DSGVO – die „Schonzeit“ ist vorbei

Erste Bestandsaufnahme, Erfahrungen und dringende To-dos

Es ist zweifelsfrei richtig, dass die Datenschutzgrundverordnung (DSGVO) insbesondere die Datenkraken ins Visier nehmen wollte. Man wollte Möglichkeiten schaffen, um den Machenschaften von Facebook, Google und Co. begegnen zu können. Aber auch kleinere, weniger digitalisierte Unternehmen rücken in den Fokus der Aufsichtsbehörden. Die Gründe hierfür sind vielfältig; sie mögen darin liegen, dass diese Datenverarbeitungen in Pflegeheimen einfacher zu verstehen sind als jene Datenverarbeitungen von Technologiekonzernen. Im Ergebnis steht jedoch fest, dass die Aufsichtsbehörden auch Pflegeeinrichtungen prüfen werden. Es ist daher notwendig, die Vorgaben der DSGVO umzusetzen. Auf den Punkt gebracht: „Weniger reden, mehr machen!“

Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten und schützt damit die Grundrechte und Grundfreiheiten jeder natürlichen Person. Dieses, in Artikel 1 der DSGVO manifestierte Ziel ist nicht neu.

In Deutschland existiert dieses Grundrecht seit 1983. Damals hatte das Bundesverfassungsgericht mit dem sogenannten „Volkszählungsurteil“ das Recht auf informationelle Selbstbestimmung, also das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen, etabliert.

Insbesondere Pflegeeinrichtungen, – unabhängig davon, ob diese ambulante, teilstationäre oder stationäre Leistungen erbringen – verarbeiten unzählige besondere Kategorien personenbezogener Daten und müssen daher das Recht auf informationelle Selbstbestimmung beachten. Die Betreuung und Pflege eines Menschen setzt voraus, dass die zur Betreuung erforderlichen Informationen über ihn erhoben, in der Pflegedokumentation verarbeitet sowie im Rahmen der Leistungserbringung und -abrechnung an Dritte weitergegeben werden müssen – sei es an einen externen Abrechnungsdienstleister, den Hausarzt oder den Medizinischen Dienst der Krankenkassen.

Umfassende Informationspflicht

Der Beginn einer Datenverarbeitung startet spätestens zu dem Zeitpunkt, zu dem der Bewohner oder Patient in einer Einrichtung aufgenommen wird. Pflegeeinrichtungen sollten ihre Datenschutzinformationen dahingehend prüfen, ob die Vorgaben der DSGVO erfüllt werden.

Konkret muss die betroffene Person verständlich darüber informiert werden, wer die Daten erhebt, wie sie gegebenenfalls den Datenschutzbeauftragten erreichen kann, welche Zwecke inklusive Rechtsgrundlage mit der Datenverarbeitung verfolgt werden und

Johannes Mönter arbeitet in der Unternehmensberatung Curacon im Geschäftsfeld Datenschutz und ist in dieser Funktion dort der Projektleiter.

wer Empfänger der Daten sein kann. Parallel dazu sollten die Pflege- und Behandlungsverträge überprüft werden. Im Kontext der beruflichen Schweigepflicht ist zudem zu prüfen, ob eine wirksame Entbindung eingeholt werden muss bzw. wird.

Unternehmen müssen ein Verzeichnis der Verarbeitungstätigkeiten führen. Dieses muss mindestens die in Artikel 30 DSGVO genannten Kriterien enthalten und stellt eine Übersicht aller im Unternehmen vorhandenen Verfahren (im Sinne von Geschäftsvorfällen bzw. personenbezogener Prozesse) dar. Auf dieser Basis muss eine Risikobewertung der vorhandenen Verfahren durchgeführt werden.

Da die Datenverarbeitung im Bereich des Gesundheitswesens allein aufgrund der Pflicht, für jede betroffene Person eine Pflegedokumentation zu führen, umfangreich ist, ergibt sich die Pflicht, eine Datenschutz-Folgenabschätzung gem. Artikel 35 DSGVO durchzuführen. Einige Datenschutzbehörden haben mittlerweile sogenannte Muss-Listen (Blacklists) entworfen und veröffentlicht, sodass sich ein Blick in diese lohnt.

Das Verzeichnis der Verarbeitungstätigkeiten muss zudem eine Übersicht der technischen und organisatorischen Maßnahmen enthalten, die insbesondere die Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit sicherstellen. Diese Maßnahmen – sowie die zugehörigen Verfahren – sind regelmäßig zu prüfen.

Damit hat der Gesetzgeber das „Plan-Do-Check-Act-Prinzip“ im Datenschutz aufgenommen, sodass es nicht ausreicht, die Datenverarbeitungen einmalig zu erfassen. Pflegeeinrichtungen sind verpflichtet, ihre Datenverarbeitungen regelmäßig zu überprüfen. Hier sei angemerkt, dass dies eine Chance darstellen kann, die internen Prozesse und Verfahren auf den Prüfstand zu stellen und im Sinne der Bewohner/Patienten und Mitarbeiter zu verbessern.

