Datenschutz-Grundverordnung

Bestellung eines Datenschutzbeauftragten und dessen Aufgaben

Am 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in Kraft getreten, die unmittelbare Geltung in den EU-Mitgliedstaaten beansprucht und das bisherige nationale Datenschutzrecht weitgehend – wenn auch nicht vollständig – ersetzt. Ziel dieser Veröffentlichung ist es, einen Überblick darüber zu geben, wie die rechtliche Bewertung hinsichtlich der Notwendigkeit der Bestellung eines Datenschutzbeauftragten (DSB) in der Arztpraxis ist und welche Aufgaben mit dieser Funktion verbunden sind. Zum Teil weisen die geltenden Regelungen Interpretationsspielräume auf, die noch nicht abschließend geklärt sind.

In den Fällen, die Artikel 37 DSGVO aufführt, besteht in allen Mitgliedstaaten die Pflicht, einen Datenschutzbeauftragten zu benennen. Die Mitgliedstaaten haben daneben allerdings auch die Möglichkeit, diese Pflicht zur Benennung eines Datenschutzbeauftragten auf weitere Fälle auszudehnen. Diese hat der nationale Gesetzgeber im § 38 Bundesdatenschutzgesetz (BDSG – neu) genutzt.

Benennung des Datenschutzbeauftragten nach Art. 37 DSGVO

Gemäß der dort genannten Kategorien wäre für die Arztpraxis ein Datenschutzbeauftragter zu bestellen, „wenn die Kerntätigkeit des Verantwortlichen […] in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 [hierzu zählen u. A. genetische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung] … besteht".
Unter Berücksichtigung von Erwägungsgrund (ErwGr.) 97 der DSGVO ist „Kerntätigkeit" die Haupttätigkeit eines Unternehmens, die es untrennbar prägt, und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit beinhaltet. Zu den Kerntätigkeiten gehören danach auch alle Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Verantwortlichen bilden. Nicht erfasst sind die das Kerngeschäft unterstützenden Tätigkeiten.

Zur Beurteilung, ob eine Verarbeitung „umfangreich" ist, sind auf Grundlage von ErwGr. 91 zur DSGVO folgende Beurteilungskriterien heranzuziehen:

- Menge der verarbeiteten personenbezogenen Daten (Volumen),
- Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt),
- Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße) und
- Dauer der Verarbeitung (zeitlicher Aspekt).

Sind mehrere dieser Kriterien hoch, so kann dies für eine „umfangreiche" Verarbeitung sprechen.

Die Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einem Kurzpapier (abrufbar unter www.saechsdsb.de/novellierung-eu-datenschutz) für die Arztpraxis ausgeführt, dass es sich regelmäßig nicht um eine, die Benennungspflicht auslösende umfangreiche Datenverarbeitung handelt, wenn „eine Verarbeitung von Patienten- oder Mandantendaten durch einen einzelnen Arzt …" erfolgt. Aufgegriffen wird hiermit ErwGr. 91 der DSGVO sowie eine Feststellung der sogenannten Artikel-29-Datenschutzgruppe.

Weiter wird ausgeführt, dass „unter Berücksichtigung der Umstände des Einzelfalles und der konkreten Elemente einer umfangreichen Verarbeitung im Sinne des ErwGr. 91 – beispielsweise bei einer Anzahl von Betroffenen, die erheblich über den Betroffenenkreis eines überdurchschnittlichen, durch ErwGr. 91 Satz 4 privilegierten Einzelarztes hinausgeht – eine umfangreiche Verarbeitung gegeben sein kann, sodass ein DSB zu benennen ist." Unklar blieb zunächst, welche Bedeutung in der Praxis dieser Erwägung zukommt.

Benennung eines Datenschutzbeauftragten nach § 38 BDSG-neu

Danach muss ein Datenschutzbeauftragter in folgenden Fällen benannt werden:

- es werden in der Regel mindestens zehn Personen ständig mit der automatischen Verarbeitung personenbezogener Daten beschäftigt oder
- es werden – unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen – Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen.

Eine Datenschutz-Folgenabschätzung ist erforderlich, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Patienten zur Folge hat, bezogen auch auf die Verarbeitung von Gesundheitsdaten.
Die Regelung geht von einem diesbezüglichen Erfordernis beim Einsatz neuer Technologien aus:

- bei systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche sowie
- umfangreicher Verarbeitung von besonderen Kategorien von personenbezogenen Daten gemäß Art. 9 Absatz 1 [DSGVO] .

