PFLICHT ZUR BENENNUNG EINES DATENSCHUTZBEAUFTRAGTEN UND ZUM FÜHREN EINES VERZEICHNISSES VON VERARBEITUNGSTÄTIGKEITEN IN DER ARZTPRAXIS

Prof. Dr. Thomas Hoeren

I. Einführung

Mit der Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union gilt seit dem 25. Mai 2018 ein neuer Rechtsrahmen für die Verarbeitung von personenbezogenen Daten innerhalb der EU. Zeitgleich hat der deutsche Gesetzgeber die nationale Rechtslage an die neue Verordnung angepasst und von den vorhandenen Öffnungsklauseln Gebrauch gemacht. Zum umfassenden Pflichtenprogramm nach der DS-GVO gehören u. a. die Benennung eines Datenschutzbeauftragten und das Führen eines Verzeichnisses von Verarbeitungstätigkeiten durch datenverarbeitende Stellen.

Die Verarbeitung von Gesundheitsdaten ist aufgrund der sensiblen Informationen über den Patienten besonders risikoreich. Angesichts der drastischen Bußgeldandrohungen durch die DS-GVO stellt sich daher gerade auch für Arztpraxen die Frage, ob sie den oben genannten Pflichten unterfallen. Diese Frage lässt sich aufgrund der vielfältigen Erscheinungsformen von Arztpraxen nicht pauschal beantworten. Zu unterscheiden ist zwischen Einzelpraxen und Gruppenpraxen. In der Einzelpraxis verfügt ein einzelner Arzt über angestellte Mitarbeiter (ggf. auch angestellte Ärzte). Bei Gruppenpraxen arbeiten entweder mehrere Ärzte mit gemeinsamen Patientenstamm zusammen (sog. Berufsausübungsgemeinschaften) oder die ärztliche Tätigkeit erfolgt getrennt bei gemeinsamer Nutzung bloßer organisatorischer Ressourcen (sog. Organisationsgemeinschaften).[1]

Zudem stellt das Datenschutzrecht unterschiedliche Anforderungen an öffentliche und nicht-öffentliche Stellen. Zwar ist das Betreiben einer ▸

[1] Dochow, PinG 2018, 51 (52).

Arztpraxis als öffentliche Stelle theoretisch denkbar. Im Regelfall sind Arztpraxen aber privatrechtliche Einrichtungen. Daher sind die Datenschutzvorgaben für nicht-öffentliche Stellen maßgeblich.

II. Benennung eines Datenschutzbeauftragten

Die Pflicht zur Benennung eines Datenschutzbeauftragten ist in Art. 37 DS-GVO geregelt. Dieser enthält im ersten Absatz eine Reihe von Tatbeständen, bei deren vorliegen in jedem Fall ein Datenschutzbeauftragter zu benennen ist. Daneben enthält Art. 37 Abs. 4 DS-GVO eine Öffnungsklausel für nationale Gesetzgeber, die es ermöglicht, auch in anderen als den genannten Fällen die Benennung eines Datenschutzbeauftragten vorzuschreiben. Der deutsche Gesetzgeber hat von dieser Öffnungsklausel für nicht-öffentliche Stellen in § 38 BDSG Gebrauch gemacht und damit die Pflicht zur Benennung eines Datenschutzbeauftragten erweitert.

1. Verpflichtende Benennung nach § 38 Abs. 1 S. 1 BDSG

Nach § 38 Abs. 1 S. 1 BDSG haben Verantwortliche einen Datenschutzbeauftragten zu benennen, „soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen". Diese Regelung gilt auch für Arztpraxen unabhängig von ihrer Organisationsform.

