Datenschutz newsbox

Ausgabe 02 2020

DATAKONTEXT

Editorial:

Während die Europäische Kommission überlegt, den Einsatz automatisierter Gesichtserkennung im öffentlichen Raum für die nächsten Jahre zu verbieten, schreitet die „Entwicklung" außerhalb von Europa weiter voran. Wobei die Entwicklung nicht in dem Voranschreiten der Technologie liegt, vielmehr schreitet der problematische Einsatz der bisherigen Technologie unter Missachtung europäischer Maßstäbe des Persönlichkeitsrechtschutzes voran.
Auch im Bereich der VR-Technologie stellen sich ethische Fragen: Ist es „in Ordnung", wenn sich eine Industrie mit der Digitalisierung von Menschen für ihre „posthume VR-Verwendung" kümmert? Ist es qualitativ etwas anderes, sich Videoaufnahmen von geliebten verstorbenen Menschen anzuschauen, als mit ihnen in einer VR-Umgebung in Interaktion treten zu wollen? Anstrengungen, nicht nur die Erinnerungen an Verstorbene wachzuhalten, sondern mit ihnen unter Zuhilfenahme von Technologie/KI auch „interagieren" zu können, gab es schon früher.

Es gibt aber auch weitaus profanere Ideen, wie sich mithilfe der Technologie Motive verfolgen lassen, die nicht dem ursprünglichen Zweck der Technologie entsprechen dürften. So kann es möglich sein, mit Hilfe von 99 Smartphones, die in einem Bollerwagen transportiert werden, einen Stau zu simulieren, um dadurch endlich tatsächlich weniger Autoverkehr zu erreichen oder für den Nutzer unsichtbare Schwankungen der Bildschirmhelligkeit zu nutzen, um damit geheime Daten von nicht mit dem Internet verbunden Rechnern oder Netzwerken auslesen zu können.

Nicht nur Technologie lässt sich für Zwecke verwenden, die auf den ersten Blick zweckfremd erscheinen. So können speziell ausgebildete Hunde bspw. Ermittlern inzwischen dabei helfen, Geräte wie Handys, Tablets, USB-Sticks, Festplatten und andere Datenträger aufzuspüren, auf denen möglicherweise Beweismittel verborgen sind. Ob man aber tatsächlich einer Firma seine genetischen Daten überlassen sollte, damit diese Firma eine auf die „persönliche Verstoffwechselung" angepasste Müsli-Mischung kreieren kann, muss am Ende wohl doch jeder selbst am besten wissen, meint

Ihr Levent Ferik

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Beschäftigtendatenschutz und DS-GVO

Ein spezielles Recht für den Beschäftigtendatenschutz wurde schon zu Zeiten vor Geltung der DS-GVO in wiederkehrender Regelmäßigkeit von vielen von DatenschutzexpterInnen, Personalprofis, Betriebsräten und anderen gefordert. Dies hat sich zwar mit Wirksamwerden der DS-GVO nicht wesentlich geändert, jedoch existiert nach wie vor kein in sich geschlossener Arbeitnehmerdatenschutz. Abgesehen von dem § 26 BDSG, der vom Regelungsgehalt her dem § 32 BDSG-alt recht nahekommt, existieren keine spezielleren datenschutzrechtlichen Normen zum Datenschutz im Beschäftigungsverhältnis. Daher lohnt es sich, noch einmal zusammenzufassen, was Aufsichtsbehörden und andere Institutionen zum Thema bisher an Informationsmaterialien veröffentlicht haben.

Ratgeber zum Beschäftigtendatenschutz mit Fallsammlung

Der LfDI Baden-Württemberg hat seinen „Ratgeber Beschäftigtendatenschutz“ im August 2019 aktualisiert hat und bietet diesen mittlerweile in der 3. Auflage an. Die Handreichung gibt einen Überblick über die Problemschwerpunkte des Beschäftigtendatenschutzes im privaten Bereich, wie sie an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) herangetragen werden, und zeigt die zulässige Verwendung personenbezogener Daten von Beschäftigten anhand von Praxisfällen auf.

Künstliche Intelligenz und Beschäftigtendatenschutz: Stellungnahme der GDD e.V.