Hier gelten die oben genannten Grundsätze der besonderen Kategorien personenbezogener Daten sowie der Definition „umfangreich" entsprechend.
Unter Berücksichtigung der Regelungsinhalte von Art. 37 DSGVO und § 38 BDSG-neu wurden die oben bereits aufgezeigten kontrovers diskutierten Fragestellungen zur Bestellpflicht eines Datenschutzbeauftragten in der Arztpraxis durch die Datenschutzbehörden des Bundes und der Länder einer Klärung zugeführt.

Hierzu hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 26. April 2018 einen für Ärzte und andere Angehörige von Gesundheitsberufen geltenden Beschluss gefasst. Das Dokument ist einsehbar unter

www.datenschutz-berlin.de/pdf/publikationen/DSK/2018/2018-DSK-DSB_Bestellpflicht_Arztpraxen.pdf

Aufgaben des Datenschutzbeauftragten

Für die Aufgaben, die ein Datenschutzbeauftragter zu erfüllen hat, macht es keinen Unterschied aufgrund welcher Regelung er bestellt wurde. Vielmehr ergeben sich seine Aufgaben unmittelbar aus der Datenschutz-Grundverordnung. Artikel 38 DSGVO verweist darauf, dass der Datenschutzbeauftragte andere Aufgaben und Pflichten wahrnehmen kann. Allerdings muss der Verantwortliche oder der Auftragsverarbeiter sicherstellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
Die Pflichtaufgaben eines Datenschutzbeauftragten nach der DSGVO lassen sich typischerweise in folgende Punkte unterteilen:

- interne Aufgaben in der Arztpraxis,
- Funktion im Verhältnis zur Aufsichtsbehörde und
- Funktion als Kontakt für betroffene Personen.

Artikel 38 DSGVO fordert die Unterrichtung und Beratung des Verantwortlichen beziehungsweise des Auftragsverarbeiters. Hierzu sind auch die Beschäftigten, die Verarbeitungen im Sinne der Datenschutz-Grundverordnung durchführen, zu zählen. Daneben verlangt die Regelung die Überwachung der Einhaltung der DSGVO anderer Datenschutzvorschriften der Union und der Datenschutzvorschriften der Mitgliedstaaten zum Beispiel des „BDSG-neu". Hierunter wiederum fällt auch die Überwachung, ob der Verantwortliche unternehmensinterne Strategien für den Schutz personenbezogener Daten einhält. Eine interne Aufgabe des Datenschutzbeauftragten, die dieser erst auf Anfrage wahrzunehmen hat, ist die Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung. Gemäß Artikel 39 DSGVO ist der Datenschutzbeauftragte zum einen Kontaktperson für die Aufsichtsbehörde, andererseits zur Zusammenarbeit mit der Aufsichtsbehörde verpflichtet.

Stark betont wird in der DSGVO die Funktion des Datenschutzbeauftragten als Anlaufstelle für Betroffene. So haben betroffene Personen das Recht, den Datenschutzbeauftragten zu sämtlichen Fragestellungen „zu Rate zu ziehen", die mit „der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte" gemäß DSGVO im Zusammenhang stehen. Schließlich sieht Artikel 37 Abs. 7 DSGVO vor, dass der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und diese Daten der Aufsichtsbehörde mitteilt.

Ist ein Datenschutzbeauftragter zu bestellen oder wird ein solcher freiwillig bestellt, kann es sich hierbei um einen Beschäftigten der Arztpraxis (interner DSB) oder eine mittels Dienstleistungsvertrag bestellte Person (externer DSB) handeln.

Voraussetzung ist, dass der Datenschutzbeauftragte aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens in den Bereichen Datenschutzrecht und -praxis sowie seiner Fähigkeiten, die ihm übertragenen Aufgaben erfüllen kann.

Weitere vertiefende Informationen sind in der Veröffentlichung der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis" zu finden: www.bundesaerztekammer.de/richtlinien/empfehlungenstellungnahmen/ beziehungsweise www.kbv.de/html/datensicherheit.php. ■

Ass. jur. Michael Kratz
Datenschutzbeauftragter der
Sächsischen Landesärztekammer