Merkblatt zur Verpflichtung auf das Datengeheimnis

Das Grundrecht auf informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung ist aus Art. 1 Abs. 1 und Art. 2 Abs. 1 des Grundgesetzes abgeleitet und in Art. 1oo und Art. 1o1 der Verfassung des Freistaats Bayern ausdrücklich verankert. Es beinhaltet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Dieses Recht ist jedoch nicht unbeschränkt. Es findet seine Grenzen in den Rechten Dritter und in den überwiegenden Interessen der Allgemeinheit.

Was folgt daraus für die öffentliche Verwaltung?

Jede Verarbeitung personenbezogener Daten durch einen Mitarbeiter einer öffentlichen Stelle ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung und darf nur auf der Basis einer Rechtsvorschrift oder mit Einwilligung des Betroffenen erfolgen. Der Mitarbeiter muss deshalb, bevor er Daten verarbeitet (z. B. erhebt, speichert, übermittelt oder nutzt) immer prüfen, aufgrund welcher Rechtsnorm er handelt. In Frage kommen bereichsspezifische Vorschriften, wie das Telekommunikationsgesetz, das Telemediengesetz, die Berufsordnung für die Ärzte Bayerns, das Bayerische Personalvertretungsgesetz oder das Bayerische Krankenhausgesetz, und die allgemeinen Bestimmungen der Datenschutzgrundverordnung, des Bayerischen Datenschutzgesetzes neu, des Bundesdatenschutzgesetzes neu und des Strafgesetzbuches. Der Einzelne hat einen Anspruch darauf, dass die öffentlichen Stellen des Freistaats mit seinen personenbezogenen Daten sorgsam umgehen.

Was beinhaltet das Bayerische Datenschutzgesetz neu?

Das Bayerische Datenschutzgesetz neu regelt in Verbindung mit der Datenschutzgrundverordnung die Verarbeitung personenbezogener Daten durch öffentliche Stellen, unabhängig davon, in welcher Form (Dateien oder Akten) sie gespeichert sind und ob es sich um automatisierte oder nicht-automatisierte Verfahren handelt. Das Datenschutzgesetz ist ein Auffanggesetz, das heißt, seine Vorschriften sind immer dann anzuwenden, wenn die konkrete Datenverarbeitung nicht durch eine bereichsspezifische Rechtsvorschrift geregelt ist. Jede darüberhinausgehende Verarbeitung personenbezogener Daten ist unzulässig, es sei denn, der Betroffene hat eingewilligt.

Wer kontrolliert die Einhaltung der datenschutzrechtlichen Vorschriften?

Öffentliche Stellen sind verpflichtet, einen behördlichen Datenschutzbeauftragten zu bestellen. Dieser berät in allen Datenschutzfragen und kontrolliert die Einhaltung der datenschutzrechtlichen Bestimmungen. Vor der Einrichtung oder wesentlichen Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten prüft er, ob die Datenverarbeitung zulässig ist und die Maßnahmen zum Schutz der Daten ausreichend sind. Die verantwortliche Stelle führt ein Verzeichnis der Verarbeitungstätigkeiten aller bei der öffentlichen Stelle eingesetzten Verfahren (Art. 3o DSGVO). Unabhängig von der Tätigkeit der behördlichen Datenschutzbeauftragten kontrolliert der Bayerische Landesbeauftragte für den Datenschutz alle öffentlichen Stellen in seiner Rolle als zuständige Aufsichtsbehörde.

Mitarbeiter einer öffentlichen Stelle können sich in allen Angelegenheiten des Datenschutzes ohne Einhaltung des Dienstweges an den behördlichen Datenschutzbeauftragten und/oder an den Bayerischen Landesbeauftragten für den Datenschutz wenden.

Welche Pflichten hat der Datenschutzbeauftragte?