Zunächst erfordert § 38 Abs. 1 S. 1 BDSG, dass es sich um eine „automatisierte Verarbeitung" personenbezogener Daten handelt. Gemeint ist damit unter anderem jede IT-gestützte Datenverarbeitung.[2] In modernen Arztpraxen dürfte dieses Tatbestandsmerkmal regelmäßig erfüllt sein. Eine rein analoge Verwaltung von Patientendaten, Terminen und Abrechnungsfragen scheint in der heutigen Zeit kaum noch denkbar.

Darüber hinaus ist eine Pflicht nur dann anzunehmen, wenn „in der Regel mindestens zehn Personen ständig" mit der Datenverarbeitung beschäftigt sind. Diese Formulierung wirft einige Fragen auf. Weitgehend klar ist, dass die relevanten Stellen zumindest auf eine gewisse Dauer angelegt sein müssen.[3] Die konkrete Besetzung ist unerheblich. Auch freie Mitarbeiter oder Leiharbeitnehmer sind in die Berechnung einzubeziehen, ebenso wie Teilzeitbeschäftigte, Auszubildende, Volontäre und Praktikanten.[4]

Wichtig ist außerdem, dass die Datenverarbeitung zumindest auch fester Bestandteil des Aufgabenkreises der Mitarbeiter ist.[5] In einer ärztlichen Praxis dürften somit etwa Putzkräfte oder Hausmeister nicht in den relevanten Personenkreis fallen. Zwar hätten diese theoretisch die Möglichkeit, von entsprechenden personenbezogenen Daten Kenntnis zu erlangen. Die Datenverarbeitung ist jedoch – anders als beispielweise bei Sprechstundenhilfen – nicht Bestandteil ihrer Aufgabenkreise.

Umstritten ist schließlich, ob der Praxisinhaber, in den meisten Fällen also der Arzt selbst, bei der Zählung der Beschäftigten mit einbezogen werden muss. In der Literatur wird dies mit dem Verweis auf den Wortlaut von § 38 Abs. 1 S. 1 BDSG überwiegend abgelehnt.[6] Dort heißt es, dass Verantwortliche einen Datenschutzbeauftragten benennen müssen, soweit sie mehr als zehn Personen „beschäftigen". Der Praxisinhaber ist dabei der Verantwortliche; er ist „Beschäftigender" und nicht selbst Beschäftigter.

Damit lässt sich im Ergebnis festhalten, dass nach § 38 Abs. 1 S. 1 BDSG eine Benennungspflicht immer dann besteht, wenn die relevante Personenzahl von zehn Beschäftigten überschritten wird. Während dies bei Einzelpraxen selten der Fall sein wird, ist dies bei überörtlichen Berufsausübungsgemeinschaften schon eher anzunehmen, da die Beschäftigten an mehreren Praxisstandorten lediglich einer verantwortlichen Stelle zuzurechnen sind.[7]

2. Verpflichtende Benennung nach Art. 37 DS-GVO

Auch direkt aus Art. 37 Abs. 1 DS-GVO kann sich für Ärzte eine Pflicht zur Benennung eines Datenschutzbeauftragen ergeben. Insbesondere Art. 37 Abs. 1 lit. c) DS-GVO ist in diesem Zusammenhang von hoher Relevanz, da Ärzte im Regelfall Gesundheitsdaten i.S.d. Art. 9 Abs. 1 DS-GVO verarbeiten. Nach § 37 Abs. 1 lit. c) DS-GVO greift nämlich die Benennungspflicht immer dann, wenn die Kerntätigkeit eines Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem.

[1] BeckOK DatenschutzR/Moos, § 38 BDSG Rn. 6.

[2] Paal/Pauly, § 38 BDSG Rn. 8.

[3] Kühling/Buchner/Kühling/Sackmann, § 38 BDSG Rn. 10.

[4] Dochow, PinG 2018, 51 (58).

[5] Dochow, PinG 2018, 51 (58); BeckOK DatenschutzR/Moos, § 38 BDSG Rn. 9.

[6] Dochow, PinG 2018, 51 (58).

