehrungen im Sinne von Satz 2 gelten als getroffen, wenn die organisatorischen und technischen Vorkehrungen nach § 8a Absatz 1 des BSI-Gesetzes oder entsprechende branchenspezifische Sicherheitsstandards umgesetzt wurden.“* (§ 75b Abs. 4 S. 2 und 3 SGB V).

Daraus folgt, dass die vertragsärztliche Versorgung durch ein Labor, welches als Organisationseinheit eines Krankenhaus-KRITIS-Betreibers, der seine Verpflichtungen nach § 8a Abs. 1 S. 1 und Abs. 3 S. 1 BSIG erfüllt, anzusehen ist, nicht zum Geltungsbereich der KBV-IT-Sicherheits-Richtlinie zählt.

Diese Ausnahmeregelung ist auch sinnvoll, da die KRITIS-Anforderungen an die entsprechenden Krankenhäuser grundlegend durch § 8a Abs. 1 BSIG bzw. ausführlich durch den branchenspezifischen Sicherheitsstandard (B3S) der Deutschen Krankenhausgesellschaft (DKG) formuliert wurden.

Als freies Labor wird aber die vertragsärztliche Versorgung nicht im Krankenhaus erbracht, weshalb der Anwendungsausschluss nach § 75 b Abs. 4 Satz 2 SGB V nicht vorliegt. Dem Wortlaut nach hat ein freies KRITIS-Labor deshalb zusätzlich die Voraussetzungen der Richtlinie der KBV zur IT-Sicherheit nach § 75 b SGB V zu erfüllen.

Diese Unklarheit im Gesetz – nämlich die doppelte Anwendung rechtlicher Vorgaben für die IT-Sicherheit einmal nach dem BSIG und einmal nach der Richtlinie der KBV – war in den Überlegungen des Gesetzgebers bereits angelegt. Es heißt dort nämlich:

„Bei den Arzt- und Zahnarztpraxen handelt es sich in der Regel um kleinere und mittlere Unternehmen, die nicht in den Anwendungsbereich der Regelungen des BSI-Gesetzes zu kritischen Infrastrukturen fallen und damit auch nicht Gegenstand der BSI-Kritisverordnung sind. Gleichwohl besteht ein großes Bedrohungspotenzial auch für die dort eingesetzten informationstechnischen Systeme." (BT-Dr. 19/13438 vom 23.9.2019, 48).

Offensichtlich konnte man sich – entgegen der geltenden Rechts- und vorliegenden Erfahrungslage – nicht vorstellen, dass es freie medizinische Labore geben könnte, die unter das BSIG und die BSI-KritisV fallen.

Dabei ist noch vor Inkrafttreten des Gesetzes dieser Irrtum des Gesetzgebers bekannt geworden. Die Bundesregierung antwortete bereits zwei Monate nach der obigen Gesetzesbegründung auf eine Kleine Anfrage von Bundestagsabgeordneten u.a.:

„Mit dem neuen § 75b SGB V erhalten die Kassenärztliche Bundesvereinigung und die Kassenzahnärztliche Bundesvereinigung die Aufgabe, die IT-Sicherheitsanforderungen in der vertragsärztlichen und vertragszahnärztlichen Versorgung in einer Richtlinie bis zum 30. Juni 2020 festzulegen. Diese

Maßnahmen dienen zur Erhöhung der IT-Sicherheit für Leistungserbringer, die nicht von der BSI-Kritisverordnung erfasst werden." (BT-Dr. 19/15031 vom 12.11.2019, 2)

Warum dennoch § 75 b SGB V im Bundesgesetzblatt vom 18.12.2019 (BGBl I S. 2562) ohne eine entsprechend formulierte Ausnahme, die auch die Labor-KRITIS-Betreiber von den Verpflichtungen befreit, ausgegeben wurde, kann nur mit handwerklichen Fehlern des Gesetzgebers begründet werden. Auch die im Bundesgesetzblatt vom 19.10.2020 ausgegebene Änderung des § 75 b SGB V korrigierte diesen Fehler nicht (BGBl I S. 2115).

6 Vorschlag zur Problemlösung

Grundsätzlich sollen die vorangehenden Ausführungen nicht als Plädoyer gegen den Grundgedanken des § 75b SGB V und der KBV-IT-Sicherheits-Richtlinie aufgefasst werden. An der Notwendigkeit zur angemessenen Absicherung der informationstechnischen Strukturen und Prozesse, die insbesondere die Aufrechterhaltung der Verfügbarkeit der vertragsärztlichen Versorgung zum Ziel hat, bestehen bei den Verfassern aus fachlicher Sicht keine Zweifel.

Die praktische Erfahrung zeigt aber, dass sich Labor-KRITIS-Betreiber bereits die Frage stellen, ob sie die Anforderungen der KBV-IT-Sicherheitsrichtlinie zusätzlich zu denen aus dem BSIG erfüllen müssen oder nicht.

Die KBV wäre gut beraten, den handwerklichen Fehler des § 75 b SGB V zu erkennen und die parallele Anwendbarkeit ihrer § 75 b SGB V-Richtlinie für diese Labore zu verneinen.

