BayLDA

Der Bayerische Landesbeauftragte
für den Datenschutz

und

Bayerisches Landesamt für
Datenschutzaufsicht

Leitfaden

Anforderungen an das Datenschutz-management in bayerischen öffentlichen und privaten Krankenhäusern

Stand: März 2018

Bayerischer Landesbeauftragter für den Datenschutz	Hausanschrift Wagmüllerstr. 18 80538 München	Postanschrift Postfach 221219 80502 München	Tel. 089.212672-0 Fax 089.212672-50	www.datenschutz-bayern.de E-Mail: poststelle@datenschutz-bayern.de
Bayerisches Landesamt für Datenschutzaufsicht	Hausanschrift Promenade 27 91522 Ansbach	Postanschrift Postfach 606 91511 Ansbach	Tel. 0981.53-1300 Fax 0981.53-5300	www.lda.bayern.de E-Mail: poststelle@lda.bayern.de

Inhaltsverzeichnis

Einleitung

Wie schon in dem Papier „Anforderungen an Technik und Sicherheit der Verarbeitung“ des Bayerischen Landesbeauftragten für den Datenschutz[1] dargelegt, stellt die Datenschutz-Grundverordnung (DSGVO) erhöhte Anforderungen an den Nachweis, dass ausreichende Maßnahmen zur Sicherstellung des Datenschutzes ergriffen wurden (Rechenschaftspflicht, vgl. Art. 5 Abs. 2, Art. 24 Abs. 1 Satz 1 DSGVO). Diese Pflicht ist dem für die Datenverarbeitung Verantwortlichen im Sinne des Art. 4 Nr. 7 DSGVO – also dem öffentlichen oder privaten Krankenhaus selbst – zugewiesen; dem Datenschutzbeauftragten des Krankenhauses kommt in diesem Zusammenhang allein eine Beratungs- und Überwachungsaufgabe zu (vgl. Art. 39 Abs. 1 DSGVO). Nachweisbarkeit bedeutet insbesondere, dass die gemäß dem Risiko für die Rechte und Freiheiten ausgewählten Maßnahmen (siehe vor allem Art. 24 Abs. 1 und 2, Art. 32 DSGVO) so gewählt, umgesetzt, dokumentiert und auf Wirksamkeit überprüft werden, dass sie jederzeit umfassend und schnell – etwa im Rahmen einer Datenschutzprüfung – dargelegt werden können.

Die Datenschutz-Grundverordnung enthält zudem weitere, bisher in dieser Form oder Ausführlichkeit nicht vorhandene und zum Teil mit Fristen versehene Pflichten, die vor allem auch im Krankenhausbereich einen strukturierten und effizienten Umgang mit dem Thema Datenschutz erfordern. Dies betrifft insbesondere die Pflicht zur Meldung von Datenschutzverletzungen an die Aufsichtsbehörden (Art. 33, 34 DSGVO), die bisher auf Fälle mit drohenden schwerwiegenden Beeinträchtigungen begrenzt war. Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) war bisher überhaupt nicht vorgesehen.

Öffentliche wie private Krankenhäuser sollten deshalb ein Datenschutzmanagement einrichten, aus dem heraus alle Fragen des Datenschutzes schnell und umfassend behandelt werden können.

[1] abrufbar unter https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“

Bestandteile eines Datenschutzmanagements in Krankenhäusern

1. Festlegung eines Teams für das Datenschutzmanagement; Allgemeine Dienstanweisung zum Datenschutz

Die aus der Datenschutz-Grundverordnung resultierenden Aufgaben des Verantwortlichen sind krankenhausintern zunächst Sache der Leitungsebene, die hierbei von dem Datenschutzbeauftragten des Krankenhauses unterstützt wird. Natürlich kann die Krankenhausleitung Aufgaben delegieren. Sie sollte somit für das Datenschutzmanagement einen festen Kreis von Personen definieren, der unter Beteiligung des Datenschutzbeauftragten für die Sicherstellung bzw. Umsetzung der datenschutzrechtlichen Anforderungen zuständig ist. Dieser Personenkreis sollte Mitglieder der jeweiligen Fachabteilungen (IT, Informationssicherheit, Beschwerdemanagement, Qualitätssicherung/Controlling, Vertreter des medizinischen Bereichs) umfassen und im gesamten Haus bekannt sein. Zudem müssen jeweils Vertretungen sichergestellt sein, damit eine Einhaltung der Fristen der Datenschutz-Grundverordnung jederzeit gewährleistet ist.