Eine effektive Regelungsfähigkeit des Einsatzes der Künstlichen Intelligenz im Beschäftigungsverhältnis setzt deutlich erkennbare Anwendungsszenarien und damit einhergehende tatsächliche Veränderungen für die Arbeitswelt voraus, um hierfür regulierende Rahmenbedingen zu setzen. Die bestehenden datenschutzrechtlichen Regelungen ermöglichen den Einsatz von Künstlicher Intelligenz im Rahmen des Beschäftigungsverhältnisses. Insbesondere im laufenden Beschäftigungsverhältnis darf bei Personalentscheidungen nicht allein auf die Künstliche Intelligenz abgestellt werden. Die arbeitgeberseitige Fürsorgepflicht gebietet durch Künstliche Intelligenz erzeugte Entscheidungen zumindest eine Überprüfung durch einen entscheidungsbefugten Personalverantwortlichen. Die ausführliche Stellungnahme können Sie hier als PDF-Dokument downloaden.

Handreichung und Ratgeber zum Beschäftigtendatenschutz

Die Publikation der Stiftung Datenschutz mit dem Titel „Handreichung Beschäftigtendatenschutz“ trägt die wichtigsten Grundsätze und Regeln zusammen, die für den Datenschutz in Beschäftigungsverhältnissen gelten. Abgerundet wird die Handreichung mit Fallbeispielen zum Thema. Die Handreichung adressiert nach eigenen Angaben vor allem Personalverantwortliche in kleinen und mittelständischen Unternehmen, aber auch Betriebsräte und ganz allgemein an Beschäftigte.

Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz

Die Orientierungshilfe der DSK (Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder) zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten zu Whistleblowing-Hotlines auf. Sie soll es den Arbeitgebern und den Interessenvertretungen der Beschäftigten erleichtern, im Unternehmen klare Regelungen zum Umgang mit Whistleblowing-Hotlines zu erreichen.

Kurzpapier Nr. 14 Beschäftigtendatenschutz

Das Kurzpapier Nr. 14 der DSK gab schon früh nach dem Wirksamwerden der DS-GVO eine erste Hilfestellung zu den einzelnen Aspekten des Beschäftigtendatenschutzes und dürfte trotz seines Versionsstandes (Stand 17.12.2018) nützliche Hinweise beim Umgang mit Beschäftigtendaten enthalten.

Europäische Leitlinie zur Videoüberwachung

Mit Wirksamwerden der DS-GVO hat der Europäische Datenschutzausschuss (EDSA) seine Arbeit aufgenommen. In diesem Gremium sind Datenschutzaufsichtsbehörden aller europäischer Mitgliedstaaten sowie der Europäische Datenschutzbeauftragte und die Europäische Kommission vertreten. Eine wichtige Aufgabe besteht darin, allgemeine Leitlinien zur Interpretation der DS-GVO herauszugeben. Damit soll Klarheit hinsichtlich der Begriffe in den europäischen Datenschutzgesetzen im Sinne einer einheitlichen Auslegung geschaffen werden. Am 28./29. Januar 2020 tagte der EDSA zum 17. Mal.
Der Europäische Datenschutzausschuss hat in Rahmen dieser Sitzung eine Leitlinie zum datenschutzkonformen Einsatz von Videoüberwachung (Guidelines 3/2019 on processing of personal data through video devices) beschlossen. Vor dem Hintergrund, dass die seit Mai 2018 wirksame DS-GVO keine speziellen Regeln zur Videoüberwachung enthalte, sei dieses Ergebnis besonders begrüßenswert, so die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Maja Smoltczyk, die die Entstehung der Leitlinie als Hauptberichterstatterin betreut hat.

Wegen einer speziellen Regelung für die Videoüberwachung ist es notwendig, die datenschutzrechtlichen Anforderungen an den Einsatz von Videoüberwachung aus den allgemeinen Regelungen des Gesetzeswerks abgeleitet werden. Dies fordert nicht nur die Unternehmen, die Videotechnik rechtskonform einsetzen möchten, heraus. Die beschlossene Leitlinie ist daher als ein wichtiger Schritt, auf dem Weg zu einer europaweit einheitlichen Handhabung im Bereich der Videoüberwachung, zu bewerten.

