17 Verarbeitung von Daten bei Einschaltung Externer

Bei vielen modernen Arztpraxen herrscht die Ansicht vor, dass man immer mehr vernetzte IT rund um die Behandlung des Patienten einsetzen muss, um ihn noch besser zu behandeln. Diese durchaus nachvollziehbare, jedoch auch diskussionswürdige Ansicht geht aber mit einer nicht unbedeutenden Konsequenz einher, die viele Ärzte, die immer mehr Digitalisierung einsetzen wollen, oftmals nicht so wirklich „auf dem Schirm" haben. Denn aus dem Einsatz von immer mehr vernetzter IT resultiert automatisch, dass damit auch immer mehr Externe, wie z. B. Softwareanbieter, Medizinprodukteherstelle r etc., Zugriff bzw. die Zugriffsmöglichkeit auf Patientendaten bekommen. Durch die Einbeziehung immer mehr externer Dienstleister in die Datenverarbeitung und die damit permanent zunehmende Übermittlung von Patientendaten an Externe steigt systemimmanent das Risiko für den Patienten, dass seine Daten nicht mehr ordnungsgemäß verarbeitet werden, mit den in *Kapitel 12* genannten Konsequenzen. Denn je mehr Stellen an einer Datenverarbeitung beteiligt sind, umso komplexer, intransparenter und schwerer beherrschbar wird diese für den Verantwortlichen (Arzt/Praxis). Konsequenterweise muss daher ein Arzt/eine Praxis mit jeder Einschaltung von Externen in die Datenverarbeitung verpflichtet werden zu gewährleisten, dass diese Externen ordnungsgemäß mit den vom Patienten anvertrauten Daten umgehen. Dieses gebieten alleine der Respekt vor dem Patienten sowie das Vertrauensverhältnis, das der Arzt zum Patienten hat. Es darf nicht sein, dass ein Arzt leichtfertig die Daten des Patienten, und damit auch das Vertrauensverhältnis zu ihm, durch die unbedachte Einbeziehung von Personen/Unternehmen, die nicht an der Behandlung beteiligt sind, aufs Spiel setzt.

Zum Schutz der Betroffenen (Patienten) und des Vertrauensverhältnisses zwischen Arzt und Patienten ist es daher auch

nur konsequent, dass die einschlägigen gesetzlichen Regelungen hohe Anforderungen an die rechtskonforme Einbindung externer Personen/Dienstleister in die Datenverarbeitung stellen. Wie durch die Regelungen der DSGVO deutlich wird (hierbei insbesondere Art. 26 und Art. 28), sieht auch die DSGVO in der Einschaltung Externer ein nicht unerhebliches Risikopotenzial. Aus diesem Grund gibt sie dem Verantwortlichen (Arzt/Praxis) strenge Vorgaben auf, die er zwingend erfüllen muss. Erfüllt der Arzt diese Vorgaben nicht, ist die von ihm bzw. dem Externen durchgeführte Datenverarbeitung rechtswidrig und es drohen die in *Kapitel 19* dargestellten Sanktionen. Mithin ist ein Arzt gut beraten, bei der Einschaltung von Externen und der damit verbundenen Möglichkeit, dass diese auf die Daten zugreifen können, sich streng an die Vorgaben der DSGVO zu halten.

Um die gesetzlichen Anforderungen überhaupt erfüllen zu können, ist es gerade bei der Einschaltung externer Dienstleister essenziell, diese Einbindung (im Vorfeld) genau zu planen. Diesbezüglich ist es notwendig, sich **VOR** Beauftragung eines Dienstleisters/Beschaffung eines Produkts umfassende Kenntnis darüber zu verschaffen, wie die Datenverarbeitung durch den Externen konkret abläuft, zu welchen Zwecken er die Daten verarbeiten will, welche Garantien er geben kann, dass die Datenverarbeitung ordnungsgemäß ablaufen kann, usw. Denn erst bei einer entsprechenden Transparenz über die Datenverarbeitung des Externen kann ein Arzt/eine Praxis als datenschutzrechtlicher Verantwortlicher entscheiden, welche „Rolle" bzw. Verantwortlichkeit dem Externen im Rahmen der Datenverarbeitung zukommen soll.

