David Seiler ist seit 20 Jahren Rechtsanwalt mit langjähriger Erfahrung als Banksyndikus und berät vornehmlich zu Fragen des Datenschutz-, IT- und Zahlungsverkehrsrechts sowie Urheber- und Fotorechts.

Überblick zur Datenverarbeitung im medizinischen Bereich unter der DSGVO

Unter Berücksichtigung der Novellierung des § 203 StGB

David Seiler

Die Datenschutz-Grundverordnung ist wegen der am 25. Mai 2018 ablaufenden Übergangsfrist und der ab dann eingreifenden erhöhten Anforderungen an den Datenschutz und die Datensicherheit sowie wegen der verschärften Sanktionen Anlass, das Thema Datenschutz in allen mit der Verarbeitung personenbezogener Daten befassten Unternehmen und Branchen einer gründlichen Revision und gegebenenfalls Anpassung zu unterziehen. Dies gilt auch und gerade im medizinischen Bereich mit besonders sensiblen Daten. Ohne Anspruch auf Vollständigkeit und mit subjektiver Schwerpunktsetzung werden nachfolgend einige datenschutzrechtliche Fragen im medizinischen Bereich mit Blick auf die Datenschutz-Grundverordnung näher behandelt.

I. Einleitung

Der medizinische Bereich umfasst nach dem hier zugrunde gelegten Verständnis insbesondere Arztpraxen, Krankenhäuser und medizinische Dienstleister, wie z. B. labormedizinische Betriebe. Für Krankenhäuser, die oft öffentlich-rechtlich organisiert sind, gelten neben der Datenschutz-Grundverordnung vielfach auch Landesdatenschutz- und Landeskrankenhausgesetze. Mit Blick auf die Konzentration des vorliegenden Beitrages auf die Datenschutz-Grundverordnung liegt der Schwerpunkt im Folgenden auf datenschutzrechtlichen Fragen der Arztpraxis. Gerade in diesem Bereich scheint es über die an und für sich selbstverständliche ärztliche Schweigepflicht hinaus für die spezifischen technischen und organisatorischen Anforderungen und Besonderheiten des Datenschutzrechts noch einiges an Aufklärung und Nachholbedarf zu geben, wie Tätigkeitsberichte der Datenschutzaufsichtsbehörden,[1] arbeitsgerichtliche Entscheidungen[2] sowie Presseveröffentlichungen[3] zeigen.

1 Z. B. 6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2013 und 2014, Ziff. 3.4.7.

2 LArbG Baden-Württemberg, Urt. v. 11. 11. 2016 – 12 Sa 22/16 (außerordentliche Kündigung einer Arzthelferin, die per WhatsApp Informationen über einen Patienten an ihre Tochter weitergibt, welche diese Informationen im Sportverein herumzeigt). LAG Berlin-Brandenburg, Urt. v. 11. 04. 2014 – 17 Sa 220/13 (Krankenschwester postet Foto eines Neugeborenen auf Facebook).

3 Plaudertaschen in vielen Praxen, Test 3/2016, S. 88 ff.

II. Begriffsdefinitionen

Bereits in den Begriffsdefinitionen finden sich im Hinblick auf die medizinische Datenverarbeitung Änderungen zum BDSG alter Fassung. Wird in § 3 Abs. 9 BDSG das Stichwort „Gesundheit" lediglich als eine Form der besonderen Art personenbezogener Daten erwähnt, findet sich in Art. 4 Nr. 15 DSGVO eine Definition des Begriffes Gesundheitsdaten, die in ErwG. 35 DSGVO näher erläutert wird. Hinzu kommt die Definition „genetischer Daten" in Nummer 13 (ErwG. 34 DSGVO) und „biometrische Daten" in Nummer 14.

1. Gesundheitsdaten

Gesundheitsdaten sind nach Art. 4 Nr. 15 DSGVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Näher erläutert wird diese Definition in ErwG. 35 DSGVO dahingehend, dass dazu alle Daten gehören, die sich auf den früheren, gegenwärtigen und künftigen Gesundheitszustand einer Person beziehen. Umfasst sind auch Informationen über die Person, die im Zuge der Anmeldung sowie der Erbringung von Gesundheitsdienstleistungen erhoben werden: Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt werden, um diese für gesundheitliche Zwecke eindeutig zu identifizieren.

Gerade die sehr weitgehende Definition, die auch an sich abstrakte Pseudonyme erfasst, macht deutlich, welche Anstrengungen für die Einhaltung datenschutzrechtlicher Bestimmungen bei der Verarbeitung medizinischer Daten für Forschungszwecke erforderlich sind, wenn die Anonymisierung der Daten beabsichtigt bzw. erforderlich ist.

