Ein Jahr DSGVO

Was ist noch zu tun?

Die DSGVO ist seit 25. Mai 2018 in Kraft. Im Vorfeld gab es viel Unsicherheit bezüglich der Umsetzung und der bevorstehenden Strafen. Inzwischen führen die Datenschutzbehörden ihre Arbeit verstärkt fort und die Rechtsprechung ist in Bewegung. Ein Datenschutzbeauftragter steht Rede und Antwort.

Auf der TheraPro 2019 in Stuttgart referierte Markus Sobau, Geschäftsführer MEDIsecur/Confina, zum Thema und berichtete von einem ersten Fall. Das Unternehmen ist spezialisiert auf Leistungserbringer im Gesundheitswesen und bietet fachliche Expertise durch gelistete Datenschutzauditoren. **THERA-BIZ** nahm auf der therapie Leipzig die Gelegenheit wahr nachzufragen und unterhielt sich mit Markus Sobau.

THERA-BIZ: Herr Sobau, wie ist die Lage?

Markus Sobau: Seit Gültigkeit der DSGVO im Mai 2018 wurde viel berichtet. Fakt ist, dass mit der DSGVO in verschiedenen Bereichen eine klare gesetzliche Regelung zum Schutz der persönlichen Daten Gültigkeit bekommen hat. Aus dem Alltag kenne ich persönlich leider schon die ersten Fälle, bei denen Abmahnungen erteilt wurden. Uns liegen die ersten Anfragen von Praxisinhabern vor, bei denen die Landesdatenschutzbehörden konkreten Hinweisen von Datenschutzverletzungen nachgehen mussten. Beispielsweise wurden in Bayern beim Versand eines E-Mail-Newsletters die persönlichen E-Mail-Adressen in Umlauf gebracht. Die Fogle: Im November 2018 wurde ein Bußgeld in Höhe von 20.000 Euro verhängt. Jeder Praxisinhaber haftet persönlich als Verantwortlicher für den Datenschutz.

THERA-BIZ: Gilt die DSGVO auch, wenn die Daten in Papierform erfasst werden und keine Rechner im Einsatz sind?
Markus Sobau: Die Datenschutzgrundverordnung besagt in Art. 4, dass es egal ist, ob mit oder ohne Hilfe automatisierter

Verfahren oder technischer Möglichkeiten Daten erfasst und verarbeitet werden. Grundsätzlich sind Vorgänge wie das Erfassen und Erheben von personenbezogenen Daten, die Organisation, das Ordnen und Verändern von der DSGVO betroffen. Man kann sagen, dass jede Art personenbezogene Daten zu sammeln, unabhängig davon, ob diese zentral, dezentral, technisch oder in Papierform erfolgt, betroffen ist.

THERA-BIZ: Viele lassen sich eine Einverständniserklärung von Patienten unterschreiben. Reicht das?
Markus Sobau: Das ist lediglich einer von acht bis zehn der wichtigsten Bereiche, welche die DSGVO regelt. Mindestens genauso relevant ist ein Verzeichnis der Verarbeitungstätigkeiten – im Prinzip eine Art Handbuch, in dem alle Datenverarbeitungsvorgänge beschrieben sind. Außerdem die sogenannten technischen und organisatorischen Maßnahmen zum Datenschutz (TOM). Dies reicht von abschließbaren Schränken über geschützte Kalender und Karteikarten bis hin zur Zutrittskontrolle einer Praxis oder die Einsehbarkeit von Computermonitoren oder Faxgeräten. Zudem sind mit sämtlichen externen Dienstleistern, die Daten erhalten oder einsehen können, sogenannte Auftragsverarbeitungsverträge zu schließen. In diesen Vereinbarungen werden externe Dienstleister oder Partner, die Daten erhalten, zur gleichen Einhaltung des Datenschutzes verpflichtet und die Haftung an diese übergeben. Selbstverständlich sind alle Patienten über ihre Rechte schriftlich zu informieren. Die Patienteninformation sollte unbedingt Widerrufserklärungen beinhalten und genau beschreiben, wie und wo ein Patient Auskunft über die gespeicherten Daten erhalten kann.
Was ebenfalls sehr wichtig ist, ist das Recht eines jeden Patienten auf Löschung seiner Daten. Das Gesetz spricht hier von einem sogenannten „Recht auf Vergessenwerden“. In diesem Fall ist dann abzuwägen, ob es steuerliche oder medizinische Vorschriften oder Auflagen gibt, die dieser Löschung entgegenstehen. Dies muss dann mit dem betroffenen Patienten besprochen und dokumentiert werden.