Datenverarbeitung zum Zwecke der Forschung

Wojciech Wiewiórowski, der mit Beschluss vom 5. Dezember 2019 zum Europäischen Datenschutzbeauftragten (EDSB) ernannt wurde, hat eine Stellungnahme zum Datenschutz in der Wissenschaft/Forschung veröffentlicht.
Wiewiórowski geht in seinem neuen Papier darauf ein, dass die Grenze zwischen privatem Sektor und akademischer Forschung oftmals fließend sind. Wissenschaftliche Forschung sei auf den Austausch von Ideen, Wissen und Informationen angewiesen. Wenn sie die Verarbeitung von Daten über Personen in der EU beinhalte, unterliege die wissenschaftliche Forschung jedoch den geltenden Vorschriften der DS-GVO sowie der VO (EU) 2018/1725.
Der Stellenwert der DS-GVO-Prinzipien wie Gesetzmäßigkeit, Zweckbindung und die Gewährleistung der Grundrechte sei im Rahmen der wissenschaftlichen Forschung nicht anders zu bewerten als sonst. Die Risiken bei der Verarbeitung sensibler Gesundheitsdaten oder politischer oder religiöser Ansichten seien naturgemäß besonders hoch sein. Dies bedinge, dass, sofern eine an eine Einwilligung, als rechtliche Grundlage für die Verarbeitung genutzt werde, an diese, strenge Anforderungen zu knüpfen seien, und diese freiwillig, konkret, informiert und unzweifelhaft erteilt werden müsse.
Forscher, die innerhalb hoheitlich gesteckter ethischer Rahmen arbeiten, sollten daher Zugang zu notwendigen Programmierschnittstellen (API) und anderen Dateien haben, so der Europäische Datenschutzbeauftragte.
Der EDSB schließt in seiner Stellungnahme mit einer Empfehlung der Intensivierung des Dialogs zwischen den europäischen Datenschutzbehörden und Ethikräten ab. Diese sollten gemeinsam für ein einheitliches Verständnis hinsichtlich der EU-Verhaltensregeln für wissenschaftliche Forschung, einen engeren Abgleich zwischen den EU-Forschungsrahmenprogrammen und den Datenschutzbestimmungen arbeiten.

Quelle: Der Europäische Datenschutzbeauftragten (EDSB)

Anforderungen an die behördliche Nutzung Sozialer Netzwerke

Wie Ende Dezember 2019 angekündigt, hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW), Dr. Stefan Brink am 31.01.2020 den Twitter-Account seiner Behörde gelöscht.
Brink sah sich vor dem Hintergrund der Entscheidung des Bundesverwaltungsgerichts BVerwGE 6 C 15.18 nicht mehr in der Lage, den Auftritt seiner Behörde auf Twitter vertreten zu können. Danach ist der Betreiber einer Fanpage im sozialen Netzwerk Facebook für die bei Aufruf dieser Seite ablaufenden Datenverarbeitungsvorgänge verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG a.F. und damit potentieller Adressat einer Anordnung nach § 38 Abs. 5 BDSG a.F.

Wie im Rahmen der Vorstellung seines Datenschutz-Tätigkeitsberichts 2019 angekündigt, stellt der LfDI nun die wesentlichen Anforderungen an die behördliche Nutzung „Sozialer Netzwerke“ vor. Mit fünf klaren Anforderungen und seinen Erläuterungen dazu greift der LfDI BW die aktuelle Rechtsprechung des Europäischen Gerichtshofs und des Bundesverwaltungsgerichts zu „Sozialen Netzwerken“ auf und konkretisiert seine bereits 2017 vorgestellte „Richtlinie zur Nutzung von Sozialen Netzwerken“ weiter.

GDD-Praxishilfe „VVT für Auftragsverarbeitung“

Die Gesellschaft für Datenschutz und Datensicherheit hatte bereits Anfang 2017 zur Anpassung der Datenschutzorganisation an die ab Wirksamkeit der DS-GVO anstehenden Anforderungen ein an die DS-GVO angepasstes Vertragsmuster für Outsourcing-Dienstleistungen im Bereich der Auftragsverarbeitung herausgebracht.
Damals waren viele Einzelfragen noch in der Diskussion, sei es die Abgrenzung zur Funktionsübertragung oder zur gemeinsamen Verantwortlichkeit, das Fortbestehen der bisherigen Privilegierung von Auftragsverhältnissen oder schlicht die Anwendung auf Fernwartungsvorgänge.
Art. 30 DS-GVO sieht für Auftragsverarbeiter eine eigene kundenbezogene Dokumentation vor. Nach Erwägungsgrund 82 der DS-GVO soll der Auftragsverarbeiter „zum Nachweis der Einhaltung dieser Verordnung“ auch das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO führen. Die zuständige Aufsichtsbehörde kann die Vorlage verlangen, um die betreffenden Verarbeitungen hoheitlich zu kontrollieren. Dieses Verzeichnis von Verarbeitungstätigkeiten – Auftragsverarbeiter (VVT-AV) unterscheidet sich grundlegend von der prozessbezogenen Dokumentation, die der Verantwortliche gemäß Art. 30 Abs. 1 DS-GVO zu führen hat. Daher widmet die GDD diesem Thema eine eigene Praxishilfe.

