Bayerisches Landesamt für Datenschutzaufsicht

Tätigkeitsbericht 2017/2018

Das für Arztpraxen zuständige Landesamt für Datenschutzaufsicht hat auf seinen nun öffentlich zugänglichen Tätigkeitsbericht hingewiesen. Diesen finden Sie im Internet unter: www.lda.bayern.de/media/baylda_report_08.pdf

Die wesentlichen Gesichtspunkte lesen Sie im folgenden Beitrag.

Der Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht kann unter www.lda.bayern.de/media/baylda_report_08.pdf heruntergeladen werden.

(4) Kontrollen und Prüfungen

Die *Frankfurter Allgemeine Zeitung* (F.A.Z.) berichtete am 9. April 2019 über das Risiko, dass „Ärzte anfällig für Hacker sind" und sieht nur wenige Praxen ausreichend geschützt.

Ransomware bei Arztpraxen (Seite 34)
Das Landesamt weist darauf hin, dass Verschlüsselungstrojaner ebenso in Bayern weiterhin aktiv sind. Durch die Schadsoftware wird der Zugriff auf Daten gesperrt und anschließend Lösegeld gefordert. Betroffen waren in dem Berichtszeitraum nach den eingehenden Meldungen oft Ärzte und kleinere Betriebe, die sich entweder der Gefährdungslage nicht bewusst waren oder nur über unzureichende Sicherungsmaßnahmen verfügten, weshalb sich das Landesamt für Datenschutzaufsicht entschied, Ärzte zum Umgang und zur Prävention von Ransomware-Attacken zu kontrollieren. Ziel war es, für ein geeignetes und wirksames Backupverhalten zu sorgen, damit Patientendaten vor der realen Gefahr solcher Kryptotrojaner angemessen geschützt werden. Die befragten Praxen hatten folgende Fragen zu beantworten:

- Werden regelmäßige, automatisierte Backups der Patientendaten durchgeführt?
- Mit welcher Software werden Backups durchgeführt?
- Auf welchen Speichermedien werden die Backups gespeichert?
- Wird das Zurückspielen von Backup-Daten getestet?
- Ist das Praxisverwaltungssystem ans Internet angeschlossen?
- Befinden sich an das Internet angeschlossene Rechner in anderen Netzsegmenten als das Praxisverwaltungssystem?
- Sind Netzlaufwerke mit relevanten Patientendaten mit Rechnern verbunden, die an das Internet angeschlossen sind?
- Wurden Awareness-Schulungen durchgeführt, die Internetbedrohungen (zum Beispiel Schadcode, Phishing, ...) zum Inhalt hatten?

Im Ergebnis sei bei der ersten Sichtung der eingegangenen Antworten zu erkennen, dass Ärzte meist nicht optimal auf derartige Angriffe vorbereitet sind. Erfreulich war jedoch, dass die bisherige Prüfung ergab, dass die Praxisinhaber durchgängig von der Gefahrensituation durch Ransomware wussten und ihre Mitarbeiter diesbezüglich sensibilisierten.

(7) Betroffenenrechte

Informationspflicht von Ärzten (Seite 45)

Deutlich hervorgehoben wird, dass Patienten nicht unterschreiben müssen, dass sie die Datenschutzinformationen in der Arztpraxis zur Kenntnis genommen haben. Im Übrigen wird betont – dies erscheint mir für medizinisch/ärztliche Callcenter oder für Anbieter von Fernbehandlungen von ganz erheblicher Bedeutung –, dass die Aufzeichnung von Telefongesprächen der informierten Einwilligung des externen Gesprächspartners bedarf.

Auskunft (Seite 46)

Patienten, die ihr Recht auf Auskunft geltend machen, ist eine vollständige Übersicht der Daten in verständlicher Form von den Arztpraxen zu geben, ohne dass dabei medizinische Fachbegriffe erläutert werden müssen.