Art. 9 DS-GVO besteht. Damit nennt die Vorschrift zwei zentrale Tatbestandsvoraussetzungen. Zum einen muss die Verarbeitung zur Kerntätigkeit des Verantwortlichen gehören; zum anderen muss die Verarbeitung selbst auch „umfangreich" sein.

Zunächst ist dementsprechend zu klären, ob die Verarbeitung von Gesundheitsdaten zur Kerntätigkeit eines jeden Arztes gehört oder ob auch hier eine Differenzierung geboten ist. Der Erwägungsgrund 97 der DS-GVO gibt zur Frage der Kerntätigkeit eine Leitlinie vor. Dort heißt es, dass sich die Kerntätigkeit des Verantwortlichen im privaten Sektor auf dessen Haupttätigkeiten bezieht und nicht auf die Verarbeitung von personenbezogenen Daten als Nebentätigkeit. Im medizinischen Sektor ist eine Kerntätigkeit damit zumindest dann anzunehmen, wenn das Geschäftsmodell eines Unternehmens auf der massenhaften Datenverarbeitung beruht, also etwa bei Laboren, die sich auf Genanalysen spezialisiert haben.[8] Im Falle von „gewöhnlichen" Ärzten wird teilweise argumentiert, die Verarbeitung von Gesundheitsdaten gehöre nicht zu deren Kerntätigkeit. Die ärztliche Profession lasse sich nicht auf eine reine Datenverarbeitung reduzieren.[9] Geschäftsmodelle von Ärzten seien keineswegs auf die Analyse von Patientendaten ausgerichtet. Vielmehr wurzelten sie in den kraft akademischer Ausbildung erlernten Fähigkeiten und geistigen Leistungen der Ärzte.

Dem wird allerdings zu Recht entgegengetreten. Die Hauptaufgabe der Ärzte ist die Behandlung von Patienten und die Bekämpfung von Krankheiten. Dies erfordert regelmäßig eine umfassende Untersuchung und Beobachtung des Patienten, typischerweise auch über einen längeren Zeitraum.[10] Ohne dabei beispielsweise in Krankenakten gesundheitsbezogene Daten der Patienten zu verarbeiten, wäre der Arzt kaum in der Lage, seiner Aufgabe in wirksamer Form nachzukommen.[11] Somit ist davon auszugehen, dass auch bei niedergelassenen Hausärzten die Verarbeitung von sensiblen Daten Teil der Kerntätigkeit ist.

Diese Datenverarbeitung muss allerdings nach Art. 37 Abs. 1 lit. c) DS-GVO auch „umfangreich" sein, damit sie die Pflicht zur Benennung eines Datenschutzbeauftragten begründen kann. Wann eine solche „umfangreiche" Verarbeitung anzunehmen ist, lässt sich der DS-GVO allerdings nicht direkt entnehmen. Lediglich Erwägungsgrund 91 der Verordnung befasst sich mit dem Begriff der umfangreichen Verarbeitung. Dabei ist allerdings zu beachten, dass sich der Erwägungsgrund eigentlich auf Art. 35 DS-GVO bezieht und sich nicht ausdrücklich mit den Kriterien des Art. 37 DS-GVO befasst. Trotzdem vermag er einen ersten Anhaltspunkt bei der Auslegung geben, da auch Art. 35 DS-GVO den Begriff der „umfangreichen Verarbeitung" nutzt und eine einheitliche Auslegung innerhalb der Verordnung nahe liegt. Nach dem Erwägungsgrund sind umfangreiche Verarbeitungsvorgänge unter anderem solche, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und – beispielsweise aufgrund ihrer Sensibilität – wahrscheinlich ein hohes Risiko mit sich bringen. Auch die Art. 29-Datenschutzgruppe schlägt für die Auslegung des Begriffs ähnliche Kriterien vor.[12]