>> Diese Praxishilfe und weitere können Sie hier downloaden.
>> Direktdownload (PDF)

DS-GVO-Verstöße abmahnbar?

Mit der Datenschutz-Grundverordnung (DS-GVO) war von Anfang an eine große Angst vor Abmahnungen im Falle von Verstößen gegen sie verbunden. Ob ein Verstoß gegen die DS-GVO abmahnfähig ist, bestimmt sich nach § 3a UWG danach, ob die verletzte Regelung eine Marktverhaltensregelung darstellt. Das OLG Naumburg (Urteil vom 07.November 2019,9 U 6/19) stellte dies nun als einen Verstoß gegen die DS-GVO fest.

Wettbewerb zwischen Apothekern

Im Sachverhalt machte der Kläger, der als Apotheker tätig ist, gegen den Beklagten Unterlassungsansprüche, Auskunftsansprüche und die Feststellung einer Schadensersatzverpflichtung aus Wettbewerbsrecht wegen des Vertriebes apothekenpflichtiger rezeptfreier Medikamente über eine Internethandelsplattform geltend. Der Beklagte ist ebenfalls Apotheker und vertreibt online apothekenpflichtige Medikamente. Nach Ansicht des Klägers verstößt der Mitbewerber gegen die DS-GVO, da er keine Einwilligung zur Verarbeitung von Gesundheitsdaten nach Art. 9 DS-GVO einholte.

Wettbewerbsverletzung durch apothekenpflichtige Medikamente über Amazon

Das OLG hatte in seiner Entscheidung nun die Frage zu beantworten, ob Verstöße gegen die DS-GVO abmahnfähig sind. Nach Ansicht des OLG handelt es sich bei Art. 9 DS-GVO tatsächlich um eine Marktverhaltensregelung, sodass der Verstoß abgemahnt werden kann. Grundsätzlich schützen die Datenschutzregeln in erster Linie das grundrechtlich geschützte informationelle Selbstbestimmungsrecht des Einzelnen. Gleichzeitig soll durch ein einheitliches Schutzniveau der grenzüberschreitende Verkehr personenbezogener Daten vereinheitlicht und eine Verfälschung des Wettbewerbs verhindert werden. Durch die Rückschlüsse, die aus den Bestelldaten über die Gesundheit des Bestellers gezogen werden können, ist der Anwendungsbereich des Art. 9 DS-GVO eröffnet. Auch wenn die Daten, die Amazon für den Bestellvorgang apothekenpflichtiger Medikamente erfasst, keine Gesundheitsdaten im engeren Sinne, wie z.B. ärztliche Befunde, darstellen, sind sie aufgrund des Sachzusammenhangs doch als personenbezogene Daten besonderer Kategorien zu qualifizieren.

Keine einheitliche Rechtsprechung zu Abmahnungen

Ob die DS-GVO nun eine Marktverhaltensregelung im Allgemeinen darstellt, lässt sich nicht im Allgemeinen bejahen. Vielmehr müssen alle 99 Artikel der DS-GVO einzeln geprüft werden, ob sie als marktverhaltensregelnd qualifiziert werden können oder eben nicht. Abmahnungen sind aber nach wie vor die große Ausnahme. Die deutsche Rechtsprechung ist in dieser Hinsicht nämlich nach wie vor wenig konsistent und verneint die Abmahnfähigkeit häufig bereits aus anderen Gründen.