In dem Zusammenhang wird auf die Unsicherheit zwischen dem Verhältnis des Art. 15 Datenschutz-Grundverordnung (DS-GVO) und § 630 g Bürgerliches Gesetzbuch (BGB) Bezug genommen. Verlangt werden könne, so im Bericht, dass der Antragsteller nach Art. 15 DS-GVO eine vollständige Übersicht der Daten in verständlicher Form erhält. Das bedeute aber nicht, dass ein Arzt einem Auskunft begehrenden Patienten in der Patientenakte stehende Begriffe oder sonstige Kurzbezeichnungen erläutern müsse. Als Einschränkung der Auskunftspflicht nach Art. 15 DS-GVO ist nach Meinung des Landesamtes für Datenschutzaufsicht sinnvoll, die Regelung des § 630 g Abs. 1 Halbsatz 2 BGB analog heranzuziehen. **Schließlich begründe das Auskunftsrecht über gespeicherte personenbezogene Daten keinen allgemeinen Anspruch auf Kopien von Dokumenten.** Unter Verweis auf die Rechtsprechung des Europäischen Gerichtshofes (EuGH) vom 17. Juli 2014 (C-141/12 und C-372/12) wird festgestellt, dass der Antragsteller eine vollständige Übersicht dieser Daten in verständlicher Form erhalten muss, jedoch nicht mehr. Das Landesamt für Datenschutzaufsicht sieht diese Rechtsprechung auch in Bezug auf das Verhältnis des Art. 15 DS-GVO zu § 630 g BGB für einschlägig an. Es stellt abschließend fest, dass manche bereichsspezifische Vorschriften über den datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DS-GVO hinausgehen, wie zum Beispiel § 630 g BGB mit dem Recht von Patienten auf elektronische Abschrift der Patientenakte, allerdings gegen Kostenerstattung.

Berichtigung (Seite 47)

Das Landesamt für Datenschutz weist im Tätigkeitsbericht darauf hin, dass gespeicherte Werturteile einem Berichtigungs- bzw. Löschungsanspruch zugänglich seien und verweist in dem Zusammenhang auch auf die Berichtigung in Versicherungs- oder Arztakten.

Löschung bei Patientendaten (Seite 48)

Hierzu betont das Landesamt, dass personenbezogene Daten insbesondere dann zu löschen sind, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 a DS-GVO). Eine Löschpflicht bestehe hier auch ohne Aufforderung durch den Betroffenen. Weiter wird hervorgehoben, dass sich eine Ausnahme von dieser Pflicht aus Art. 17 Abs. 3 e DS-GVO ergebe, da die objektive Verjährungsfrist für Schadensersatzansprüche wegen Körper- oder Gesundheitsverletzungen gemäß § 199 Abs. 2 BGB 30 Jahre nach Vornahme des potenziell schadensträchtigen Verhaltens betrage. Hierbei sei eine Abwägung unter Berücksichtigung der Interessen der Betroffenen und der Wahrscheinlichkeit der Geltendmachung von Ansprüchen vorzunehmen. Grundsätzlich Patientendaten für die Dauer von 30 Jahren aufzubewahren, wäre, so das Landesamt, nicht datenschutzkonform, weshalb eine individuelle Risikobewertung erforderlich sei.

Datenübertragbarkeit bei Ärzten (Seite 49)

Unter Bezugnahme auf einen unter diesem Punkt geschilderten Fall verlangte ein Patient von einem medizinischen Labor, unter Verweis auf sein Recht auf Datenübertragbarkeit (Art. 20 Abs. 1 lit. a DS-GVO), die Laborrechnung in einem maschinenlesbaren Format, um die Angaben für seine Zwecke bequem weiterverarbeiten zu können. Das Landesamt erklärt, dass personenbezogene Daten, die auf der Rechtsgrundlage des Art. 9 Abs. 2 h DS-GVO verarbeitet werden (wie zum Beispiel die Verarbeitung von Patientendaten in einem medizinischen Labor) nicht vom Recht auf Datenübertragbarkeit erfasst sind.

Bewertungsportale (Seite 52)

Unter Bezugnahme auf den Tätigkeitsbericht 2013/2014 (dort Punkt 7.5) wurde auf die damalige datenschutzrechtliche Bewertung Bezug genommen. Nunmehr sei auf der Grundlage der DS-GVO eine Welle weiterer Eingaben, insbesondere von Ärzten, festzustellen, die das Erfordernis einer grundsätzlichen datenschutzrechtlichen Neubewertung sehen. Das Landesamt weist darauf hin, dass es allerdings eine nahezu gleichlautende Rechtsgrundlage für eine rechtmäßige Verarbeitung personenbezogener Daten fände, wie dies in den Vorschriften der früheren Fassung des Bundesdatenschutzgesetz (BDSG) der Fall war und Grundlage für die Beurteilung der grundsätzlichen datenschutzrechtlichen Zulässigkeit gewesen sei. Eine Verarbeitung sei auch jetzt rechtmäßig, wenn