THERA-BIZ: Als besonders sensibel gilt der technische Datenschutz.
Markus Sobau: Ja, in den Bereich des technischen Datenschutzes gehören Homepage, Server, Verwaltungs- und Abrechnungssoftware und selbstverständlich auch E-Mail-Verschlüsselung. All das sollte überprüft werden, ähnlich wie beim Auto der regelmäßige TÜV-Termin. Ein neutraler Experte schaut sich den aktuellen Status quo an und stellt eventuell Mängel fest. Die Mängelliste muss dann mit dem bisherigen Dienstleister abgearbeitet werden.

THERA-BIZ: Ab wann ist wirklich ein Datenschutzbeauftragter nötig?
Markus Sobau: Der Sachverhalt ist relativ einfach: Praxen bis zu neun Mitarbeitern brauchen keinen Datenschutzbeauftragten, wobei hier von den Mitarbeitern nur diejenigen gemeint sind, die mit Patientendaten zu tun haben. Trotzdem empfehlen die Landesdatenschutzbehörden – wenigstens für die Anfangszeit –, einen externen Datenschutzbeauftragten zu engagieren, um alle Vorgaben umzusetzen und die Praxis quasi so zu qualifizieren und anzuleiten, dass sie die DSGVO erfüllt.
Sind in einer Therapieeinrichtung mehr als 9 Mitarbeiter mit den Patientendaten betraut, ist ein Datenschutzbeauftragter zu bestellen. Er muss bei der Landesdatenschutzbehörde gemeldet werden und ist die erste Anlaufstelle für Patienten, die sich über den Datenschutz informieren möchten.
Zusätzlich ist zwischen internen und externen Datenschutzbeauftragten zu unterscheiden. Bei internen Datenschutzbeauftragten wird ein Mitarbeiter – und dies darf nicht der Inhaber oder ein Verwandter des Inhabers sein – bestellt und fortan ist diese Person für für den Datenschutz innerhalb der Praxis zuständig. Diese Person muss, sofern ihr noch das Wissen fehlt, qualifiziert und fortgebildet werden, um die Aufgabe erfüllen zu können. Die Alternative ist ein externer Datenschutzbeauftragter, der sofort fachkompetent zur Verfügung steht und persönlich die Haftung für die Einhaltung der Datenschutzrichtlinie übernimmt. Für Praxisinhaber, die ihre Haftung reduzieren wollen, ist dies der einfachste Weg, um dies zu erreichen.
Wichtig ist, dass jede Praxis, jede Einrichtung auf jeden Fall verpflichtet ist, die DSGVO mit allen Vorgaben einzuhalten, denn das Gesetz gilt für alle Praxen.

THERA-BIZ: Welche Kosten kommen für die Umsetzung auf Praxisinhaber zu?
Markus Sobau: Je nach Praxisgröße und Aufwand können die Kosten zwischen 1.000 bis 3.000 Euro für den einmaligen DSGVO-Check anfallen. Größere Einrichtungen könnten teurer werden. Neben den einmaligen Kosten für die Umsetzung sind laufende Gebühren oder Kosten, wie in einem Update-Vertrag oder Servicevertrag in Höhe von 100 bis 400 Euro monatlich zu kalkulieren. Man kann die Kosten senken, indem Praxisinhaber oder interne Datenschutzbeauftragte mehr Aufgaben in Eigenregie übernehmen. So sind die Kosten um circa die Hälfte zu senken.
Vielen Dank für das Gespräch.

Das Interview führte Reinhild Karasek.