Fotos: ein sehr sensibles Thema

Eine entscheidende Rolle spielt die Rechtsgrundlage, nach welcher Pflegeeinrichtungen personenbezogene Daten erheben dürfen. Die Datenverarbeitung personenbezogener Daten bedarf regelmäßig einer gesetzlichen Grundlage oder einer Einwilligung. Hierbei ist insbesondere auf die Verarbeitung besonderer Kategorien personenbezogener Daten zu achten, da an die Verarbeitung dieser Daten besondere Anforderungen geknüpft sind.

Pflegeeinrichtungen können sich hierbei regelmäßig auf den Zweck zur Durchführung des Behandlungsvertrags oder die Erfüllung einer gesetzlichen Verpflichtung berufen. Für alle sonstigen Datenverarbeitungen, die von keiner gesetzlichen Rechtsgrundlage gestützt werden können, benötigen Pflegeeinrichtungen für den konkreten Zweck eine wirksame Einwilligung.

Insbesondere beim sehr sensiblen Thema Fotos sollten Pflegeeinrichtungen darauf achten, dass für die Verarbeitung – insbesondere für die Veröffentlichung von Fotos auf der Homepage – nach herrschender Meinung die schriftliche Einwilligung des Betroffenen vorliegen muss. Dies ergibt sich aus den Regelungen, welche im Kunsturhebergesetz vorzufinden sind sowie aus der Datenschutzgrundverordnung (Artikel 6 Absatz 1 lit. a, ggf. i. V. m. Artikel 9 Absatz 2 lit. a DSGVO). Wie bei jeder Einwilligung sollte an geeigneter Stelle darauf hingewiesen werden, dass die Erteilung der Einwilligung freiwillig ist, sowie dass diese mit Wirkung für die Zukunft widerrufen werden kann, ohne dass der betroffenen Person dadurch Nachteile entstehen würden.

In Bezug auf die Fotothematik spielt auch die Pflegedokumentation einer Wunde mithilfe von Fotos eine entscheidende Rolle. Werden Fotografien im Rahmen der Pflegedokumentation angefertigt, ist auch hier eine Einwilligung erforderlich. In diesem Zusammenhang ist besonders wichtig, dass die Mitarbeiter in keinem Fall ihr privates Mobiltelefon für die Fotodokumentation nutzen. Die Einwilligung der Betroffenen umfasst nicht die Weitergabe der Fotos in Cloud-Dienste, wie sie auf fast allen Mobilfunkgeräten standardmäßig vorinstalliert sind.

Im Bereich der digitalen Pflegedokumentation ist der Schutz der personenbezogenen Daten zu integrieren, da diese Entwicklung die Datenschutzrisiken für die Betroffenen weiter verschärft. Mit heutiger Technik können sensible Daten auf bestimmte Merkmale hin durchleuchtet und auf definierte Attribute untersucht werden. In diesem Zusammenhang birgt insbesondere die Schnittstelle zwischen analoger und digitaler Welt die größten Risiken.

Daher gilt es, die Dateneingabe nachvollziehbar und sicher zu gestalten sowie durch geeignete technische und organisatorische Maßnahmen vor dem Zugang unbefugter Personen zu schützen. Konkret bedeutet dies zudem, dass Zugriffe auf personenbezogene Daten nachvollziehbar sind und kontrolliert werden können. Ein sogenannter „Station Account“ bietet sich hierfür regelmäßig nicht an, sodass personalisierte Benutzer eingerichtet werden sollten.

Einsichtsrecht in Pflegedokumentation

Ein weiterer Punkt ist das Einsichtsrecht in die Pflegedokumentation. Grundsätzlich hat der Betroffene das Einsichtsrecht in die Dokumentation. Dies stellt eine spezielle Form des allgemeinen Rechts auf Auskunft dar. Konkret bedeutet dies, dass Pflegeeinrichtungen ein Verfahren implementieren sollten, welches sicherstellt, dass das Recht auf Auskunft sowie die weiteren Betroffenenrechte gemäß DSGVO gewährt und zum Beispiel vom Recht auf Akteneinsicht (nach dem Patientenrechtegesetz) unterschieden werden kann.

Das Auskunftsrecht nach DSGVO geht über die Voraussetzungen des Rechts auf Akteneinsicht hinaus. Insbesondere die Identitätsfeststellung muss hier geregelt sein, da die unzulässige Offenlegung an nicht eindeutig identifizierten Betroffenen und dadurch gegebenenfalls unbefugten Dritten negative Folgen nach sich ziehen kann.