» die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordert, überwiegen. Art. 17 Abs. 3 a DS-GVO bestimme, dass ein Recht auf Löschung personenbezogener Daten nicht bestehe, soweit die Verarbeitung erforderlich sei zur Ausübung des Rechts auf Meinungsfreiheit und Information. Zugesichert wird jedoch, dass die Rechtsprechung über Anträge auf Löschung von Profilen in Arztbewertungsportalen auf der Grundlage der DS-GVO beobachtet wird und sich daran das Prüfverhalten orientieren werde.

Datenschutzbestimmungen auf Websites (Seite 53)

Einen breiten Raum nimmt das bezeichnete Thema ein. Besonders wird dabei die Frage des Einsatzes von WhatsApp im beruflichen Umfeld angesprochen. Zusammenfassend bestehen bezüglich des Einsatzes von WhatsApp im beruflichen Umfeld große Datenschutzbedenken, da die Daten diesbezüglich nicht geschützt werden können und von der Vielzahl der Kontakte das Einverständnis hierfür nicht vorliegt. Auf Seite 58 werden Alternativen zu WhatsApp namentlich benannt, die als sichere Plattformen gelten.

Speziell zur Gesundheit (Seite 91 ff.)

Einen eigenen Punkt (16.) nimmt die Gesundheit ein. Hier geht das Landesamt auf die Frage der Einwilligung ein und erklärt, dass von Patienten oft unnötige Einwilligungen für die Datenverarbeitung verlangt würden. Eine Einwilligung sei zum Beispiel bei der Abrechnung durch private Abrechnungsstellen notwendig oder im Einzelfall, auf der Grundlage nationaler Vorschriften, wie zum Beispiel dem § 73 Abs. 1 b Sozialgesetzbuch (SGB) V.

Einen deutlichen Verbesserungsbedarf sieht die Datenschutzbehörde bei der Anmeldung im Sprechzimmer und spricht dabei Diskretionsmissstände an. Das Landesamt gibt Empfehlungen, wie beispielsweise der Bereich an der Anmeldung geschützt werden kann. Besonders betont das Landesamt, dass der Patient in der Arztpraxis durchaus mit Namen angesprochen werden könne, da dies gesellschaftsüblich und es deshalb nicht erforderlich sei, in Arztpraxen ein Nummernsystem einzuführen oder auf eine unpersönliche Ansprache auszuweichen. Die Frage, ob Ärzte bei Anfragen von Gerichten die Vorlage einer Schweigepflichtentbindungserklärung verlangen müssten, wird verneint und Bezug genommen auf einen Beschluss des Sozialgerichts Frankfurt vom 24. September 1998, wonach der Arzt nicht berechtigt sei, das Zeugnis mit dem Argument zu verweigern, das Gericht habe ihm gegenüber die Entbindung von der Schweigepflicht nicht nachgewiesen. Es sei ausreichend, wenn das Gericht dem Arzt mitteilt, dass die entsprechende Erklärung vorliege. Zum eigenen Punkt Abholung von Rezepten und Vereinbarung von Arztterminen durch den Ehepartner erklärt das Landesamt, dass diesbezüglich die Einwilligung und eine Schweigepflichtentbindungserklärung notwendig seien. In dem Zusammenhang wird darauf hingewiesen, dass zwar strafrechtlich betrachtet ein konkludentes Handeln ausreiche, jedoch gemäß Art. 9 Abs. 2 a DS-GVO eine ausdrückliche Einwilligung des Patienten vorliegen müsse. Hierfür reiche jedoch eine einmalige entsprechende Erklärung aus. Zur E-Mail-Kommunikation zwischen Arzt und Patient erklärt das Landesamt, dass ein Patient bei der E-Mail-Kommunikation mit dem Arzt auf eigenen Wunsch auf die Ende-zu-Ende-Verschlüsselung verzichten könne. Dennoch wird dringend empfohlen und dies auch für notwendig erachtet, beim E-Mail-Verkehr eine Transport- und eine Inhaltsverschlüsselung vorzunehmen.

Soweit ein kurzer Einblick in den 138 Seiten umfassenden Tätigkeitsbericht.

Peter Kalb (BLÄK)