Der Bayerische Landesbeauftragte
für den Datenschutz

Auftragsverarbeitung bei bayerischen öffentlichen Krankenhäusern

Aktuelle Kurz-Information 43

Stichwörter: Auftragsverarbeitung – Gesundheitsdienstgesetz 2022 – Krankenhäuser, bayerische öffentliche – Krankenhausgesetz, Bayerisches – Patientendaten | **Stand:** 1. Juni 2022

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Nach Aufhebung von Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz erweitern sich die Handlungsmöglichkeiten bayerischer öffentlicher Krankenhäuser bei der Begründung von Auftragsverarbeitungsverhältnissen.
- Die Begründung von Auftragsverarbeitungsverhältnissen unterliegt allerdings weiterhin den gesetzlichen Bindungen insbesondere aus der Datenschutz-Grundverordnung.

Bayerische öffentliche Krankenhäuser durften sich bislang zur Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patientinnen und Patienten erforderlich sind, nur anderer Krankenhäuser bedienen. Diese nicht mehr ganz zeitgemäße Vorgabe aus Art. 27 Abs. 4 Satz 6 Bayerisches Krankenhausgesetz (BayKrG) in der bis zum 31. Mai 2022 geltenden Fassung hat der bayerische Gesetzgeber durch die am 1. Juni 2022 in Kraft getretene Novelle des Gesundheitsdienstgesetzes (GDG)[1] aufgehoben. Das hat zur Folge, dass Auftragsverarbeitungsverhältnisse insoweit nun auch mit anderen Auftragsverarbeitern als Krankenhäusern begründet werden dürfen. Der in Art. 27 Abs. 4 BayKrG verbleibende Regelungsbestand wird weiterhin durch die allgemeinen Regelungen der Datenschutz-Grundverordnung (DSGVO) zur Auftragsverarbeitung ergänzt; ein regelungsloser Zustand tritt nicht ein. 1

Was die Rechtsänderung betrifft, möchte ich bayerische öffentliche Krankenhäuser auf folgende Gesichtspunkte aufmerksam machen: 2

1. Gestaltungsimpulse bei Auftragsverarbeitung im Krankenhaus

Die Gesetzesänderung macht bewusst, dass bayerische öffentliche Krankenhäuser Patientendaten betreffende Auftragsverarbeitungsverhältnisse mit externen IT-Dienstleistern nun noch mehr als bislang aktiv gestalten müssen. Das ist keine „banale“ Aufgabe: 3

- In Krankenhäusern werden große Mengen an Daten verarbeitet, welche die Gesundheit der Patientinnen und Patienten und damit deren intimsten Lebensbereich betreffen.
- Durch die Beteiligung externer Stellen wird der Kreis derer, die mit sensiblen medizinischen Patientendaten in Berührung kommen, größer. Gleichzeitig sinken die direkten Einflussmöglichkeiten der Krankenhäuser auf den Umgang mit den Daten ihrer Patientinnen und Patienten.

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

- Krankenhäuser sind nicht selten Opfer von Cybercrime-Attacken mit teilweise schwerwiegenden Folgen für die Patientinnen und Patienten. Eine Konzentration der Patientendatenverarbeitung auf wenige IT-Dienstleister erhöht die Attraktivität und damit die Eintrittswahrscheinlichkeit von Cybercrime-Angriffen in diesem Bereich.

- Für die Verarbeitung setzen nicht wenige IT-Dienstleister Betriebsmittel ein, bei denen die Zulässigkeit einer (möglichen) Datenübermittlung in ein Drittland oder an eine internationale Organisation gewährleistet sein muss. Übermittlungen dieser Art sind seit Geltungsbeginn der Datenschutz-Grundverordnung allerdings strikt reglementiert, wie das Urteil des Europäischen Gerichtshofs in der Rechtssache Schrems II[2] zeigt. Dabei ist zu beachten, dass auch ein Fernzugriff, den eine Stelle in einem Drittland auf die im Europäischen Wirtschaftsraum befindlichen Patientendaten hat, eine Übermittlung begründen kann.

- Im Krankenhausbereich sind mit zunehmender Digitalisierung sehr viele neue, innovative Formen der Verarbeitung von Patientendaten – oft unter Beteiligung mehrerer Stellen – zu beobachten. In diesem Zusammenhang ist es empfehlenswert, frühzeitig die jeweilige datenschutzrechtliche Rolle einer an der Verarbeitung beteiligten Stelle (wie etwa eigenständiger oder gemeinsamer Verantwortlicher, Auftragsverarbeiter, Datenexporteur, Datenimporteur) mit ihren datenschutzrechtlichen Pflichten und Befugnissen zu identifizieren und die damit erforderlichen Nachweise und sonstigen Unterlagen zu erarbeiten (wie beispielsweise eine Auftragsverarbeitungsvereinbarung, eine Datenschutz-Folgenabschätzung oder eine allgemeine Risikoanalyse).