Die Verarbeitung personenbezogener Daten ist auf das zur rechtmäßigen Aufgabenerfüllung erforderliche Maß zu beschränken. Unrichtige, unzulässig erhobene oder gespeicherte sowie nicht mehr erforderliche Daten sind von Amts wegen zu berichtigen bzw. zu löschen. Die Daten verarbeitenden Stellen sind ferner verpflichtet, sich gegenseitig zu unterrichten, wenn unrichtige oder unzulässig erhobene oder unzulässig gespeicherte personenbezogene Daten berichtigt, gesperrt oder gelöscht wurden. Der Datenschutzbeauftragte muss in Koordination mit den dafür zuständigen Stellen außerdem geeignete technische und organisatorische Maßnahmen treffen, um die Einhaltung der Datenschutzvorschriften sicherzustellen. Sie hat unter anderem eine Beschreibung für jedes von ihr eingesetzte

Verfahren in der Datenverarbeitung zu erstellen. Der behördliche Datenschutzbeauftragte kann die Einrichtung oder wesentliche Änderung eines automatisierten Verfahrens formal freigeben, sofern der Verantwortliche dies festlegt.

Der Datenschutzbeauftragte hat auch umfangreiche Aufklärungspflichten gegenüber dem Betroffenen. Sofern Daten beim Betroffenen mit seiner Kenntnis erhoben werden, ist er unter anderem in geeigneter Weise über den Zweck der Erhebung, die Art und den Umfang der Verarbeitung, etwaige Datenempfänger sowie bestehende Auskunfts- oder Berichtigungsansprüche zu informieren. Dabei ist auch auf bestehende Rechtsvorschriften sowie die Freiwilligkeit von Auskünften hinzuweisen und über mögliche Folgen von Auskunft-verweigerungen aufzuklären. Werden die Daten nicht beim Betroffenen erhoben, so hat die öffentliche Stelle ihn hierüber nachträglich zu unterrichten.

Wer ist bei der „Datenverarbeitung“ beschäftigt?

Bei der Datenverarbeitung sind alle Personen beschäftigt, deren Aufgabengebiet sie regelmäßig mit personenbezogenen Daten, im Krankenhausbereich sind dies insbesondere Patientendaten, in Verbindung bringen.

Was sind Patientendaten?

Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus Kliniken oder Abteilungen des Krankenhauses. Außer den in automatisierten Verfahren gespeicherten oder in Akten aufgezeichneten Angaben gehören auch die auf andere Weise festgehaltenen Informationen über den Betroffenen zu den Patientendaten, wie

- Röntgenaufnahmen
- Grafische Aufzeichnungen, wie EKG, Blut- und Gewebeproben
- Diagnose
- Therapien
- Pflegerische Maßnahmen
- Abrechnungsrelevante Sachverhalte, wie Pflegeklasse, Kostenträger.
- Gemäß DSGVO auch genetische und biometrische Daten.

Auch auf mündlichem Wege erlangte und nicht ausgezeichnete Kenntnisse über persönliche oder sachliche Verhältnisse sind Patientendaten. Patientendaten sind auch die personenbezogenen Daten von Angehörigen und anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden. Bereits der Aufenthalt eines Patienten im Krankenhaus stellt ein schutzwürdiges Patientendatum dar.

Welche Datenschutzvorschriften sind beim Umgang mit Patientendaten zu beachten?

Im Krankenhaus dürfen Patientendaten nur erhoben (beschafft), verarbeitet (erfasst, aufgenommen, aufbewahrt, verändert) oder sonst genutzt werden, soweit die DSGVO i. V. m. Art. 27 Bayerisches Krankenhausgesetz (BayKrG) dies erlaubt oder der Patient eingewilligt hat. Ohne die Einwilligung des Patienten dürfen seine Daten nur in den Fällen des Art. 27 BayKrG an Personen oder Stellen außerhalb des Krankenhauses übermittelt (weitergegeben, mitgeteilt) werden.

Mit der Einwilligung dürfen die gesetzlichen Erlaubnisgründe für die Verarbeitung, sonstige Nutzung und Übermittlung von Patientendaten nicht beliebig erweitert werden. Die Einwilligung bedarf der Schriftform, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist. Die Einwilligung des Patienten als Alternative zu den sonstigen Erlaubnistatbeständen hat Ausnahmecharakter und kann nur in Betracht kommen, wenn der Patient eine echte Entscheidungs- und Wahlfreiheit hat, die größtenteils nicht gegeben ist, da / wenn er sich in einer Situation befindet, die an die Stelle der Freiwilligkeit eine „Scheinfreiwilligkeit“ treten lässt.

Dürfen medizinische Daten für Forschungszwecke verwendet werden?

