Foto: Getty Images/ivanastar

Neue Regeln für Datenschutz

Recht Die Europäische Datenschutzgrundverordnung gilt ab 25. Mai 2018 in allen Mitgliedstaaten der Europäischen Union. Die Verordnung wirkt wie ein reguläres nationales Gesetz und ersetzt die bisherigen Gesetze der Mitgliedsstaaten. Gesundheitseinrichtungen müssen sich eingehend mit den neuen Regelungen befassen, denn bei Nichtbeachtung drohen empfindliche Geldbußen.

Von Prof. Hans Böhme

Die Europäische Datenschutzgrundverordnung (DSGVO) betrachtet Datenschutz als ein Grundrecht aller Bürger. Ziel der Verordnung ist es, einen angemessenen Ausgleich zwischen diesem Grundrecht und der Verarbeitung personenbezogener Daten durch Unternehmen sicherzustellen.

Die datenschutzrechtlichen Rechte und Pflichten ergeben sich künftig im Wesentlichen unmittelbar aus der DSGVO, die damit „primäres Datenschutzrecht" ist. Soweit nationale Regelungen den Vorgaben der DSGVO widersprechen, sind diese nicht anzuwenden.

Verantwortliche in Gesundheitseinrichtungen müssen sich eingehend mit den Regelungen der DSGVO auseinandersetzen. Bei Nichtbeachtung drohen nach Art. 83 DSGVO empfindliche Geldbußen bis hin zu 20 Millionen Euro beziehungsweise bis zu vier Prozent des Jahresumsatzes eines Unternehmens.

Die Regelungen im Einzelnen

Datenschutzbeauftragter: Nach Artikel 37 Abs. 1 DSGVO sind öffentliche Stellen verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen.

Für private Gesundheitseinrichtungsträger ergibt sich diese Verpflichtung aus der umfangreichen Verarbeitung von Gesundheitsdaten, die juristisch gesehen zu den besonders sensiblen Daten zählen. Für eine Unternehmensgruppe oder mehrere öffentliche Stellen kann auch ein gemeinsamer Datenschutzbeauftragter bestellt werden. Ein Datenschutzbeauftragter hat zu beraten, zu kontrollieren und darauf hinzuwirken, dass der Datenschutz im Unternehmen eingehalten wird. Er fungiert zudem als Anlaufstelle für die Aufsichtsbehörde und betroffene Personen. Der Datenschutzbeauftragte ist unmittelbar der obersten Managementebene unterstellt und weisungsfrei.

Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht werden.

Die Qualifikation des Beauftragten umfasst Fachwissen auf dem Gebiet des Datenschutzrechtes und der Datenschutzpraxis sowie soziale Fähigkeiten, um die Aufgaben erfüllen zu können. Interessenskonflikte müssen vermieden werden. Das wird zum Beispiel dann angenommen, wenn der Beauftragte in leitender Position in der Geschäftsleitung, in der IT-Abteilung oder in der Personalabteilung tätig ist.

Einwilligung zur Verarbeitung von Gesundheitsdaten: Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung von persönlichen Daten, vor allem von Gesundheitsdaten, grundsätzlich verboten. Gesundheitsdaten sind nach Artikel 4 Nr. 15 DSGVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Es bedarf künftig der ausdrücklichen Einwilligung des Betroffenen nach Art. 9 Abs. 2 a DSGVO in Verbindung mit Art. 6 und 7 DSGVO. Zwar gibt es neben der Einwilligung noch den Weg über eine grundsätzliche datenschutzrechtliche Zulässigkeit der Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 2 h in Verbindung mit Art. 9 Abs. 3 DSGVO und nach § 22 Abs. 1 und 2 BDSG in der neuen Fassung, die am 25. Mai 2018 in Kraft treten (BGBl Teil I Nr. 44, Seiten 2097 ff.). Die Einholung einer rechtskonformen Einwilligung dürfte aber unumgänglich sein. Empfehlenswert ist die schriftliche Einwilligung. Die Einrichtungsleitung wird also die hausinternen Formulare an die neue Rechtslage anpassen müssen.