- Die fortschreitende Digitalisierung und die wachsende Komplexität aktueller IT-Systeme führen regelmäßig dazu, dass IT-Dienstleister als Auftragsverarbeiter zur Erbringung ihrer Leistungen weitere Unterauftragsnehmer nutzen, deren Verarbeitung ebenfalls die Anforderungen der Datenschutz-Grundverordnung erfüllen müssen (vgl. Art. 28 Abs. 4 DSGVO).

2. Regelungsrahmen

4 Bayerische öffentliche Krankenhäuser müssen bei der Begründung von Auftragsverarbeitungsverhältnissen weiterhin die Regelungen beachten, welche die Datenschutz-Grundverordnung dafür bereithält. Dies betont auch der neu gefasste Art. 27 Abs. 6 BayKrG. Darin heißt es seit dem 1. Juni 2022:

> „Im Anwendungsbereich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), insbesondere Art. 28 DSGVO (Auftragsverarbeiter) und Art. 32 DSGVO (Sicherheit der Verarbeitung), sind besondere Schutzmaßnahmen technischer und organisatorischer Art zu treffen, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können."

5 Bayerische öffentliche Krankenhäuser können bei der Erfüllung dieser Aufgabe auf vielfältige Informationsmaterialien zurückgreifen. Zu nennen sind insbesondere:

- meine Orientierungshilfe „Auftragsverarbeitung";[3]

- mein „Leitfaden zum Outsourcing kommunaler IT";[4]

- meine Aktuelle Kurz-Information 39 „Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen“;[5]
- meine Materialien zur Risikoanalyse;[6]
- das Vertragsmuster zur Auftragsverarbeitung des Bayerischen Staatsministeriums des Innern, für Sport und Integration;[7]
- die „Leitlinien 07/2020 zu den Begriffen ‚Verantwortlicher‘ und ‚Auftragsverarbeiter‘ in der DSGVO“ des Europäischen Datenschutzausschusses[8] sowie
- die „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ des Europäischen Datenschutzausschusses.[9]

Dass bei der Erfüllung dieser Aufgabe ein Synergiepotenzial für die bayerischen Krankenhäuser besteht, spricht die Gesetzesbegründung zum neuen Gesundheitsdienstgesetz ausdrücklich an: 6

> „Durch die Aufhebung von Art. 27 Abs. 4 Satz 6 BayKrG gehen bewährte Schutzelemente für die Verarbeitung von Patientendaten zunächst ersatzlos verloren. Diese Lücke sollte für die verantwortlichen Krankenhäuser bedarfsgerecht und idealerweise auf Selbstverpflichtungsbasis zum Beispiel durch ein einvernehmlich geschaffenes Regelwerk geschlossen werden, welches nach Maßgabe der Datenschutz-Grundverordnung die unabdingbaren technischen und organisatorischen Maßnahmen präzisiert und damit den Weg ebnet für eine möglichst einheitliche Anwendungspraxis bei gleichbleibend hohem Schutzniveau für die Patientendaten. Ein derartiges Regelwerk zur Präzisierung der technischen und organisatorischen Maßnahmen könnte beispielsweise seitens der Interessensvertretung der bayerischen Krankenhausträger und deren Spitzenverbände ins Leben gerufen werden.“[10]

Um ein einheitlich hohes Sicherheits- und Datenschutzniveau sicherzustellen, empfehle ich den beteiligten Verkehrskreisen nachdrücklich, möglichst zeitnah mit der Erarbeitung eines solchen Regelwerks zu beginnen. 7

1 Vom 10. Mai 2022 (GVBl. S. 182). – Die Aufhebung von Art. 27 Abs. 4 Satz 6 BayKrG ist in Art. 32c Nr. 2 Buchst. a GDG geregelt, das Inkrafttreten in Art. 33 Abs. 1 Satz 1 GDG.
2 Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18.
3 Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“.
4 Stand 3/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“.
5 Stand 12/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen“.
6 Überblick im Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA“.
7 Internet: https://www.innenministerium.bayern.de, Rubrik „Schutz und Sicherheit – Datenschutz und Cybersicherheit – Schutz persönlicher Daten – Datenschutzreform-Arbeitshilfen“.
8 Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de.

[9] Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

[10] LT-Drs. 18/19685, S. 30.