Zu den Gesundheitsdaten gehören weiterhin diagnostische Daten, die aus der Prüfung oder Untersuchung des Körpers, eines Körperteils (z. B. durch bildgebende Verfahren) oder körpereigener Substanzen (Gewebeproben, Blutproben, Stuhl- und Urinproben), sowie Daten, die aus genetischen Daten und biologischen Proben abgeleitet werden. Auf die Herkunft der Daten kommt es nicht an. Potentielle Datenquellen können ein Arzt, sonstige Angehörige eines Gesundheitsberufs, ein Krankenhaus, ein Medizinprodukt (z. B. Blutkonserven) oder eine In-Vitro-Diagnostik sein. Deutlich wird an der Erwähnung genetischer Daten, dass es zu einer Überschneidung mit der Begriffsdefinition in Art. 4 Nr. 13 DSGVO kommt. Die Abgrenzung zwischen Gesundheitsdaten und genetischen Daten dürfte dort zutreffend sein, wo aus den abstrakten genetischen Daten, Bewertungen und Schlussfolgerungen gezogen werden, die Aussagen über den Gesundheitszustand, Krankheiten, Behinderungen oder Gesundheitsrisiken einer konkreten Person beinhalten.

2. Biometrische Daten

Art. 4 Nr. 14 DSGVO definiert biometrische Daten als physische, physiologische oder verhaltensbedingte Merkmale einer natürlichen Person, z. B. Gesichtsbilder oder Fingerabdrücke. Es handelt sich somit zwar um körperliche Merkmale, die auch „diagnostische" Daten wie Körpertemperatur und Pulsgeschwindigkeit beinhalten können, deren Erhebungszweck sich jedoch nicht auf medizinische, sondern auf sicherheitstechnische Anwendungen bezieht.

3. Genetische Daten

Genetische Daten werden nach ErwG. 34 DSGVO als personenbezogene Daten über ererbte oder erworbene genetische Eigenschaften verstanden, die aus der Analyse von Chromosomen, DNS oder RNS gewonnen werden. Einer irgendwie gearteten Bewertung dieser Daten im medizinischen Sinne bedarf es zur Erfüllung der Begriffsdefinition nicht.

4. Besondere Kategorien personenbezogener Daten

Sowohl genetische wie biometrische Daten als auch Gesundheitsdaten gehören nach Art. 9 DSGVO zu den besonderen Kategorien personenbezogener Daten. Deren Verarbeitung ist grundsätzlich untersagt, Art. 9 Abs. 1 DSGVO, wenn nicht einer der in Abs. 2 genannten Ausnahmefälle vorliegt. Insbesondere ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn die betroffene Person ausdrücklich eingewilligt hat, Art. 9 Abs. 2 lit. a) DSGVO, oder die Datenverarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich ist und die betroffene Person zum Beispiel aus körperlichen Gründen außerstande ist, ihre Einwilligung zu geben.

Bei Patienten, die bei Bewusstsein und Verstand sind, stets eine Einwilligung einzuholen, welche den Bedingungen für eine Einwilligung nach Art. 7 DSGVO genügen müsste, wären in der ärztlichen Praxis eine kaum zu leistende Anforderung. Daher sieht Art. 9 Abs. 2 lit. h) der DSGVO für die Verarbeitung besonderer Kategorien von Daten, insbesondere Gesundheitsdaten, für Zwecke der Gesundheitsversorgung und für die medizinische Diagnostik sowie die Versorgung und Behandlung eine Ausnahme vor, wenn diese Datenverarbeitung aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufes erfolgt[4] und die Datenverarbeitung von Fachpersonal durchgeführt wird, welches einem Berufsgeheimnis unterliegt. Bei dem Vertrag wird es sich regelmäßig um einen Behandlungsvertrag nach § 630a BGB handeln. Das Berufsgeheimnis ergibt sich für Ärzte und andere Angehörige von Heilberufen aus § 203 Abs. 1 Nr. 1 StGB sowie aus dem in § 9 MBO-Ä verankerten hippokratischen Eid.

Somit dürfte sich zumindest in diesem Punkt, was die ärztliche Praxis der Datenverarbeitung und deren Zulässigkeit angeht, keine wesentliche praktische Änderung ergeben. Zwar böte es sich an, wenn ohnehin eine Aufklärung über und eine Einwilligung in die Behandlung zum Ausschluss einer Körperverletzung und zur Vermeidung von Haftungsrisiken erfolgt, auch eine ausdrückliche datenschutzrechtliche Einwilligung einzuholen. Jedoch besteht hierbei das Risiko, die strengen Bedingungen an eine informierte Einwilligung nach Art. 7 DSGVO nicht ausreichend einzuhalten. Die Rechte der Betroffenen, insbesondere die Pflicht zur transparenten Information nach Art. 12 f. DSGVO, sind gleichwohl einzuhalten.

4 Durch die Qualifizierung des Vertragspartners und Verantwortlichen geht diese Regelung über Art. 6 Abs. 1 lit. b) DSGVO hinaus.