Gesetzliche Befugnisnorm: Art. 9 Abs. 2 h DSGVO – ähnlich § 22 Abs. 1 Nr. 1 b und c BDSG – erlaubt die Datenverarbeitung, wenn diese unter anderem für die Zwecke der Gesundheitsvorsorge oder für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich ist und dies auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs geschieht. Nach Art. 9 Abs. 3 DSGVO muss die Verarbeitung durch Fachpersonal oder unter dessen Verantwortung erfolgen. Das Fachpersonal muss nach dem Unionsrecht oder dem nationalen Recht dem Berufsgeheimnis oder einer Geheimhaltungspflicht unterliegen. Die Einrichtungsleitung muss einrichtungsintern, gegebenenfalls unter Zuhilfenahme von externer Hilfe, die in der Einrichtung stattfindenden Verarbeitungstätigkeiten definieren und die dazugehörige Befugnisnorm bestimmen.

Verzeichnis der Verarbeitungstätigkeiten: Die Verarbeitungstätigkeiten müssen nach Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten schriftlich, gegebenenfalls in einem elektronischen Format, führen und pflegen. Diese Anforderung gilt für alle Verfahren, unabhängig ob automatisiert oder papiergebunden, mit denen personenbezogene Daten systematisch verarbeitet werden, also exemplarisch auch die Mitarbeiterdaten, Patientendaten und Lieferantendaten.

Dieses Verzeichnis dient damit als Grundlage für die Nachweispflichten gegenüber der Aufsichtsbehörde, für die Auskünfte an Betroffene, für die Information der Betroffenen, für das interne Risikomanagement und ist auch die Grundlage für die Datenschutzfolgeabschätzung (DSFA).

Inhalte des Verzeichnisses sind der Name und die Kontaktdaten des Verantwortlichen, der Zweck der Verarbeitung, die Beschreibung der Daten- und Betroffenenkategorien, die Kategorien von Empfängern, die Übermittlung der Daten in Drittländer, die Fristen für Löschung und die Beschreibung der Sicherheitsmaßnahmen sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Das Verzeichnis ist von zentraler Bedeutung für ein datenschutzkonformes Management in der Gesundheitseinrichtung. Das Verzeichnis hilft den Mitarbeitern der Gesundheitseinrichtung, sich einen Überblick über die Verarbeitungsvorgänge zu verschaffen, was dort mit Daten geschieht, wie es geschieht und ob dies rechtmäßig geschieht.

Datenschutz-Folgeabschätzung: Nach Art. 35 Abs. 1 DSGVO hat insbesondere bei der Verwendung neuer Technologien eine Daten-

schutz-Folgeabschätzung (DSFA) stattzufinden, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Das gilt nach Art. 35 Abs. 3 DSGVO in Verbindung mit Art. 9 DSGVO insbesondere für die Verarbeitung von Gesundheitsdaten.

Die Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge hat vorab stattzufinden. Dabei müssen zunächst eine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der jeweiligen Verarbeitungen erfolgen, um sodann die Schutzmaßnahmen und deren Bewertung darzustellen.

Durch entsprechende Technikgestaltung soll eine Risikominimierung erfolgen. Dazu ist eine Implementierung von IT-Sicherheitsprozessen zur Gewährleistung von Vertraulichkeit, Unversehrtheit und Verfügbarkeit in der Einrichtung vonnöten. Die Einführung eines Berechtigungsmanagements und die Verschlüsselung von Inhalten, zum Beispiel bei E-Mail-Kommunikation, ist erforderlich. Maßnahmen zur Abwehr von Sicherheitsrisiken, beispielsweise Hackerangriffen, und Maßnahmen für eine benutzerfreundliche Technikgestaltung – etwa Zugang, PW-Schutz, Benutzeroberflächen und benutzerfreundliche Geräte – schließen die Maßnahmen ab.

Auftragsverarbeitung: Neue Regelungen gelten auch für den Einsatz externer Dienstleister, sogenannter Auftragsverarbeiter. Nach Art. 4 Abs. 4 Nr. 8 SGVO ist Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Wie bisher muss mit dem Auftragsverarbeiter ein schriftlicher Vertrag über die weisungsgebundene Tätigkeit abgeschlossen werden. Inhaltlich werden die Aufsichtsbehörden ein besonderes Augenmerk auf die Darstellung der erforderlichen Maßnahmen zur Sicherheit der Verarbeitung legen.