Praxishilfen zum Gesundheitsdatenschutz

Unter der Mitarbeit des GDD-Arbeitskreises „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“ (AK GSW) wurden Praxishilfen zu den Themen „Datenschutz und klinische Register“ sowie „Datenschutz bei klinischen Studien“ erarbeitet und veröffentlicht.
Die Arbeitshilfe „Datenschutz und klinische Register“ führt anhand ihres strukturellen Aufbaus durch die wesentlichen datenschutzrechtlichen Aspekte, die bei der Errichtung und beim Betrieb von klinischen Registern zu beachten sind. Zu diesen Aspekten gehört beispielsweise der Umstand, dass Patientendaten in Gesundheitseinrichtungen vorrangig zum Primärzweck der Patientenversorgung erhoben bzw. verarbeitet werden und eine Verarbeitung zum Zweck der Verwendung in einem klinischen Register lediglich nachrangig erfolgt. In der Praxis entwickeln sich klinische Register aber zu einem wertvollen und unverzichtbaren Instrument, welches die Beurteilung von Therapieverhalten unter Realbedingungen ermöglichen kann. Mithilfe dieser Register kann z.B. dargestellt werden, wie sich die Versorgungslage in Ländern darstellt, aber auch wo ggf. Verbesserungspotential besteht. Ein Beispiel hierfür bildet das sogenannte Trauma Register, welches die Verbesserung der Versorgung Unfallverletzter in den letzten 20 Jahren maßgeblich beeinflusst hat. Grundsätzlich benötigen klinische Register daher Patientendaten um ihre Zwecke, unter anderem Forschung und Qualitätssicherung, mit Erfolg erfüllen zu können. Eine Verarbeitung von Patientendaten für diese Ziele erfolgt daher auf Grund einer sogenannten datenschutzrechtlichen „Sekundärnutzung“ für die Zwecke klinischer Register. Für die Zulässigkeit dieses sekundären Verarbeitungszwecks personenbezogener Daten bedarf es aber immer eines entsprechenden Erlaubnistatbestands des anwendbaren Datenschutzrechts. Die entsprechenden datenschutzrechtlichen Bestimmungen müssen diesbezüglich bei der Erstellung sowie dem Betrieb und der Pflege von klinischen Registern beachtet und nachweisbar eingehalten werden. Mithilfe dieser Praxishilfe soll unter anderem Betreibern von klinischen Registern eine Hilfestellung gegeben werden, damit datenschutzrechtlichen Herausforderungen entsprechend begegnet werden kann.

Datenschutz bei klinischen Studien

Die Arbeitshilfe „Datenschutz bei klinischen Studien“ wurde entwickelt, um sowohl Forscher als auch Datenschutzbeauftragte im Umgang mit datenschutzrechtlichen Anforderungen klinischer Studien zu unterstützen. Klinische Studien verfolgen das Ziel einer stetigen Verbesserung von eingesetzten Diagnose- und Therapiemethoden und bilden daher einen unverzichtbaren Pfeiler des medizinischen Fortschritts. Im Gegensatz zu anderen Forschungsmethoden werden bei jeder klinischen Studie sensible Gesundheitsdaten oder auch genetische Daten von Betroffenen im Rahmen der Studie direkt verarbeitet. Dies ist vor dem Hintergrund bedeutsam, dass eine diesbezügliche Verarbeitung von besonderen Kategorien personenbezogener Daten stets erhebliche Risiken für Grundrechte und Grundfreiheiten betroffener Personen mit sich bringt. Der Umgang mit den genannten Daten bedarf daher stets besonderer Sorgfalt. Die Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben bei klinischen Studien ist unabdingbar, weil selbst im Umgang mit anonymisierten Daten die hierfür verarbeiteten Daten zunächst personenbezogen erfasst werden müssen, bevor sie in einem weiteren Verarbeitungsschritt zu anonymisierten Daten verarbeitet werden. Bei dieser Umsetzung datenschutzrechtlicher Vorgaben, welche zu jeder seriösen Studie gehören, soll diese Arbeitshilfe wertvolle Unterstützungsarbeit leisten.

Download

Beide Praxishilfen können Sie im Word-, Pdf-, Epub- oder Azw3-Format kostenfrei auf den Seiten der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V. herunterladen. Die Praxishilfe „Datenschutz und klinische Register“ finden Sie unter: https://gesundheitsdatenschutz.org/html/klin_register.php. Die Praxishilfe „Datenschutz bei klinischen Studien“ können Sie unter https://gesundheitsdatenschutz.org/html/klin_studien.php abrufen.