In einer allgemeinen Dienstanweisung zum Datenschutz sollte festgelegt werden, welche Stellen oder Personen innerhalb des Krankenhauses für welche Aufgaben, die dem Verantwortlichen nach der Datenschutz-Grundverordnung obliegen, zuständig sind. Dies gilt insbesondere für die nachfolgend genannten Themen. Die Dienstanweisung sollte zudem die zur ordnungsgemäßen Erfüllung dieser Aufgaben notwendigen Arbeitsabläufe und Informationsströme regeln und deutlich machen, dass Datenschutz auch die Aufgabe jedes einzelnen Beschäftigten ist.

2. Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO

Dieses Verzeichnis löst das bisherige Verfahrensverzeichnis ab und ist zukünftig durch den Verantwortlichen zu führen. Es bietet sich beispielsweise an, diese Aufgabe dem Team für das Datenschutzmanagement zu übertragen. Ein Musterformular hierfür findet sich in den Datenschutzreform-Arbeitshilfen des Bayerischen

Staatsministeriums des Innern, für Bau und Verkehr[2], sowie – einschließlich umfangreicher Hinweise – auf der Homepage des Bayerischen Landesamts für Datenschutzaufsicht[3].

Das Verzeichnis von Verarbeitungstätigkeiten ist eine zentrale Ausprägung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Viele der in dieses Verzeichnis aufzunehmenden Angaben werden auch für die Erfüllung der Betroffenenrechte benötigt. Es bietet sich an, zu den einzelnen Verarbeitungstätigkeiten weitere sinnvolle Angaben aufzunehmen, die über den Mindestkatalog des Art. 30 Abs. 1 Satz 2 DSGVO hinausgehen (beispielsweise die Rechtsgrundlage oder die Feststellung, ob für die Verarbeitung eine Datenschutz-Folgenabschätzung durchgeführt werden muss).

Das Verarbeitungsverzeichnis ist aktuell zu halten. Es muss sichergestellt sein, dass die Stelle, die das Verzeichnis führt, zeitnah erfährt, wenn bereits in das Verzeichnis aufgenommene Verarbeitungstätigkeiten geändert oder neue, für das Verzeichnis relevante Verarbeitungstätigkeiten durchgeführt werden.

3. Auflistung der vorhandenen Datenschutzkonzepte für Verfahren

Soweit bereits Datenschutzkonzepte für einzelne Verfahren vorhanden sind, sollten diese ebenfalls beim Datenschutzmanagement hinterlegt werden.

4. Auflistung aller Verträge zur Auftragsverarbeitung

Der Verantwortliche sollte in der Lage sein, jederzeit Auskunft über alle Auftragsverarbeitungen zu geben. Es empfiehlt sich daher, eine Auflistung der vorhandenen Verträge zentral beim Datenschutzmanagement-Team zu hinterlegen.

---

[2] abrufbar unter
http://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php

[3] abrufbar unter https://www.lda.bayern.de/de/infoblaetter.html

5. Ergebnisse von durchgeführten Risikoabschätzungen, ergriffene Maßnahmen

Die Datenschutz-Grundverordnung sieht für technische Verfahren einen risikobasierten Ansatz vor, bei dem die Risiken für natürliche Personen (wie beispielsweise die Patienten) zu betrachten sind. Die Abschätzung, ob die Datenverarbeitung wahrscheinlich zu einem hohen Risiko führt, ist zudem die Basis für die Entscheidung über die Durchführung einer Datenschutz-Folgenabschätzung (siehe WP 248 der Art. 29-Gruppe[4]).

Hierfür muss zunächst festgelegt werden, mit welcher Methode eine Einschätzung der Risiken getroffen wird. Die Ergebnisse und Einschätzungen sowie die ergriffenen Maßnahmen sollten sodann dokumentiert werden, da nur so eine Nachweisbarkeit erreicht werden kann. Zudem muss die Risikobewertung regelmäßig überprüft werden, da sich Risiken ändern können. Das Datenschutzmanagement sollte daher entsprechende Fristen vorsehen und überwachen.