Die Gesundheitseinrichtung darf künftig nur noch mit geeigneten Auftragsnehmern arbeiten, die Garantien dafür bieten, dass eine Verarbeitung im Einklang mit den datenschutzrechtlichen Vorgaben der DSGVO gewährleistet ist, um die Rechte der Betroffenen zu gewährleisten. Verträge müssen überprüft und der neuen Rechtslage angepasst werden.

Vorkehrungen für Schutzverletzungen: Art. 33 und 34 DSGVO enthalten erweiterte Meldepflichten bei Verletzungen des Schutzes von personenbezogene Daten an die Aufsichtsbehörde und an die betroffene Person. Aufsichtsbehörden sind bereits dann zu informieren, wenn eine Datenpanne zu einem Risiko für die Rechte und Freiheiten der Betroffenen führen kann. Der Betroffene muss hingegen nur informiert werden, wenn ein hohes Risiko besteht und dieses durch entsprechende technische und organisatorische Maßnahmen nicht abzuwenden ist. Die Meldefristen betragen ganze 72 Stunden. Überdies sind Fakten, Auswirkungen und Abhilfe zu dokumentieren. Die Einrichtungsleitung muss somit ein schnell funktionierendes Meldewesen und die Festlegung der Meldeketten installieren. Ganz wichtig ist dabei die Information der Mitarbeiter, die eine Datenpanne intern zu melden haben. Dazu müssen sie aber zunächst über die Meldepflichten aufgeklärt werden und die zuständigen Ansprechpartner im Betrieb kennen.

Betroffenenrechte: In den Art. 12 bis Art. 22 DSGVO sind die Betroffenenrechte geregelt. Der Betroffene – identifizierte oder identifizierbare natürliche Person nach Art. 4 Nr. 1 DSGVO – hat Anspruch auf eine transparente Darstellung der Verarbeitungsvorgänge in verständlicher Form und auf Erfüllung der bestehenden Informationspflichten über Verarbeitung und Zweck. Neben dem Recht auf Auskunft über die geplante Dauer der Speicherung gehört dazu auch das Recht auf Berichtigung und Löschung („Recht auf Vergessenwerden"). Nach Art. 12 Abs. 3 DSGVO ist die Auskunft unentgeltlich zu erteilen und muss ohne unangemessene Verzögerung innerhalb eines Monats erfolgen. Nach Art. 20 DSGVO ist der Verarbeitende verpflichtet, die zur Verfügung gestellten Daten einem Dritten in einem entsprechenden Format zur Verfügung zu stellen. Damit widersprechen diese Regelungen dem § 630 g BGB, der nur ein Einsichtsrecht und die kostenpflichtige Erstellung von Kopien regelt. Die Einrichtungsleitung muss somit Maßnahmen zum Vorgehen bei Auskunftsrechten der Betroffenen schaffen und auch Möglichkeiten zur Berichtigung bereithalten. Vorgaben für Löschung/Sperrung sowie Möglichkeiten für Einschränkung und Widerspruch sind zu schaffen.

Für klare Regelungen sorgen

Die Einrichtungsleitung hat für klare Regelungen bei den Zuständigkeiten und Verantwortlichkeiten zur Erstellung, Führung, und Aktualisierung dieser Verzeichnisse zu sorgen. Die Mitarbeiter müssen entsprechend geschult werden. Die Einrichtungsleitung hat somit eine besondere Verantwortung bei der Umsetzung der DSGVO. Wenn auch der betriebliche Datenschutzbeauftragte zunächst die Geschäftsleitung zu informieren hat, bleibt die Verantwortung für die Einhaltung der datenschutzrechtlichen Grundlagen bei der Einrichtungsleitung.

Empfehlenswert ist eine strukturierte, projektbezogene Vorgehensweise in Teamarbeit. Im Hinblick auf die vielen bußgeldbewerten Tatbestände ist den Entscheidungsträgern in den Gesundheitseinrichtungen zu empfehlen, sich eingehend mit den Vorgaben der DSGVO auseinanderzusetzen und die erforderlichen Umsetzungsmaßnahmen vorzunehmen.

Prof. Hans Böhme ist Jurist und Soziologe. Er wirkt als Honorarprofessor an der Ernst-Abbe-Hochschule Jena.
Mail: info@boehme-igrp.de