Studie beleuchtet Fragestellungen zum Digitalen Nachlass

Hinterbliebene stehen vor vielen Herausforderungen, wenn sie an Vertragsinformationen gelangen müssen und Online-Konten von Verstorbenen verwalten sollen. Ohne Passwörter und Zugangsdaten haben Erben oft keinen Zugriff auf den digitalen Nachlass wie Online-Konten. Sie können sich nicht umlaufende Geschäfte wie Internetauktionen, Abos oder Bestellungen kümmern oder Verträge kündigen. Im schlimmsten Fall entstehen hohe laufende Kosten und finanzielle Schäden. Nur wenige Unternehmen stellen bislang Regeln auf, unter welchen Bedingungen ein Account aufgelöst werden kann und wer darüber entscheiden darf. Manche Regelungen sind zudem rechtlich fragwürdig.
Der Bundesgerichtshof hat 2018 zur Vererblichkeit von Nutzungsverträgen mit sozialen Netzwerken festgestellt, dass das Erbrecht des Bürgerlichen Gesetzbuchs auch für den digitalen Nachlass uneingeschränkt Anwendung findet. Danach rückt der Erbe auch hinsichtlich des digitalen Nachlasses vollständig in die Stellung des Erblassers ein.
Was passiert nach dem Tod eines Menschen mit dessen digitalen Daten? Wie vererbt man wertvolle Accounts in Online-Spielen oder PayPal-Guthaben? Es gibt viele offene Fragen im Umgang mit dem digitalen Nachlass eines Menschen.

Handlungsempfehlungen für den Umgang mit digitalem Nachlass

Die Studie befasst sich deshalb mit den wichtigsten praktischen, rechtlichen und technischen Fragen des Vererbens von digitalen Daten und Vermögenswerten und gibt Handlungsempfehlungen für die Praxis. Erstellt wurde die Studie vom Fraunhofer-Institut für Sichere Informationstechnologie SIT gemeinsam mit der Universität Regensburg und der Universität Bremen/IGMR. Die Erstellung der Studie wurde vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) gefördert.
Die gesamte Studie kann unter folgendem Link kostenfrei heruntergeladen werden: www.sit.fraunhofer.de/digitalernachlass. Zudem findet sich dort eine kurze Zusammenfassung der Studie mit allen Empfehlungen an Verbraucherinnen und Verbraucher, Erben, Unternehmen, Vorsorgebevollmächtigte sowie den Gesetzgeber

Quelle: Fraunhofer-Institut für Sichere Informationstechnologie

Anforderungen für IT-Sicherheit der vertragsärztlichen und -zahnärztlichen Versorgung

Die Kassenärztliche Bundesvereinigung (KBV) hat bis zum 30. Juni 2020 eine Richtlinie vorzulegen, womit die Anforderungen an die IT-Sicherheit in der vertragsärztlichen und -zahnärztlichen Versorgung geregelt werden sollen. Diese müssen geeignet sein, Störungen der informationstechnischen Systeme zu vermeiden. Dieser Auftrag des Gesetzgebers resultiert aus der Normierung eines neuen § 75b SGB V. Teil der Sicherung soll auch die Sicherung der Telematikinfrastruktur sein, woran speziell die Gesellschaft für Telematik (gematik) beteiligt werden soll. In die Bewertung der allgemeinen Anforderungen sollen insbesondere der aktuelle Stand der Technik und das Gefährdungspotenzial einfließen, einschließlich einer jährlichen Aktualisierung.

Beteiligung und Zustimmung zahlreicher Akteure

Die Richtlinie verlangt das Einvernehmen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und die Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), der Bundesärztekammer, der Bundeszahnärztekammer, der Deutschen Krankenhausgesellschaft und der für die Wahrnehmung der Interesse der Industrie maßgeblichen Bundesverbände aus dem Bereich der Informationstechnologie im Gesundheitswesen.

Für wen gilt die Richtlinie?

Diese Richtlinie ergeht verbindlich für alle Einrichtungen der vertragsärztlichen und -zahnärztlichen Versorgung. Ausgenommen sind lediglich die Krankenhäuser, die bereits angemessene Vorkehrungen nach § 8a Abs. 1 des BSI-Gesetzes getroffen haben. Bei der Umsetzung der Richtlinie sind die Leistungserbringer von eigens zertifizierten Anbietern zu unterstützen. Die Anforderungen an eine Zertifizierung dieser Anbieter muss das BSI bis zum 31. März 2020 erstellen.