Neben dem Auskunftsrecht spielt zunehmend das Recht auf Löschung eine wesentliche Rolle. Hierbei ist dafür Sorge zu tragen, dass Daten, die für das Unternehmen nicht mehr erforderlich sind, gelöscht werden müssen. Ist das Löschen nicht möglich, da beispielsweise gesetzliche Aufbewahrungsfristen dem entgegenstehen, sind die Daten zu sperren. Aus der Tatsache, dass Daten nicht gelöscht werden dürfen, lässt sich daher nicht ableiten, dass diese weiterhin im Unternehmen frei verfügbar sein dürfen.

Im Fokus der Betrachtung stehen außerdem die in den ambulanten Pflegediensten häufig verwendeten Tourenpläne. Die Pläne enthalten

Gesundheitsinformationen. In den meisten Fällen sind dies Informationen zur Hilfebedürftigkeit und Daten mit Hinweisen zur Wohnung der pflegebedürftigen Person. Aber auch Mitarbeiterdaten sind im Rahmen der Tourenpläne vorzufinden. Insbesondere in Bezug auf eine mögliche Mitarbeiterüberwachung sind entsprechende Absprachen mit dem Betriebsrat zu treffen und die personenbezogenen Mitarbeiterdaten zu schützen. Konkret ergibt sich hieraus, dass auch Tourenpläne – unabhängig ob diese digital auf dem Smartphone oder analog auf Papier geführt werden – vor dem Zugriff und der Einsichtnahme unbefugter Dritter geschützt werden müssen.

In der Praxis haben sich zudem weitere Fallstricke gezeigt. Diese reichen zum Beispiel von der Nutzung bestimmter Messenger-Dienste über Social-Media-Kanäle bis hin zur Einhaltung der Privatsphäre am Empfang von Pflegeeinrichtungen.

Überprüfung der Auftragsverarbeitungen

Eines der größten Probleme stellt der Messenger-Dienst WhatsApp dar, der in vielfältiger Weise die Vorgaben des geltenden Datenschutzrechts verletzt. So werden unter anderem Daten in einem Drittland gespeichert und an die Konzernmutter Facebook weitergegeben, mit dem Ziel, Nutzerprofile zu erstellen. Da WhatsApp von vielen Verantwortlichen und Mitarbeitern nicht nur in Pflegeeinrichtungen als eine unkomplizierte Plattform zur Kommunikation genutzt wird, scheint ein Verbot der Nutzung in der Praxis nur schwer durchführbar. Helfen kann das Aufzeigen von alternativen Diensten, Unterweisungen, Vorschriften oder Schulungen.

Insbesondere sind folgende Aufgaben für Pflegeeinrichtungen umzusetzen: Datenpannen müssen innerhalb von 72 Stunden nach Kenntnisnahme an die zuständige Aufsichtsbehörde gemeldet werden. Nach bisherigem Recht war der Vorfall „unverzüglich“ zu melden, wobei die Rechtsprechung einen Zeitraum von zwei Wochen als Obergrenze für unverzügliches Handeln noch als angemessen erachtet hat.

Eine Meldung kann lediglich unterbleiben, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für den Betroffenen führen wird. In der Gesundheitsbranche ist dieses Risiko jedoch regelmäßig gegeben, sodass der Ausnahmetatbestand sich lediglich auf Informationen über die Teilnahme an „öffentlichen“ Veranstaltungen oder ähnlicher Daten begrenzen dürfte.

Eine weitere wesentliche Maßnahme ist die Überprüfung der Auftragsverarbeitungen. Auftragsverarbeitungen liegen vor, sofern externe Dritte personenbezogene Daten der Pflegeeinrichtung im Auftrag dieser verarbeiten.

Dies ist zum Beispiel der Fall bei der Verwendung von Softwarelösungen für die Dokumentation, bei der Lohnabrechnung durch einen Dienstleister, der Wartung sogenannter Multifunktionsgeräte oder der Hinzuziehung eines Letter-Shops. Ebenfalls sollte in diesem Kontext berücksichtigt werden, dass „Konzerntöchter“ ebenfalls als Auftragsverarbeiter klassifiziert werden könnten.

Fazit: Die „Schonzeit“ ist vorbei. Umso deutlicher wird dies, wenn man die Nachrichten der vergangenen Wochen und Monate liest. Einem Bericht des Handelsblatts zufolge wurden bundesweit bereits 42 Bußgeldbescheide verschickt (vgl. Handelsblatt online, 18. Januar 2019: *https://www.handelsblatt.com/23872806.html?share=mail);* Tendenz steigend.

Unternehmen, welche sich bisher nicht oder nur nebenbei mit der Umsetzung der DSGVO beschäftigt haben, dürften mittelfristig Probleme bekommen. Zum einen, weil die betroffenen Personen oder ihre Angehörigen immer häufiger von ihren Rechten Gebrauch machen – zum anderen, weil die strukturierte Umsetzung der gesetzlich geforderten Maßnahmen personelle sowie zeitliche Ressourcen erfordert, die in den wenigsten Fällen vorhanden oder bestenfalls geplant sind. ◆

Johannes Mönter, Curacon GmbH