Speziell in Bezug auf den medizinischen Sektor ist nach dem Erwägungsgrund nicht von einer umfangreichen Verarbeitung auszugehen, wenn die Verarbeitung personenbezogener Daten von Patienten durch einen einzelnen Arzt erfolgt. Dies legt nahe, dass das Kriterium der Beschäftigtenzahl bzw. die Zahl der Personen, die auf die Daten Zugriff haben, auch im Rahmen der Benennungspflicht nach der DS-GVO eine Rolle spielen mag. Gleichwohl sorgt aber auch dieser Hinweis nicht für die nötige Rechtssicherheit in der Praxis. Wann nämlich im positiven Sinne eine „umfangreiche Verarbeitung" und damit einhergehend eine Benennungspflicht anzunehmen ist, lässt sich dem Erwägungsgrund nicht entnehmen.

Teilweise wird bei der Frage nach einer „umfangreichen Verarbeitung" i.S.d. DS-GVO auch auf § 38 Abs. 1 BDSG verwiesen. Der Bundesgesetzgeber habe bei der Schaffung des § 38 Abs. 1 BDSG die Wertung nachvollzogen, dass eine „umfangreiche Verarbeitung" erst in Betracht kommt, wenn mindestens zehn Personen mit der Datenverarbeitung befasst seien.[13] Dieses Argument vermag jedoch nicht zu überzeugen. Die DS-GVO ist unabhängig vom ▸

[8] Dochow, PinG 2018, 51 (58).
[9] Dochow, PinG 2018, 51 (58).
[10] Kühling/Buchner/Bergt, Art. 37 DS-GVO Rn. 24.
[11] Art. 29-Datenschutzgruppe, WP 243, S. 8.
[12] Art. 29-Datenschutzgruppe, WP 243, S. 9.
[13] Dochow, PinG 2018, 51 (59).

Willen der nationalen Gesetzgeber auszulegen. Das Recht der nationalen Gesetzgeber zur Regelung der Benennungspflicht umfasst nur andere als die in Art. 37 Abs. 1 DS-GVO genannten Fälle, vgl. Art. 37 Abs. 4 DS-GVO.

Trotzdem sieht auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine Benennungspflicht für Ärzte vor, soweit diese in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen.[14] Dabei soll der Praxisinhaber selbst mitzuzählen sein. Wenn weniger als zehn Personen mit der Verarbeitung beschäftigt sind, soll in der Regel kein Datenschutzbeauftragter zu benennen sein. Eine Ausnahme davon sei zu machen, wenn im Einzelfall ein hohes Risiko für Rechte und Freiheiten zu erwarten ist.

Wenngleich diese Hinweise der Aufsichtsbehörden vor dem Hintergrund der Rechtssicherheit zu begrüßen sind, so findet die pauschale Festlegung einer relevanten Personenanzahl in der DS-GVO selbst keinerlei Stütze. Vielmehr gebietet eine unionsrechtskonforme Auslegung eine umfassende Abwägung im Einzelfall anhand der oben genannten Kriterien. Bei Einzelpraxen dürfte diese Abwägung – schon wegen der ausdrücklichen Nennung in Erwägungsgrund 91 – regelmäßig dahingehend ausfallen, dass die Benennung eines Datenschutzbeauftragten nicht erforderlich ist.

III. Führen eines Verzeichnisses von Verarbeitungstätigkeit

In einem weiteren Schritt stellt sich die Frage, ob eine Arztpraxis ein „Verzeichnis von Verarbeitungstätigkeiten" führen muss, welches das nach altem Recht bekannte Verfahrensverzeichnis ersetzt. Ein solches Verzeichnis ist eine schriftliche oder elektronische Aufzeichnung aller Verarbeitungstätigkeiten mit personenbezogenen Daten.[15] Diese Auflistung ist vorzuhalten und gem. Art. 30 Abs. 4 DS-GVO der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Zur Erstellung und Führung eines solchen Verzeichnisses ist nach Art. 30 Abs. 1 DS-GVO jeder „Verantwortliche" verpflichtet. Verantwortlicher ist gem. Art. 4 Nr. 7 DS-GVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern gilt die Pflicht zum Führen eines Verzeichnisses gem. Art. 30 Abs. 5 DS-GVO allerdings nicht, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 DS-GVO.