Im Rahmen von Forschungsvorhaben dürfen Ärzte für eigene wissenschaftliche Forschungsvorhaben mit personenbezogenen Patientendaten nur arbeiten, wenn dies zur Erreichung des Forschungsziels unabdingbar notwendig ist. Sobald der Forschungszweck es erlaubt, sind die personenbezogenen Daten zu anonymisieren. Eine Übermittlung von Patientendaten an Dritte und eine Verarbeitung oder sonstige Nutzung sind nur zulässig, soweit der Patient eingewilligt hat. Die übermittelnde Stelle hat den Empfänger, die Art der zu übermittelnden Daten, die betroffenen Patienten und das Forschungsvorhaben aufzuzeichnen.

Datenschutz ist mehr als nur Verschwiegenheit!

Eine besondere Form des „Datenschutzes" ist die ärztliche Schweigepflicht der Ärzte und des medizinischen Personals. Sie schützt das Patientengeheimnis und gilt zusätzlich zu den übrigen Datenschutzvorschriften. Die unbefugte Offenbarung des Patientengeheimnisses kann nach §2o3 Strafgesetzbuch geahndet werden.

Wann ist die Offenbarung des Patientengeheimnisses befugt, wann ist sie unbefugt?

Das Patientengeheimnis wird unbefugt offenbart, wenn es ohne Zustimmung des Patienten oder ohne ein anderes Recht zur Mitteilung in irgendeiner Weise an einen anderen (Dritten) gelangt. Dabei ist es gleichgültig, ob der Dritte seinerseits zur Verschwiegenheit verpflichtet ist oder ob es sich um einen Angehörigen des Patienten handelt. Dritte in diesem Sinne sind nicht an der Behandlung eines Patienten im Krankenhaus beteiligte Ärzte und deren Hilfspersonal sowie die z. B. mit der Patientenverwaltung betrauten, die im Rahmen der Datenverarbeitung tätigen Personen, der so genannten „zum Wissen berufene Personenkreis".

Das Patientengeheimnis wird befugt offenbart, wenn der Patient die betreffenden Personen von der Schweigepflicht entbunden hat. Dies hat in der Regel schriftlich zu erfolgen. Ohne eine Entbindung von der Schweigepflicht ist die Offenbarung nur befugt (und damit straffrei), wenn in einem Gesetz die Mitteilung vorgeschrieben ist (z.B. Infektionsschutzgesetz) oder unter bestimmten Voraussetzungen (z.B. BayKrG) zugelassen ist.

Welche Rechte hat der Betroffene?

Um sein Recht auf informationelle Selbstbestimmung wahrnehmen zu können, muss der Betroffene wissen, welche Stellen Daten über ihn gespeichert haben und woher diese Daten stammen. Deshalb hat jeder das Recht auf kostenfreie Auskunft über seine Daten, deren Herkunft und Empfänger, also die Personen und Stellen, an die seine personenbezogenen Daten weitergegeben wurden, sowie über Zweck und Rechtsgrundlagen der Verarbeitung. Dem Betroffenen kann statt Auskunft Einsicht in seine Daten (Krankenunterlagen) gewährt werden. Soweit Auskunfts- und Einsichtsansprüche medizinische Daten des Patienten betreffen, darf sie nur der behandelnde Arzt erfüllen.

Er kann sich jederzeit an den Bayerischen Landesbeauftragten für den Datenschutz als Aufsichtsbehörde des Klinikums wenden (Anrufungsrecht) und hat bei Schäden, die aufgrund von Verstößen gegen datenschutzrechtliche Vorschriften eingetreten sind, Anspruch auf Schadensersatz. Er kann eine Berichtigung, unter bestimmten Voraussetzungen auch eine Sperrung seiner Daten verlangen. Darüber hinaus steht einem Betroffenen in Einzelfällen ein Widerspruchsrecht gegen eine sonst zulässige Verarbeitung seiner Daten zu, wenn hierfür ein besonderes Interesse vorliegt, das diese Beschränkung rechtfertigt.

Was geschieht bei einer Verletzung datenschutzrechtlicher Vorschriften?

Verstöße gegen datenschutzrechtliche Vorschriften können als Ordnungswidrigkeit oder als Straftat geahndet werden. Wer beispielsweise gegen die Datenschutzgrundverordnung verstößt, kann in bestimmten Fällen mit einer Geldstrafe von bis zu 4% des Jahresumsatzes bestraft werden.