6. Auflistung durchgeführter Datenschutz-Folgenabschätzungen

Nach derzeitigem Stand ist davon auszugehen, dass die Krankenhäuser zukünftig für einige ihrer Verfahren zur Verarbeitung personenbezogener medizinischer Daten grundsätzlich eine Datenschutz-Folgenabschätzung durchführen müssen. Der große Unterschied zwischen der Datenschutz-Folgenabschätzung und den auch sonst zu ergreifenden Maßnahmen liegt in dem höheren Detaillierungsgrad und der Systematik der Risikobestimmung sowie der Überprüfung der Wirksamkeit der Risikoeindämmung. Alle Schritte sowie Ergebnisse einer Datenschutz-Folgenabschätzung sollten daher dokumentiert werden, ebenso die Entscheidung, ob eine vorherige Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO erforderlich ist, wann diese gegebenenfalls erfolgt ist und mit welchem Ergebnis.

[4] abrufbar unter http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Für die Durchführung einer Datenschutz-Folgenabschätzung wird ein Team aus mehreren Personen nötig sein. Der Datenschutzbeauftragte des Krankenhauses ist zwar nach Art. 35 Abs. 2 DSGVO an der Datenschutz-Folgenabschätzung zu beteiligen; es ist jedoch nicht seine Aufgabe, diese durchzuführen. Es bietet sich an, die Datenschutz-Folgenabschätzung vom Datenschutzmanagement-Team unter Beteiligung der betroffenen medizinischen Fachabteilungen durchführen zu lassen.

7. Behandlung von Datenschutzverletzungen

Die Datenschutz-Grundverordnung sieht in Art. 33 für den Verantwortlichen die Pflicht vor, eine Verletzung des Schutzes personenbezogener Daten (zum Begriff vgl. Art. 4 Nr. 12 DSGVO) unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde zu melden. Hiervon kann nur abgesehen werden, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies dürfte nur selten der Fall sein.

Diese Pflicht kann nur erfüllt werden, wenn Datenschutzverletzungen im Haus bekannt werden und entsprechende Meldewege und Ansprechpartner existieren. So muss beispielsweise sichergestellt sein, dass Beschwerden von Patienten auch dahingehend geprüft werden, ob eine Datenschutzverletzung vorliegt. Zudem sind Rückmeldungen aus der IT-Abteilung zu Angriffen und proaktive Maßnahmen wie eine Auswertung der Protokollierung im KIS erforderlich.

Alle Datenschutzverletzungen und (um ein weiteres Auftreten zu verhindern) ihre Behandlung müssen entsprechend dokumentiert werden (Art. 33 Abs. 5 DSGVO). Es muss außerdem eine Person oder Organisationseinheit definiert werden, die für die Meldung an die Aufsichtsbehörde und gegebenenfalls – unter den Voraussetzungen des Art. 34 DSGVO – für die Benachrichtigung der betroffenen Person zuständig ist.

8. Betroffenenrechte

Die Art. 13 ff. DSGVO normieren eine Reihe von Rechten betroffener Personen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten. Als Verantwortlicher ist das Krankenhaus verpflichtet, diese Rechte zu erfüllen. Dabei sind auch die form- und verfahrensbezogenen Vorgaben des Art. 12 DSGVO zu beachten.

Art. 13 f. DSGVO regeln umfassende Informationspflichten bei der Erhebung personenbezogener Daten. Diesbezüglich ist festzulegen, auf welche Weise diesen Pflichten nachgekommen wird. Neben den bisher schon bestehenden Einsichtsrechten in medizinische Akten sieht Art. 15 DSGVO ein Auskunftsrecht für die betroffene Person vor. Es sollte daher geregelt sein, wer die Auskünfte erteilt und wie die Vollständigkeit der Unterlagen (Papierakten, elektronische Akten, Protokollierung etc.) sowie die fristgerechte Auskunft sichergestellt werden. Das Team für das Datenschutzmanagement sollte entweder diese Auskünfte selbst erteilen oder in jedem Fall beteiligt werden. Die Bearbeitung des Auskunftsersuchens sollte dokumentiert werden.

Auch hinsichtlich der weiteren Betroffenenrechte – wie etwa dem Recht auf Berichtigung (Art. 16 DSGVO) oder Löschung (Art. 17 DSGVO) personenbezogener Daten – sind entsprechende Verfahrensweisen und Zuständigkeiten festzulegen.

9. Dokumentation von Zertifizierungen, Nachweis der Sicherheit

Zukünftig soll es auch möglich sein, den Nachweis, dass eine Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung erfolgt, über Zertifizierungen zu führen (Art. 42 und 43 DSGVO). Wurden Zertifizierungen durchgeführt oder werden zertifizierte Produkte/Verfahren eingesetzt, so sollte dies entsprechend dokumentiert werden. Auch hier sollte eine schnelle und umfassende Auskunft jederzeit möglich sein.