Damit sind auch Arztpraxen zum Führen eines Verzeichnisses von Verarbeitungsvorgängen verpflichtet. Zum einen entscheiden Ärzte über die Verarbeitung von personenbezogenen Daten in ihrer Praxis und sind damit Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO. Zum anderen werden in einer Arztpraxis regelmäßig besondere Kategorien personenbezogener Daten verarbeitet, zu denen nach Art. 9 Abs. 1 DS-GVO auch Gesundheitsdaten gehören.[16] Wie ein solches Verzeichnis für eine Arztpraxis aussehen könnte, hat das Bayerische Landesamt für Datenschutzaufsicht in einem Muster beispielhaft dargestellt.[17]

IV. Fazit

Die Frage nach der Pflicht zur Benennung eines Datenschutzbeauftragten ist für Arztpraxen differenziert zu beantworten. Unproblematisch besteht eine solche Pflicht aus § 38 Abs. 1 S. 1 BDSG nur, wenn ein Arzt in seiner Praxis mindestens zehn Mitarbeiter mit der Datenverarbeitung beschäftigt. Gerade für Arztpraxen mit weniger als zehn Mitarbeitern ist allerdings vieles streitig. Hingegen besteht für sämtliche Arztpraxen die Pflicht zum Führen eines Verzeichnisses von Verarbeitungsvorgängen. Diese Pflicht besteht insbesondere unabhängig von der Mitarbeiterzahl und verlangt nicht, dass die Datenverarbeitung zur Kerntätigkeit der Praxis gehört.

[14] Datenschutzkonferenz, Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/04/DSB-Bestellpflicht.pdf (zuletzt abgerufen am: 10.09.2018).

[15] Siehe allgemein zum Verzeichnis von Verarbeitungstätigkeiten: Datenschutzkonferenz, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO, abrufbar unter: https://www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf (zuletzt abgerufen am: 10.09.2018).

[16] Bundesärztekammer, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, S. 12, abrufbar unter: https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf (zuletzt abgerufen am: 10.09.2018).

[17] Bayerisches Landesamt für Datenschutzaufsicht, Muster 5: Arztpraxis – Verzeichnis von Verarbeitungstätigkeiten, abrufbar unter: https://www.lda.bayern.de/media/muster_5_arztpraxis_verzeichnis.pdf (zuletzt angerufen am: 10.09.2018).

V. Weiterführende Links

• *Bayerisches Landesamt für Datenschutzaufsicht*, Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. – Muster 5: Arztpraxis, abrufbar unter:

https://www.lda.bayern.de/media/muster_5_arztpraxis.pdf

(zuletzt abgerufen am: 10.09.2018).

• *Bundesärztekammer*, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, abrufbar unter:

https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf

(zuletzt abgerufen am: 10.09.2018).

• *Datenschutzkonferenz*, Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken, und sonstigen Angehörigen eines Gesundheitsberufs – Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018, abrufbar unter:

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/04/DSB-Bestellpflicht.pdf

(zuletzt abgerufen am: 10.09.2018).

• *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Die Datenschutz-Grundverordnung tritt in Kraft – das müssen selbstständige Heilberufler beachten, abrufbar unter:

https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbstaendige-Heilberufler-beachten.html

(zuletzt abgerufen am: 10.09.2018).

Über den Autor

Prof. Dr. Thomas Hoeren

Rechtswissenschaftliche Fakultät
ITM – Institut für Informations-, Telekommunikations- und Medienrecht - Landeskompetenzzentrum - Zivilrechtliche Abteilung

▶ www.uni-muenster.de