Die Einordnung der Verantwortlichkeit sollte niemals auf einer „Pi mal Daumen"-Entscheidung beruhen, sondern aufgrund der Tragweite, die mit dieser Entscheidung verbunden ist, immer anhand der ermittelten Fakten des jeweiligen Einzelfalls erfolgen. Dabei ist es essenziell zu prüfen, welche Aufgaben der Externe konkret erfüllen und in wie weit er bei der Erfüllung

dieser Aufgaben „weisungsgebunden" bzw. „weisungsfrei" sein soll. Mithin kommt es bei der Bestimmung der Verantwortlichkeit darauf an zu prüfen, ob und inwieweit der Arzt/die Praxis dem Externen vorgeben kann, wie dieser die Daten verarbeiten soll. Wie nachfolgend dargestellt werden wird, ist die rechtliche und faktische Weisungsgebundenheit des Externen ein nicht unerhebliches Indiz für die Annahme einer sog. Auftragsverarbeitung. Fehlt eine solche Weisungsgebundenheit und verarbeitet der Externe die Daten nach seinem eigenen „Gusto", dürfte keine Auftragsverarbeitung vorliegen, sondern eine eigene bzw. gemeinsame datenschutzrechtliche Verantwortlichkeit, was wiederum Konsequenzen für beide Seiten nach sich ziehen kann. Die Grenzen zwischen den unterschiedlichen Rechtsfiguren „Gemeinsame Datenverarbeitung", „Auftragsverarbeitung" und „Übermittlung von Daten an einen weiteren Verantwortlichen" sind fließend, weshalb es essenziell ist, den jeweiligen Verarbeitungssachverhalt genau zu analysieren und anhand der Fakten eine Entscheidung zu treffen. Denn alle diese Rechtsfiguren zählen zu den Empfängern. Bevor sich das vorliegende Kapitel mit den einzelnen Rechtsfiguren auseinandersetzt, soll kurz der Begriff des „Empfängers" von Daten, der bspw. auch im Rahmen des Verarbeitungsverzeichnisses eine Rolle spielt, erläutert werden.

17.1 Empfänger

Um Transparenz über die Datenverarbeitungen zu erhalten, sieht die DSGVO wie in *Kapitel 11.7.5* beschrieben vor, dass ein Verantwortlicher im Verarbeitungsverzeichnis die jeweiligen **Empfänger** bzw. Kategorien von Empfängern aufführen muss, die Daten von ihm erhalten. Meiner Ansicht nach will die DSGVO mit dieser Anforderung u. a. erreichen, dass der Verantwortliche die bei ihm stattfindenden Datenströme etc. genau analysiert und sich dadurch der weiteren Beteiligten, die seine Daten erhalten (Empfänger), bewusst wird (*siehe hierzu auch Kapitel 7.4*).

Der Begriff des Empfängers ist in Art. 4 Nr. 9 definiert. Dieser Definition folgend, können Empfänger quasi alle Personen, Unternehmen, Behörden, etc. sein, denen der Verantwortliche Daten übermittelt bzw. die „Einsicht" in personenbezogene Daten erhalten/erhalten können.

Daher bezieht sich der Begriff des Empfängers zum einen auf interne Empfänger, wie z. B. die in der Organisation des Verantwortlichen tätigen Personen oder Abteilungen.

Darüber hinaus betrifft dieser Begriff aber gerade auch externe Personen/Unternehmen, die Daten des Verantwortlichen erhalten bzw. auf diese zugreifen können. Bei diesen externen Empfängern gilt es, streng zwischen „gemeinsamen Verantwortlichen", „Auftragsverarbeitern" und „weiteren, zusätzlichen Verantwortlichen", die gerade keine „gemeinsamen Verantwortlichen" sind, zu unterscheiden.

Gerade die mit der DSGVO für Deutschland neu eingeführte Rechtsfigur des „gemeinsam Verantwortlichen" gem. Art. 26 dürfte in der Praxis noch für einigen Diskussionsbedarf sorgen.

17.2 Gemeinsam für die Verarbeitung Verantwortliche

Die DSGVO regelt in Art. 26 die „Gemeinsam für die Verarbeitung Verantwortlichen". Dieses Rechtsinstitut war bereits in der damaligen EG-Datenschutzrichtlinie vorgesehen, doch hat der deutsche Gesetzgeber dieses, aus welchen Gründen auch immer, niemals in deutsches Recht transferiert. Durch die Neuregelung des Art. 26, der aufgrund der direkten Anwendbarkeit der DSGVO auch in Deutschland direkt anzuwenden ist, sollte sich ein Arzt/eine Praxis mit diesem Rechtsinstitut auseinandersetzen. Dieses empfiehlt sich insbesondere deshalb, weil an die gemeinsame Verantwortlichkeit Verpflichtungen geknüpft sind, bei deren Nichteinhaltung Sanktionen drohen können (vgl. Art. 83 Abs. 4 a).