Die IT-Sicherheitsvorkehrungen aus dem BSIG sind nach Auffassung der Verfasser prioritär. Dies ergibt sich u.a. aus den folgenden Überlegungen:

1. Der Gesetzgeber möchte keine doppelte Regulierung der IT-Sicherheit; dieser gesetzgeberische Wille wurde im Kontext der Informationsinfrastrukturen von vertragsärztlichen Leistungserbringern innerhalb von Krankenhäusern zum Ausdruck gebracht. *„Die Informationsinfrastrukturen in den Krankenhäusern sollen nicht wahlweise zwei verschiedenen und nicht zwingend deckungsgleichen IT-Sicherheitsregimen – denen des Gesetzes über das Bundesamt für Sicherheit in der Infor-*

mationstechnik und denen des § 75 b – unterworfen werden." (BT-Dr. 19/20708 vom 1.7.2020, S. 167).

2. Der Wille des Gesetzgebers kommt auch in der vorgenannten Antwort der Bundesregierung klar zum Ausdruck, wonach die Richtlinie der KBV *„zur Erhöhung der IT-Sicherheit für Leistungserbringer, die nicht von der BSI-Kritis-Verordnung erfasst werden"*, dient. (BT-Dr. 19/15031 vom 12.11.2019, S. 2).

3. Der Gesetzgeber hat offenkundig übersehen, dass es freie Labore in einer Größe geben kann, die der BSI-Kritis-Verordnung unterfallen (BT-Dr. 19/13438 vom 23.09.2019, S. 48). Wäre der Gesetzgeber diesem Irrtum nicht unterlegen, spricht der anderer Stelle geäußerte gesetzgeberische Wille für einen Vorrang des BSIG und der BSI-KritisV.

4. Der Vorrang des BSIG und der BSI-KritisV kommt in § 75 c Abs. 3 SGB V und § 75 b Abs. 4 Satz 2 SGB V klar zum Ausdruck. Nur so weit die dort genannten Krankenhäuser nicht als Betreiber kritischer Infrastrukturen nach dem BSIG zu gelten haben, sollen die (neuen) Sicherheitsvorkehrungen der §§ 75 b, 75 c SGB V gelten.

5. Verstöße gegen die (neuen) §§ 75 b, 75 c SGB V sind – derzeit – nicht bußgeldbelegt. § 395 SGB V, der die Bußgeldvorschriften enthält, wurde vom Gesetzgeber nicht angepasst; eine Begründung hierfür findet sich in den Gesetzesmaterialien nicht. Demgegenüber sieht das BSIG in § 14 Bußgelder von bis zu 100.000 Euro für bestimmte ordnungswidrige Verhalten auch der Labor-KRITIS-Betreiber vor. Daraus kann abgeleitet werden, dass die Anforderungen und Verpflichtungen aus dem BSIG als prioritär gegenüber solchen aus § 75 b, 75 c SGB V zu bewerten sind.

7 Empfehlung

Dem Gesetzgeber wird empfohlen, für eine Klarstellung des Anwendungsbereichs des § 75 b SGB V zu sorgen. Diese gesetzliche Klarstellung kann in § 75 b Abs. 4 Satz 2 SGB V – in Anlehnung an § 75 c Abs. 3 SGB V – wie folgt eingefügt werden (Formulierungsvorschlag unterstrichen):

Die Richtlinie ist nicht anzuwenden für die vertragsärztliche und vertragszahnärztliche Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen getroffen werden und für die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer, die ohnehin als Betreiber kritischer Infrastrukturen gemäß § 8 a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

Labor-KRITIS-Betreibern empfehlen wir, auf Anfragen oder Aufforderungen zur Abgabe von Nachweisen zum Umsetzungsstand der KBV-IT-Sicherheits-Richtlinie auf den Status als Betreiber kritischer Infrastrukturen nach dem BSIG hinzuweisen.

Es ist bereits rechtsdogmatisch fraglich, ob die auf § 75 b Abs. 1 SGB V gestützte Richtlinie der KBV Nachweis- oder Informationsforderungen gegenüber vertrags(zahn) -ärztlichen Versorgungseinrichtungen begründen kann. Denn die Rechtsgrundlage für den Richtlinienerlass nach § 75 b Abs. 1 SGB V ermächtigt lediglich Anforderungen zur Gewährleistung der IT-Sicherheit festzulegen, ebenso die Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der Telematik-Infrastruktur. Weitergehende (Eingriffs-) Befugnisse gesteht diese Richtlinienkompetenz der KBV nicht zu, sodass die KBV allein durch die Richtlinie auch keine eigenen (Eingriffs-) Ermächtigungen schaffen darf.

Es gilt zu vermeiden, dass Labor-KRTIS-Betreiber zwei verschiedenen und nicht zwingend deckungsgleichen IT-Sicherheitsregimen unterworfen werden, weshalb bei fehlender Einigung mit der KBV die Einholung fachlicher und juristischer Expertise empfohlen wird.

Autoren

Prof. Dr. med. Andreas Becker

Öffentlich bestellter und vereidigter Sachverständiger für Qualitäts-, Informationssicherheits- und Risikomanagement in Krankenhäusern (IHK zu Köln) / Qualifikation „Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG“
Nonnenweg 120a
51503 Rösrath (Deutschland)
www.becker-sachverstaendiger.de
becker@becker-sachverstaendiger.de

Edgar Gärtner

Rechtsanwalt, Fachanwalt für Strafrecht, Compliance Officer (Univ.), Zertifizierter Verteidiger für Wirtschafts- und Steuerstrafrecht (DSV)
Viktoriastrasse 28
68165 Mannheim
www.gaertner-slania.de
gaertner@gaertner-slania.de

Interessenkonflikte

Keine.